VII.83

11 February 1965

Recollections of Work on Russian

The first formal U.S. effort to solve a Russian crypto-system was undertaken in the early 1930's, an effort directed at the messages of the Amtorg Trading Corporation, which at that time was under investigation by a committee of Congress. The Chairman of the committee, Representative Hamilton Fish, had subpeonaed the Amtorg files, which contained a considerable volume of code messages. The committee felt that these messages were important and Representative Fish formally requested that the Navy Department's experts try to recover the plain text of the messages. This work was undertaken in the Code and Signal Section by Safford and Wenger.

After the Navy worked several weeks without success, Representative Fish requested the assistance of the Army's experts, and a conference was held between members of the SIS (Mr. Friedman, Dr. Kullback, Dr. Sinkov, and Mr. Rowlett) and CDR Safford and LT Wenger of the Navy Department. Safford and Wenger explained that they had recovered some elements of the Russian cryptography employed in the Amtorg messages; however, they were unable to recover the basic system employed or to provide translations of the messages. In summary, they concluded that the system involved the following elements:

Basic code books, numerical.

Additive books.

A literal substitution applied to the numerical text resulting from the application of the additives to the basic code. The Navy cryptanalysts had recovered the literal substitution and developed certain information about the indicator systems which designated the pads used for the respective messages. They had been unable to go beyond this point.

The Army cryptanalysts accepted copies of the materials from the Navy Department and undertook to validate and extend the work done by the Navy. After several weeks, it was finally concluded that the Navy

cryptanalysts had done all that could be accomplished with the data and that the Army group could not offer any hopes of additional success. (At Tab A will be found an extract of TRQ: 77: Data on Soviet Cryptographic Systems 1917-1933, Historical Unit, AS-14A, which presents this episode in fuller detail.)

In the priorities of effort applied to the early Army group, three nations stood out from all others: Japan was highest, followed by Germany and Italy. The other nations of the world were grouped together in lower priority. Because of the limited number of personnel available, very little cryptanalytic work was done on the last group of nations. However, any governmental traffic from these nations which fell into our hands was identified and filed, with the expectation that when the opportunity arose work would be started on those countries which offered the greatest promise of results. In these early days a small amount of Russian traffic was accumulated, but no cryptanalytic effort was undertaken. I do recall that several times between 1935 and the outbreak of World War II we examined the Russian materials available to us; however, this examination was cursory and no serious effort was started in this period.

When World War II broke out, the Army had to decide whether to concentrate all its signal intelligence effort on the military systems of the Axis or to divert certain of its resources to a study of the diplomatic traffic of the Axis nations and of certain other powers, such as Russia, Brazil, Vichy France, Portugal, Spain, etc. This decision was complicated by the fact that the Navy, shortly after Pearl Harbor, had directed all its effort at naval traffic, dropping all effort on diplomatic traffic. If the Army similarly directed its total effort exclusively at the military communications of the Axis powers, the U.S. Government would then be left without any awareness of the diplomatic situation as it developed through the progress of the war. Happily, the Army took the decision to expend some of its resources against the diplomatic traffic of the Axis powers and provided for undertaking work on the traffic of other nations of high interest. It might be worth noting that certain of us in the Army were convinced, although we could not prove it at that time, (1) that the earliest indications of the weakening of the Axis would appear in their diplomatic messages, (2) that the reliability of the so-called friendly nations could be sensed through reading their diplomatic

traffic, and (3) that valuable information could be derived from the other nations regarding their intentions and activities toward both the Axis and the Allies. A further and most important consideration: we realized that, if the war was successfully prosecuted, the Government would have in being an active COMINT organization with continuity developed from the favorable (that is, to the cryptanalyst) circumstances of a world emergency, for such a situation provides many opportunities arising from misuse and "second-story cryptanalysis" that could be exploited. In retrospect, it appears that this approach was based on the accurate premise that, while the war might last several years, ultimately the Allies would be successful.

Shortly after the SIS moved to Arlington Hall Station, the General Cryptanalytic Branch was formed, with the general mission of developing an effort on all diplomatic systems, both Axis and other, and all military systems except Japanese.

