~~SECRET~~

A. Important Contributions to Communications Security, 1939-1945.

1. Converter M-134 A--On 25 July 1933 a secret patent application (Serial No. 682,096) was filed by the Chief Signal Officer, on my behalf, covering Converter M-134-T2, the predecessor of Converter M-134 C (Sigaba). The principle disclosed in Serial No 682,096 is of highest importance in that it was the first invention and disclosure covering Electrical control (as distinguished from mechanical control) of a set of cipher rotors in cascade, permitting a departure from the regular and periodic or metric angular displacements of such cipher rotors. The following is quoted from a Secret Navy report* on the history of the development of the Sigaba (ECM):

> "However, under date of 25 July 1933, The Chief Signal Officer filed on behalf of Friedman a patent application (Serial No. 682,096) covering a cryptographic system and machine in which the stepping of the code wheels was very irregular and under the control of a keying tape. Electric Control thus made its first appearance!"

A complete assignment of all rights to my invention was made to the Secretary of War on 10 September 1936, and the patent application was placed in the secret category on 9 September 1936, where it still remains.

Two service test models of Converter M-134-T2 were constructed by the Signal Corps Laboratories at Fort Monmouth, New Jersey in 1936 and service tests were conducted by an exchange of cryptograms between the War Department, Washington, and The Panama Canal Department, Balboa, C.Z., in November 1936. It demonstrated that the machine was operable at the rate of 30-35 words per minute and afforded the highest degree of security yet attained by any cryptographic machine for cryptonet communication (multiple holders of the same cryptographic key).

On 19 February 1937 the military characteristics of Converter M-134 were approved, soon thereafter a contract for the construction of 12 machines was placed with Wallace and Tiernan, Indiana, of Belleville, New Jersey. The machines were delivered to Washington on 2 August 1938.

I developed and wrote the cryptographic keying instructions and in October 1938 first shipment was made of the machines, two each, for the Headquarters of the Ninth Corps Area (San Francisco), Panama Canal, Hawaiian, and Philippine Departments. Four machines were kept in Washington. The machines were promptly put into service for all the highly secret communications between the War Department and the headquarters indicated. Later, as more machines became available, a further distribution was made to equip all Corps Areas and Departments, including the Puerto Rican, with a sufficient number of machines to meet

* See Enclosure labelled "Exhibit 4"

requirements. Eight machines were placed in the War Department Code Center. Only 75 of these machines were built in all but they formed the backbone of the quipment for high command secret and confidential communications of the War Department and the Army from the date of their introduction into service until the end of 1941, when they were replaced by Converter M-134-C, the Sigaba. In 1940 the War Department sent by special officer courier two of these machines to the U. S. Military Attache in London, to meet the very urgent needs for high speed, high-security communication between Washington and London. Later two more were sent there, making four for the Military Attache.

On 29 November 1941 the War Department provided the Department of State with four machines, two for Washington and two for the American Embassy in London; later on, four or more additional machines were provided the Department of State. During the vital years 1940-1942, confidential and secret intercommunication between these two points and among the offices indicated could not have been successfully conducted without these machines.

In January 1942 arrangements were made to use the M-134-A for direct communication between the President and the British Prime Minister and it was used for this purpose for a number of months. Later this machine in that circuit was replaced by Converter M-134 C, in a special adapter made under my supervision by the Signal Corps and the Western Union. This permitted of high speed, secure communication between the White House and Downing Street at a very critical period.

The M-134 was also used to a large degree by the Signal Intelligence Service itself for forwarding intercept traffic to Washington from overseas intercept stations. It replaced Cipher Device M-138 for this purpose and thus greatly facilitated the prompt receipt of the raw traffic for cryptanalysis.

Later on, a number of them (totaling 29 or 30 at the end) as they became available, were provided the Office of the Coordinator of Information (later the Office of Strategic Services) for secret communication between Washington, London and other capitals where the OSS maintained headquarters. Some of these machines (about 16) maybe and probably are still in service.

During the years from 1939 to 1942, when Converterm M-134 was replaced by Converter M-134-C (Sigaba) it is doubtful if the voluminous secret and confidential traffic of the highest echelons of the Army and the War Department could have been handled as successfully as it was, had it not been for the invention, development and availability of this machine.

There is not a scrap of evidence in Ticom reports that either the Germans or the Japanese or any other government was able to solve any of the traffic enciphered by this machine.

~~SECRET~~

2. Converter M-134-C (Sigaba).—In the course of studies of Converter M-134-T2 and before manufacture of the latter machine was well under way, my principal assistant, Mr. Frank B. Rowlett, and I investigated various means of improving the cryptographic machine with a view to eliminating the perforated tape which controlled the aperiodic stepping of the rotors. Various schemes were studied, including cam wheels with different diameters and variable "off" and "on" pin arrangements. About 15 June 1935 Rowlett conceived an idea which finally resulted in making it possible to eliminate the tape control. Basically his invention was that of using a set of rotors as a key generator, that is, using the rotors to generate a long keying sequence by sending electrical impulses through a set of rotors which themselves were caused to step in a regular manner. The successive elements of the keying sequence, as they were generated could control the stepping of the rotors actually employed to encipher the letters of the message to be enciphered. Rowlett and I then jointly developed the idea by setting down on paper various methods by which it could be applied to replace the tape control employed in Converter M-134-T2, and although no models were built the results of our theoretical studies were incorporated in a patent application filed on 23 March 1936 (Serial No. 70,412) in our name as joint inventors. A complete assignment of the invention to the Secretary of War was made on 2 April 1936 and the patent application was placed in the secret category, where it still remains.

The Navy was then trying to improve its own machine (Mark I E C M), the security of which was unsatisfactory. Though this machine generated a long keying sequence the number of available starting points in that sequence was so limited that considerable "depth", that is, messages enciphered in exactly the same key, could be expected every day and thus solution potentially made relatively easy. On three occasions, at Navy request, the drawings and principles later embodied in Serial No. 70,412 were shown and explained to Navy representatives several times in October and November of 1935, with the result that the Navy initiated a development contract with the Teletype Corporation and work thereon was started in January 1938. This was done, however, without advising us or anybody else in the Signal Corps until March 1939, when the Teletype Corporation engineers brought to Washington the first completed set of drawings of the Mark II E C M. Rowlett and I were invited to the conference with the Teletype engineers and in the course of the discussions it was brought out and acknowledged that the Navy had based the cryptographic features of the new machine upon the Army's disclosure. A first model was then built and delivered on 3 February 1940, when Major General Mauborgne, then Chief Signal Officer, Rowlett, and I were invited by Admiral Noyes and Captain Safford to see the model. On that occasion Captain Safford acknowledged, in the presence of all those witnessing the demonstration, the fact that the Navy had used the Friedman-Rowlett invention. Further development of the machine was thereafter on a joint Army-Navy basis, and on 19 June 1940 the Signal Corps added its order of an initial 85 machines to the Navy order, at a cost of $1856.90 each.

~~SECRET~~

The Mark II ECM (Navy nomenclature)--Converter M-134-C was adopted by the Army to replace Converter M-134 A, not because the former might afford greater security than the latter but because the M-134 C was not only a much more rugged, reliable and rapid machine but also because it dispensed with perforated tapes, thus being more practical than the M-134 C. The following is quoted from the Navy Department's "History of the ECM:"

> "Electric control of the ECM by means of the Friedman-Rowlett 'Stepping Maze' is the essential feature that places the Mark II ECM in a class by itself as regards security."

On 17 March 1941 the first 10 machines were delivered to the Signal Corps and were given a prompt service test, which proved the machines to be highly satisfactory. On 4 October 1940 action was initiated by the Signal Corps to procure an additional 149 machines, and thereafter, in successive contracts several thousand more of them were procured, the production schedule in July 1942 calling for the delivery of the machines to the Signal Corps at the rate of 150 per month. By 31 August 1942 a total of 373 Sigabas had been delivered and 364 were already in service; by 30 April 1943 the total number ordered was 1867, the number delivered was 862, and the number in use 807; by 28 March 1944 a total of 333 machines had been ordered, 1827 delivered, and 1681 were in service. In all, the Signal Corps actually procured a total of 3392 of these machines for Army use, and the Navy procured more than that number for Navy use. In the Army the machines were distributed to all commands down to and including headquarters of Divisions. They were also used in all the important fixed headquarters in the Communications Zone, in all theaters and in the U. S. Under special precautions they were used in U. S. installations in foreign countries where we had no troops, as for example, in Moscow, for our special military mission. Whenever and wherever the late President went during the war, the Sigaba went too. They were installed in the late President's signal center whenever he visited his home at Hyde Park; they were on board the Presidential Train, etc.