With the exception of the effort on Russia, the work done by the General Cryptanalytic Branch is covered in "The General Cryptanalytic Problems, Volume II" of the History of the Signal Security Agency. The work on the Russian was not recorded in the Branch history because it was considered highly sensitive and precarious. In late 1942 a small section was formally established to organize the intercepted Russian traffic and to attempt a diagnosis of the Russian cryptosystems. This small section was to be backstopped by the skilled cryptanalysts of the Research Section of the Branch. 1/ This first Russian section was short-lived - for some reason which I do not remember it was disbanded. A few

1/ This Research Section was composed of a number of individuals who were recognized as the best cryptanalysts of the Army Security Agency: Mr. Ferner, Chief, and Mr. Albert Small, deputy, both of whom actively participated in the work of the Russian Section.

I believe that the establishment of this Research Section was the genesis of our present P1 concept; it was probably broader than our present concept in that this group was formally committed to supporting the analysis of our own COMSEC systems as well as to provide assistance to the various sections of the General Cryptanalytic Branch and, when required, to assist in difficult problems of the sister branch, the Japanese Military Branch.

weeks later, its successor was established under one of our best Russian scholars - Lt Ferdinand Coudert of the famous New York law firm, who had undertaken the study of Russian as an avocation. This group, which was gradually expanded, endured throughout the war, operating under the strictest possible compartmentation. (See Tab B)

In this period, there were three major sources of Russian traffic; the most important was the Washington/Ladd Field, Alaska, landline. The Russian government had been provided telegraphic facilities by the U.S. Signal Corps for communications between its mission in Washington and the operations at Ladd Field, a key point on the Lend-Lease logistics route. Simultaneous with the installation of this special facility for the Russians, "spy" teleprinters were installed in A Building at Arlington Hall Station to provide copies of all messages passing on the circuit. Traffic from this source proved invaluable in the later development of certain high level systems. Another important source was the so-called SHAMROCK.

[redacted]

At this point it should be noted that, in the early liaison with the U.K., the technical results of the U.K.'s long-established Russian effort was not provided to the cryptanalysts at ASA. The intelligence activities - G2 and ONI - did receive, on a limited distribution basis, certain information developed by the U.K., but the ASA technical effort was denied the advantage of British technical results in the development of its Russian effort until the end of the war.

Another, and most significant, event occurred several months after we had begun our work on the Russian, some months before the end of the war. Colonel Carter Clark, who was assigned to G2 during most of the war, met with Col Corderman, Chief, Army Security Agency, and myself (I was OIC of the General Cryptanalytic Branch). Clark told us that he had received instructions - allegedly from the White House - to

(b) (1)
(b) (3)-50 USC 403
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

the effect that the Army was not to work on Russian communications and that any effort which had been undertaken would be stopped. Apparently the White House had learned that the Army Security Agency had been successful in breaking Russian codes and had concluded that this activity was not in keeping with the spirit of our relations with the Russian government. Fortunately, Col Clark never relayed this order formally to AHS, since the circumstances by which he received the instructions were suspiciously informal and lacked the validity of a White House order.[2] In fact, following this episode, additional resources continued to be assigned to the Russian section as required, when appropriate skills were available.

After VE day (May 1945), the ASA intensified the build-up of its Russian effort. Skilled technicians freed from the German effort were assigned to it. These were selected carefully, with a view to insuring that the full spectrum of analysis (TA, linguistics, code recovery, additive recovery, machine cryptanalysis) was represented by the best skills available. Individuals, both at Arlington Hall and in the overseas contingents, who had made names for themselves through their work on the German and Japanese systems were earmarked for assignment to the problem as soon as they could be spared from the closing out of the problems to which they had been assigned.

2/ Later considerations led to the conclusion that this "edict" originated with a prominent member of Mr. Roosevelt's staff, who was later alleged to be a "fellow traveler." At the time this event occurred, we had not been successful in reading any worthwhile Russian system; we had, however, solved certain simple systems and it may be that our success with these simple systems, filtering through G2 to the staff member, was distorted by him into what could be construed as a major success against the Russians. We could, of course, speculate that this would cause him to take this action and that our phenomenal success on Japanese and German cryptography would lead him to the conclusion that we would be equally successful on Russian. We could further speculate that he did not want to run the risk that his name would appear in an Arlington Hall translation of a Russian message.