The fact that identical machines were employed by the Army and the Navy at all high and intermediate headquarters not only speeded up the exchange of classified messages of all categories (secret, confidential, and restricted) within each of the Services but also facilitated Joint Communications. The following is also quoted from the Navy's History of the ECM:

> "This use of an identical machine with interchangeable code wheels has been of great military value, particularly in the early stages of the war, when distribution of machines and code wheels was incomplete. In the Philippines, Java, Australia, and even in North Africa, Navy wheels have been used in Army ECM's, Army Wheels in Navy ECM's; machines have been borrowed back and forth between the two services; Army messages have been sent in Navy ECM ciphers and Navy messages sent in Army ECM ciphers."

We know now from Ticom reports that neither the Japanese nor the Germans had the slightest success in their efforts to solve messages in the Sigaba, though the Germans certainly tried hard enough. The absolute security of Army and Navy high command and high echelon communications throughout the war was made possible by the Sigaba. In view of the fact that the high-level communications of the German, Italian, and Japanese Governments and Armed Forces were successfully attacked by the U. S. and the British communications intelligence staffs, and that the intelligence resulting therefrom was of highest diplomatic, strategic, and tactical importance, whereas our own high-level communications were inviolate, it may be said that the Sigaba contributed materially to the successful outcome of the war.

3. Converter M-228 (Sigcum, Sighuad).--The need for a cryptographic mechanism to protect land-lines teletype communications was felt even in World War I. In 1936 the Army was anxious to have something practical developed for this purpose and studies that had been underway for a number of years culminated in 1939, when Rowlett and I, applying Rowlett's idea of using cascade rotors as a key generator, then jointly conceived the principles underlying what later became Converter M-228 (Sigcum). Patent Application Serial No. 443,320 was filed on 16 May 1942; assignment of rights to the Secretary of War was signed on 13 May 1942 and the application was placed in the Secret category, where it still remains.

On 16 July 1941 military characteristics were approved by The Adjutant General and the Signal Corps Laboratories at Fort Monmouth, New Jersey, undertook the development. On 12 March 1942 a satisfactory service test and working demonstration of the first two models of Converter M-228 was made; one machine was at Fort Monmouth, the other at the Bell Laboratories, New York City. The provided for automatic on-line keyboard encipherment, transmission, reception, decipherment and printing of messages at the rate of over 360 characters (= approximately 60 words) per minute, with good security.

On 7 April 1942 the budget for FY 1943 included provision for procurement of 2400 machines at $500 each, a total of $1,200,000.

On 18 June 1942 representatives of the Signal Corps and the Navy witnessed a demonstration of the machine in New York and as a result the Navy decided to procure 200 for its use.

On 24 November 1942 action was initiated to purchase 1467 machines and on 25 December the first 10 machines were shipped from the factory to Washington.

Although Converter M-228 was not intended for radio-teletype usage, the urgent need for speed in overseas communications and the availability of radio-teletype circuits practically forced the use of the machine on these circuits to protect these communications. On 9 January 1943 the first official message using Converter M-228 on a radio circuit was sent from Washington to Algiers, and thereafter extensive use of the machines for radio-teletype communications was made, although it was decided, for security reasons, to transmit only confidential and restricted messages by this means. (Secret and Top Secret Messages had to be enciphered by Sigaba or by Sigtot, the one-time tape System).

By 11 September 1943 a total of 3867 machines had been ordered, and 3044 had been manufactured. The rate of production was 500 per month. By that date the "stop-gap" teletype-encipherment system using two short loops of key tape was discontinued, because general distribution of the M-228 had been completed. On 31 May 1943 the A. C. of S., G-2, War Department, approved the installation of this machine for use on the Defense Teletypewriter Network linking the several U. S. Army Headquarters in the United Kingdom.

In April 1944 the War Department approved a policy under which the machine could be turned over to the British for the specific purpose of use in Combined Operations; and on 23 May 1944 the A. C. of S., G-2, War Department, approved disclosure of the principles of the machine to the British.

By 5 June 1944 a total of 3200 of these machines had been built and 1488 issued for use, including 200 to the Navy. The machine was employed to encipher a tremendous volume of traffic, including raw material for cryptanalysis from all intercept stations. Under the special conditions and with some modification (Sighuad) the machine was also used in special circuits in Washington, between Arlington Hall Station, the Military Intelligence Service in The Pentagon, of the highest classification. This same modification (Sighuad) permitted the machine to be used by the Air Forces in the U. S. and in the Pacific, to transmit, by radio meteorological and weather data, thus greatly facilitating operations.

The British did not have any machine similar to the Sigcum or Sighuad and only at the end of the war was their long-standing desire to be able to use it granted. The Germans had teletype encipherment equipment but a large volume of traffic in the various types of machines they built was solved and read on a current basis by the British. Toward the end of the war the Germans had improved models which resisted solution, but they came too late. The Japanese had no such equipment at all.

Results of Ticom operations have established that neither the Germans nor the Japanese were successful in their efforts to solve our Sigcum traffic, despite its great volume, and it is my belief that had we used this machine for secret radio-teletype communications no serious harm to our security would have followed. Although it was not used for secret radio-teletype communications, the machine was nevertheless widely used for secret, confidential, and restricted communications by land-line teletype and for a great volume of confidential and restricted communications by radio-teletype in the U. S. as well as in all overseas theaters. The Sighuad version of this machine was, however, used to a limited extent for secret traffic by radio. Had we not possessed such a machine our rapid communications would have been severly handicapped by the necessity of encipherment by slower means.

4. Cipher Device Type M-138.---Early experiments with the old cylindrical Cipher Device M-94, which had been introduced into the U. S. Army and U. S. Navy in about 1922, began in about 1933. Various modifications, in the form of a flat cipher device using variable, instead of fixed alphabets, were made, culminating in a device on which a patent application in my name was filed (Serial No. 300,212) on 19 October 1939. On 16 July 1940 the application, which the usual license rights were assigned to the Government on 16 October 1939, was placed in the secret category under the provisions of the Act of 6 October 1917 as amended 2 July 1940.

About five thousands of these devices were manifactured under War Department Contracts. They were used throughout the war and are still used by a large number of military fixed and mobile headquarters. In fact, until the manufacture of the automatic cipher machine (Sigaba) had progressed to the point where a sufficient number had been produced to meet distribution requirements, the Strip Cipher System using Cipher Device M-138 formed the backbone of Army Secret and Confidential communications; thereafter it served and still serves as the secondary or back-up system for the holders of the Sigaba. For stations not equipped with the Segaba the Strip Cipher System still constitutes the principal means for such communications. At the present in the U. S. all Posts, Camps and Stations use this device as the primary cryptographic means. Until recently it was also the primary means for communication between the War Department and all Military Attaches as well as for intercommunication among military attaches; at present it is employed only for circular messages to or among military attaches.

The same device was also provided by the War Department in large quantitites for use by the Department of State, for Secret and Confidential Communications between that Department and its Embassies, Legations, and Consulates, as well as for intercommunication among those offices.

Certain Allied Services, such as the British, Italian, and Russian were also provided with these devices in small quantities both by the War and the Navy Departments. The U.S. Navy also adopted the device at first in practically identical form; the Navy produced some minor improvements later on and employed and is still employing the device very extensively in its own communications. In addition the Strip Cipher System was used during the war as a Joint Army-Navy system and as a Combined System. The fact that the same device was used by both the Army and the Navy greatly facilitated Joint Communications. The production of the paper strips bearing the variable cipher alphabets employed in the device presented numerous problems which were successfully solved by me or by people under my direction. I conceived the first rotary cutter for cutting the strips apart and had the first cutter built at the Government Printing Office. This machine greatly facilitated the production of the strips and made the matter practical.

5. General.—Throughout the years mentioned, in my capacity as Head Cryptanalyst and later as the Director of Communications Research, many problems directly related to our communications security were brought to my attention and I believe that my long experience in the field formed a solid foundation for mature, sound judgment in arriving at proper, practical, and satisfactory answers to those problems.

Before our Converter M-228 was ready for distribution the urgent need for a means of enciphering teletype communications for the Military Intelligence network in the United States led to my suggesting the adoption of a temporary expedient for this purpose. This took the form of double-loop, key-tape encipherment system which had been tried out in a small way at the end of World War I. Having studied this method in 1919-1921 and knowing the pitfalls to which such a system is subject from the security point of view, I was able to suggest ways of usage to minimize the dangers inherent in a double-tape encipherment method. The system was used for a number of months not only within the U. S. but also within theaters of operations, thus meeting an urgent need for teletype encipherment until the M-228 was ready for distribution.

Later on, when the one-time tape or Sigtot System was being considered for secret and top secret radio-teletype communications, I was consulted and in view of my experience with all preceding teletype encipherment systems was able to give technical approval on the new proposal and to insure that the production of keying tapes was properly safeguarded.

For a number of years prior to 1941 I had been more or less intensively studying all the various cryptographic devices and machines which had been invented and produced by private inventors both in the United States and in foreign countries. Files of patents issued domestically and abroad were kept, and theoretical studies made to ascertain the security of the products of invention in this field.