With 0.9+ probability I speculate that the individual in question was [illegible]. His name & [illegible] (Russian) [illegible] in [illegible] read [illegible] material.

An important consideration in the intensification of the Russian effort arose out of the Potsdam Big Three Conference (July 17 - August 2, 1945). Starting on 11 July 1945, and before the conference opened, a series of most important Japanese diplomatic messages were deciphered. These contained instructions to the Japanese Ambassador in Moscow directing him to approach the Russian Foreign Office with a view to having the Russians intercede with the Allies for negotiating an "honorable peace." (At Tab C will be found a typical message in the exchange which is representative of the position taken by the Japanese Foreign Office.) The end result, in effect, was that the Japanese were given a diplomatic "brush-off." Decoded Japanese Diplomatic (Purple) messages between Moscow and Tokyo show that the Japanese Ambassador and the Russian Foreign Office had discussed this in Moscow shortly before the Big Three Conference (Truman, Stalin and Churchill, who was replaced by Atlee after July 25). As I understand it, Stalin did not reveal the Japanese proposal to the Allies during this conference. Truman, Churchill and Atlee of course were fully informed of the Japanese proposal and the results of the discussions with the Russians; translations of the Japanese messages had been made available to each as the demarche developed. I believe it was this episode which, more than any one other single action or consideration, convinced us (both the Army and Navy) that Russia was our overriding postwar cryptologic target.

The Tokyo-Moscow messages mentioned above served another purpose: they provided positive information to the Army and Navy technical groups that the defeat of Japan could be expected in the next few weeks. As a measure of prudent planning, the technical managers in both services began informally to develop plans for redirecting the technical effort and developing its postwar configuration. One of the earliest acts was the establishment of the so-called "BOURBON" arrangement (BOURBON was the cover name for the Russian problem). This arrangement was aimed at providing the most effective collaboration of the Army and Navy on the Russian problem and envisaged extension of the U.K. wartime collaboration into the postwar years. (At Tab D will be found a paragraph dealing with the collaboration with the U.K. as copied from "The Narrative History of AFSA/NSA - Part I.")

/s/ FRANK B. ROWLETT

FRANK B. ROWLETT
Special Assistant to the Director

4 Incls.
a/s

The Amtorg Trading Company Case

"The Amtorg Trading Company case.--In 1931 the attention of the cryptanalysts of the Signal Intelligence Section, Office of the Chief Signal Officer, turned their attention to the traffic of the Amtorg Trading Corporation, a Soviet affiliate operating in New York City.

"This project had its raison d'etre in an investigation conducted by Representative Hamilton Fish of New York into Communist propaganda in the United States. The Congressional Committee subpoenaed about 3,000 code messages sent by the Amtorg Corporation to Moscow and submitted them to the Code and Signal Section of the Navy for solution.* (*See the report of the Committee on the Investigation of Communist Propaganda, House Report No. 2290, 1931, p. 35. A copy of this report is filed in TRQ 60.) This unit consisted at that time of only two experts, whose efforts to solve the system met with no success. The Code and Signal Section had made some slight progress and had collected some information from a former member of the Amtorg Staff (see below). At this point Representative Fish requested Lieutenant Colonel O. S. Albright, MID, to forward the text of the messages to the Signal Intelligence Section for study. The story of what happened next is best told in the words of a memorandum to Colonel Albright from Major D. M. Crawford, 24 February 1931 (TRQ 35):

> "In November, 1930, the officer-in-charge of the Code and Signal Section, Navy Department, furnished this office with a complete file of these messages with an informal request that they be studied with a view to assisting in their solution. This request was approved and Mr. Friedman, Chief of the Signal Intelligence Section, was directed to devote as much time as possible to the project. He himself devoted about a month's time to the study, and four student assistants, together with two clerks, devoted approximately six weeks full time to this study. Throughout the investigation there was a constant exchange of findings and conclusions between the Code and Signal Section and the Signal Intelligence Section, so that there was close cooperation and little

or no duplication of effort. Although certain interesting and important data were obtained, results were nil so far as concerns actual solutions to any of the messages. It may therefore be stated that (sic) since the efforts of two or three experts and a large group of assistants in both the Signal Intelligence Section and the Navy Code and Signal Section, all working for several months have been entirely fruitless, the problem is apparently one of extreme difficulty because of the complexity of method and the absence of definite information relative to the basic system employed in cryptographing messages. It is also probable that even were the latter information available, considerable difficulty might still be experienced in reading the messages because, judging by what is known of Russian cryptographic methods in general, the correspondents in this case are employing complicated, scientifically constructed systems designed to resist the organized efforts of expert cryptanalysts. It is my belief that half-way measures and sporadic attempts will get nowhere in this case; nothing short of a deep, long continued, and painstaking analysis has any chance of leading to a successful solution.