[redacted] This resulted in improvements in the security of the machine and led finally to the adoption of Converter M-209 as a field instrument. Over 100,000 of them were manufactured, and used by both the Army and the Navy. While the machine was by no means perfect, it met a need that could hardly have been fulfilled otherwise.

For a number of years I served on the Joint and the Combined Codes and Ciphers Committee and the Joint and Combined Security Committee. I was a member of a special Ad Hoc Committee, consisting of two Navy officers, General (then Colonel) Corderman, and myself, appointed by the Joint Communications Board in 1944 to investigate the security of communications in all non-military bureaus and departments of the Government, making recommendations for improvement therein. The deliberations of the Ad Hoc Committee resulted in the establishment, by President Truman, of the Cryptographic Security Board for U. S. Government communications, consisting of the Secretaries of the three Departments, State, War, and Navy.

As technical adviser to the Chief, Signal Security Agency and to the Chief of the Security Division, I was constantly consulted by them in connection with the many problems affecting communications security. I also served in an advisory capacity in connection with all research and development of communications security equipment, including ciphony and cifax. One of my important contributions in this capacity was to urge the development of the voice security equipment, now known as the Sigsaly system, at a time when that project had been practically abandoned.

The new Synchronous Polarity Reversal System of Cifax recently developed by us is based upon an invention of mine (Serial No. 478,193) filed on 3 June 1943 and assigned to the Secretary of War on 18 October 1943. Lieutenant Colonel Rosen's invention of the important feature whereby the polarity reversals in the interaction of keying and picture elements are synchronized made the system practical and highly secure; in fact, there is reason to believe that the security of cifax transmissions by the Friedman-Rosen inventions can be made almost absolute.

In 1941 I undertook a study of the general basis of the distribution of Army cryptographic systems, evolving the new idea of "cryptonets", and thus improving security of communications. By isolating cryptographic systems according to levels of command and reducing the amount of intra-net traffic within any one system, the security of all systems is enhanced at the same time that provision is made for inter-net traffic. The cryptonet system has worked in a highly satisfactory manner in practice.

B. Important Contributions to Communications Intelligence, 1939-1945

1. Solution of Japanese Diplomatic Communications.--On 20 February 1939 the Japanese Foreign Office began using a new machine called by them the "B-Machine" for the highly secret communications between Tokyo and its embassies throughout the world. We had been successfully solving and reading practically all of the communications of the Japanese Foreign Office up to that time; many of them were in a machine ("A Machine") which we had also solved and reconstructed by pure analysis in about the year 1937, but a large number were also in hand operated systems involving a small code, superenciphered by various schemes, usually transposition.

The urgency of solution of the new machine, in view of the increasingly difficult relations between the United States and Japan, was apparent. However, in view of the small number of trained cryptanalysts available, the pressure of work in the sections operating on currently readable systems and in the sections producing our own codes, ciphers, and key lists, the number of people who could be placed on this new and very difficult problem was very limited. By August 1939, no important progress having been made, the Chief Signal Officer directed that I drop, so far as practicable, certain administrative duties as assistant chief of Signal Intelligence Service (Major W. O. Reeder had been brought in as officer in charge in April 1938) and to participate actively in the studies of the "B Machine," in addition to generally supervising the technical cryptanalytic and cryptographic work of the office. Thus, from that month until success was attained, the "B-Machine" studies were under my active supervision but at the same time I had to carry on some other duties from which, it was impracticable to relieve me.

By the end of 1939, the machine having been in use almost a full year, hundreds of messages had accumulated; very occasionally a tiny fragment of a message was read; rarely, longer fragments. But no message was read in its entirety. Nevertheless important progress had been made. Intensive work was continued by me and my technical staff

of half a dozen cryptanalysts, with the clerical assistance of another half dozen people, and the occasional assistance of our two Japanese translators. On 20 September 1940 came the very first indication that we were on the right path and might be successful in solving the machine; under the pressure of great excitement, working almost day and night, by 27 September the first two translations representing the very first actual solution to the B-Machine were sent to G-2.

There remained, however, much work to be done, since only the data applicable to but one out of the whole set of 120 indicators were at hand. By 14 October 1940 solutions for over one-third of the 120 indicators were available and certain current messages could be read.