"It was therefore proposed by Major Crawford that Representative Fish be asked whether it could assign sufficient funds to enable the Signal Intelligence Section to employ Mr. Herbert O. Yardley to study this traffic.....

"Yardley was obviously uninterested in such a proposal - he was about to publish the articles in the Saturday Evening Post which were to precede the fuller account in The American Black Chamber.

"To return to the actual problem - the messages were transmitted in ten-letter groups, which were normal until about 1933. It had been discovered by the Naval experts that these letters were a conversion (digraphs for dinomes) of the basic digit groups used in this system. The conversion table had been solved and it was possible to transform the conversion in reverse, but no further success was achieved. Traffic for each month was segregated and labelled with a different letter. Frequency studies were made for each group but produced nothing. The reason for this failure, as was afterwards learned from another source, was the fact that the Russians were using a one-time pad for their encipherment.

.....

"In connection with the Amtorg traffic, there remains only to give a digest of some information obtained by the Director of Naval Communications from a man named Delgass, formerly a member of the Amtorg staff. His testimony is reported in a memorandum dated 27 September 1930 (TRQ 35) and may be summarized as follows:

"Delgass was a chemical engineer and was concerned, while with Amtorg, primarily with chemicals and explosives. He professed to know little about the Amtorg systems but apparently was willing to tell what he knew. Secret messages were sent only in Russian. An 'ordinary code' was used for confidential communications, the 'War Code' for those requiring a high degree of secrecy. Both code books were small, containing from 30 to 50 pages with about 20 groups to the page. Apparently proper names were spelled out in some form different from the code. The resultant cipher text was then converted to digits and the digits altered by some process. Finally, the digits were once more converted to letters. None of these processes were known to Delgass.

"The codes were prepared in Moscow by two experts, and changed at frequent intervals (every month or two). The obsolete code books were then returned to Russia and reissued to other stations. An Amtorg book had previously been used at Teheran. When ARCOS in London was raided in 1927* (ARCOS, Ltd., was a trading company financed by Russian capital.... .....), all cipher messages were stopped for several weeks until new systems could be distributed. The process of encoding and decoding is very slow, requiring about two hours to encode a message of 100 letters. 'It has taken two men as long as two days to decode a message.' The code clerks were four in number, named Tretiakoff, Shulega, Rykoff, and one, recently arrived from Russia, whose name was unknown to Delgass. They worked a twelve-hour day (9:00 A.M. to 9:00 P.M.), sometimes all night. About ten messages were sent on an average day.

.....

"The same memorandum goes on to summarize what the Code and Signal Section of the Navy had already concluded by analysis:

"a. The system used digits, the letters which appear in the intercepts being a conversion of the digits. The conversion table had been solved.

"b. The encipherment was changed about every two months.

"c. The system was complicated and of very high security.

"d. The system for the New York-Paris and New York-Berlin circuits differed from that of the New York-Moscow circuit, except that 'information copies' (circulars?) were sent to Moscow in the same system as to Berlin and Paris.

"e. A different key was used for each message.

"f. Enciphered code was suspected but not certain.

.....the systems remained unsolved."

Signal Intelligence Service before

~~TOP SECRET~~

HEADQUARTERS
ARMY SECURITY AGENCY
WASHINGTON 25, D. C.

TOP SECRET

WDGSS-90

12 March 1946

File T
3.

SUBJECT: History of BOURBON Problem

TO: Colonel M. A. Solomon
2E-777 The Pentagon
Washington 25, D. C.

1. The following is submitted with respect to your telephone conversation 11 March 1946 regarding the origin and history of the BOURBON problem.