By careful analytical reasoning, by studying the external cryptographic phenomena manifested by the system, by correct reasoning and a knowledge of cryptographic mechanisms, the principles underlying the cryptographic functioning of the B-Machine were soon derived by induction and deduction. A hand-operated, crude model using flash-light bulbs was hurriedly constructed, while at the same time parts were ordered for two fully automatic, keyboard-operated machines, which were then constructed as rapidly as possible. All of this work also was under my general direction as Principal Cryptanalyst. By November 1940 the two fully automatic machines had been constructed and were in successful operation. We had, it is true, reconstructed the Japanese "A-machine" by pure analysis, too, but so far as I am aware, this is the first time in cryptanalytic history that a machine capable of deciphering traffic of the complexity of that produced by the Japanese B-Machine was completely reconstructed by pure analysis. When we began the study we had no inkling as to the nature of the machine; soon thereafter we had ascertained that the cryptographic textual letters fell into two classes, but to this day we have never seen a complete Japanese machine in working order. Some time in 1942, long after our work of analysis had been completed, we did see the smashed, burned and almost unrecognizable remains of a B-Machine which the Japanese had destroyed on or about 5 December 1941 in Mexico and which remains came into possession of the F. B. I., who were anxious to reconstruct the machine if possible; also, and as a result of European Ticom operations, we did find two or three of the rotary-switch assemblies in a box taken from the ruins of the Japanese Embassy in Berlin, but of course these glimpses of one of the most important elements of the machine were by this time only of academic interest.

In January 1941 a Joint Army-Navy Cryptanalytic Mission to GC and CS took with it one machine and a complete story of how to decipher diplomatic messages enciphered by the Japanese B-Machine. This system was one of the very few which had resisted all of GC and CS efforts to solve it.

As to the importance of the solution of the B-Machine, or Purple System, as it was designated soon after solution, I need only refer to the disclosures of the current Joint Congressional Investigation of the attack on Pearl Harbor and to certain statements relative to the solution of the Japanese diplomatic machine contained in the letter dated 27 September 1944, which the Chief of Staff sent to Mr. Dewey, a copy of which is attached hereto. While that solution represents the achievement of a cooperative effort by a number of people, it was made possible by good coordination and proper technical direction of a fair number of skilled cryptanalytic personnel who were selected and trained by me and who worked under my direction for over 18 months as a harmonious team. In addition, certain of the cryptographic phenomena which ultimately led to the solution were uncovered by me in the course of those studies. A more detailed history of the solution is attached hereto.

We know that the German cryptanalytic staffs tried to solve the B-Machine and failed; as noted above, even as competent as was the British staff, it also failed to solve this machine and we gave them the solution. There is reason to believe that the Russian staff did not succeed, if they even undertook the problem, which we do not know. I belive it is true that as a result of our reading certain messages early in 1941 the State Department was able to give the Russian Government early information as to the coming secret offensive by the Germans, which began on 21 June 1941. Had the Russians been able to read the Purple, this would not have been necessary. As to the Japanese diplomatic communications in other systems, their messages in those systems were being read as promptly as facilities and personnel permitted, with priority being given those in the Purple System, although many important messages were also read in the various other systems, such as PA-K2, CA, and LA.

2. General.--As Head Cryptanalyst in the years 1939-1941, I was in technical charge of a staff of people numbering several thousand, working on all problems in the communications intelligence field, and also supervised the selection and training of new personnel. Some of the problems being worked on during those years and successful in their outcome were those involving the diplomatic communications of several other governments than the Japanese such as the Italian, German, and Mexican. During the succeeding years, 1941-1945, the Agency accomplished many feats in cryptanalysis, too numerous to mention.

The diplomatic communications of many countries were read, some almost in toto; the communications of the Japanese Army and Air Force were read to a very large degree, contributing greatly to our victory in the Pacific.

The extent to which the Agency engaged in the research, development, and use of high speed analytic equipments to facilitate the application of cryptanalytic techniques and processing is worthy of mention and my technical advice and collaboration was used in all these cases. I was largely responsible for urging the development of the "oo3" equipment and had general supervision over its design, construction, and installation by the Bell Telephone Laboratories and the Western Electric Company. The fruits of that equipment and the modifications which followed and which were applied to the solution of German Enigma traffic represent some of the best achievements of the Agency. Our important developments in the field of photo-electric rapid analytical machinery also resulted from my insistence upon embarking upon such developments. In all these matters my advice was sought and obtained by the Chief of the Agency and special reports were prepared for him from time to time on these subjects. These equipments aided considerably in the solution of the diplomatic and military communications which were worked on by the Agency.