2. For reasons not known to personnel now at ASA, the BOURBON problem was first begun late in 1942 (employing two persons), was for some reason abandoned soon after, and was again started early in the spring of 1943. The unit grew to number twenty-five persons by 1 January 1944, an increase necessitated by the tremendous volume of traffic passed by the country in question. The first solution entry was gained late in 1943 in diplomatic traffic, and the exploitation of this break-in, combined with the increase in traffic, brought the number of personnel employed in the project to about seventy-five by V-J Day. Solution of two military systems (now obsolete) had been accomplished in the winter 1944-45, but otherwise little had been done with operational traffic before 15 August 1945. This was true also of (radio teletype) traffic, which began to come in only in the spring 1945. After victory over Japan when personnel became available and positions in the monitoring stations became idle, it was possible at last to study military-operational traffic and to develop the teletype activity; the availability of personnel also affected favorably the diplomatic studies, in which a large amount of hand work is essential because of the nature of the systems. Finally, collaboration with the British, becoming effective on the technical level in August 1945, gave a much extended picture of the BOURBON traffic of every sort, since their intercept covers an area hitherto unattained by U. S. sources.

James B. Greene
JAMES B. GREENE
Lt. Colonel, Signal Corps
Acting Chief,
Intelligence Division

~~TOP SECRET~~

Tab I

From: Tokyo (TOGO)
To: Moscow
12 July 1945
JAA-2-JAJ

893

Very urgent.

Reference my #890[b] and others.

I have not yet received a wire about your interview with MOLOTOV. Accordingly, though it may smack a little of attacking without sufficient reconnaissance, it has seemed to me that it would be appropriate to go a step further on this occasion and to inform the Russians before the opening of the Three-Power Conference of the Imperial will concerning the ending of the war. I should like you, therefore, to present this to MOLOTOV in the following terms:

'His Majesty the Emperor, mindful of the fact that the present war daily brings greater evil and sacrifice upon the peoples of all the belligerent powers, desires from his heart that it may be quickly terminated. But so long as England and the United States insist upon unconditional surrender in the Greater East Asia War, the Japanese Empire has no alternative but to fight on with all its strength for the honor and the existence of the motherland. His Majesty is deeply reluctant to have any further blood lost among the people on both sides. For this reason, it is his desire, for the welfare of humanity, to restore peace with all possible speed.'

The Emperor's will, as expressed above, arises not only from his benevolence towards his own subjects but from his concern for the welfare of humanity, in general. It is his private intention to send Prince KONOE FUMIMARO to your place as a special envoy and have him take with him a letter from the Emperor containing the statements given above. Please inform MOLOTOV of this and get the consent of the Russians to having the party enter the country. (I shall telegraph the names of the members of the party later.) Now, though it would be impossible to have this delegation get to your place before the big men in Moscow leave for the Three-Power Conference, we must arrange for a meeting immediately after their return, so I should like to have the trip made by plane, if possible. Please try to arrange for a Soviet plane to go as far as Manchouli or Ch'i - Ch'i - Ha - Erh.

Paragraph dealing with the collaboration with the U.K. as copied from "The Narrative History of AFSA/NSA - Part I."

On 12 June 1945 ANCIB proposed to the British that they extend their collaboration to efforts, then under way on both sides of the Atlantic, to read Russian communications. Agreement took the form of an understanding between the ANCIB Chairman (RADM H. Thebaud) and an LSIB representative in Washington (Group Captain Eric Jones).

During the war, the U.S. Army and the U.S. Navy had made separate agreements with the British COMINT authorities, and had used separate liaison channels. With respect to Russian COMINT, they cooperated closely at home and, near the war's end, agreed to create a single American liaison channel with the British. A plan proposed in July 1945 by ANCICC and accepted by the British provided that

Aside from these liaison arrangements, [redacted] sent representatives to the other to gain experience [redacted] center BOURBON processing. The BOURBON project became operational early in August 1945, and continued functioning until it was merged in a much broader Anglo-American collaboration under the BRUSA Agreement of 5 March 1946. Preparation of semi-monthly reports on the status of liaison and of technical progress in BOURBON decryption was begun on 15 August.

(b)(1)
(b)(3)-50 USC 403
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

Tab D