CONTRIBUTIONS IN THE FIELDS OF

COMMUNICATIONS SECURITY AND COMMUNICATIONS INTELLIGENCE

1. As Principal Cryptanalyst (1939-1940), Head Cryptanalyst (1941), then Director of Communications Research (1942 to date) I have had technical and staff supervision over a large staff (in 1945 amounting to almost 10,000 people) of cryptographic and cryptanalytic personnel working on many complicated problems in communications security and communications intelligence before and during World War II. My specific contributions in these two fields are briefly summarized below.

2. My contributions in the Communications Security field during the years 1939-1945 include practically all the systems and devices employed during World War II for cryptographic purposes by the Army and the majority of the systems and devices employed for the same purpose by the Navy and the Department of State. A detailed statement is attached covering the following:

a. Converter M-134 and M-134 A, covered by patent application (Serial No. 682,096) filed by the Chief Signal Officer in my name as inventor on 25 July 1933. This machine was the predecessor of the Converter M-134 C (Sigaba) and represented the first invention of electrical control, as distinguished from mechanical control of a set of cipher rotors in cascade, thus getting away from the regular or metric stepping of the rotors. During the important years 1939-1941 this machine was used for enciphering the bulk of the highly secret and confidential administrative traffic of the War Department in communications with the Headquarters of Overseas Departments, Corps Areas, Defense Commands, and headquarters of GHQ Air Force and 2d Air Force. In addition, it was extensively used by the Signal Intelligence Service in forwarding traffic from our intercept stations in Honolulu and Manila. It was also used during 1940 and 1941 for communications between the War Department and the U. S. Military Attache in London. In 1941 the War Department provided a number of these machines for the Department of State, for use in secret and confidential communications between the Secretary of State and the American Ambassador in London and these were used from 1941 to 1944 for that purpose. It was also used in a special circuit for a number of months in 1942 for direct communication between the President and the Prime Minister in London. After these machines were taken out of War Department service a number of them (29 or 30) were provided the Office of the Coordinator of Information (later OSS) for secret communications between Washington, London, and other capitals where the OSS maintained headquarters. Some of these machines are probably still in service.

b. Converter M-134 C, covered by patent application (Serial No. 70,412) filed on 23 March 1936 by the Chief Signal Officer in the name of Friedman and Rowlett as joint inventors, arose as a result of studies having the aim of improving Converter M-134 A. About 15 June 1935, Rowlett conceived the idea of using a set of rotors in the M-134 A. Rowlett and I then jointly developed the idea by setting down on paper various methods by which it could be applied in practice to the M-134 A. All of these methods were disclosed to the Navy, then engaged in attempts to improve their own unsatisfactory Mark I ECM. The Navy took one of these methods and incorporated it in the design of their Mark II ECM, work on which was begun in January 1938 by Navy contract with the Teletype Corporation. This was done, however, without advising us or anybody else in the Signal Corps until March 1939, when the Teletype engineers brought to Washington the first completed set of drawings of the Mark II ECM, at which time Rowlett and I were invited to the conference with the engineers. A first model was built and delivered on 3 February 1940. Further development was on a completely joint Army-Navy basis and on 19 June 1940 the Signal Corps added its order of an initial 85 machines to the Navy order. On 17 March 1941 the first 10 machines were delivered to the Signal Corps and were given a prompt service test, proving the machines highly satisfactory. In successive contracts the Army procured a total of 3392 machines and almost 2000 were in service by March 1944. The Navy also procured a larger quantity. In the Army the machines were distributed to all commands down to and including HQ of Divisions. They were also used in all important fixed headquarters in the Communications Zone, in all theaters and in the U.S. Whenever and wherever the late President went during the War, the Sigaba went too, on the Presidential Train, at Hyde Park, Yalta, etc. For further information regarding its value in Joint Army-Navy communications, see the detailed notes attached. We know that neither the Germans nor the Japanese were able to solve our Sigaba traffic, though we were able to solve their high echelon traffic, obtaining intelligence of great diplomatic, strategic, and tactical value. In view of the foregoing, the Sigaba contributed materially to our success in the war.

c. Converter M-228 (Sigcum, Sighuad), covered by patent application (Serial No. 443,320) filed on 16 May 1942 by The Chief Signal Officer in the name of Friedman and Rowlett as joint inventors, was a cryptographic machine to protect teletype communications, by providing for automatic off-line or on-line (keyboard) encipherment, transmission, reception, decipherment, and printing of messages (in a single operation) at the rate of over 360 characters per minute, with high security. On 12 March 1942 the first two models, constructed at Fort Monmouth, were given a satisfactory service test. On 18 June 1942 the Navy witnessed a demonstration of the machine and decided to procure 200. By 5 June 1944 a total of 3200 machines had been manufactured and 1488 in service, including 200 by Navy. In May 1943 the machines were used in the United Kingdom to link together all U. S. Army headquarters

in the Defense Teletypewriter Network and these machines were used to encipher a tremendous volume of messages, including raw material for cryptanalysis from all intercept stations. Most of the traffic that was sent by radio teletype was confidential, but on land lines secret teletype messages could be sent by this machine. A modification (Sighuad) permitted use of the machine for transmitting weather data (secret) by the Air Force in two theaters; the same modification permitted use of the machine for secret messages between certain headquarters in Washington. In April 1944 the War Department approved a policy under which the machine could be turned over to the British for use in Combined Communications.

For further information on these machines and additional items relating to contributions in the Communications Security field, see detailed account attached hereto.

d. Cipher Device M-138, covered by patent application (Serial No. 300,212) filed on 19 October 1939. Thousands of these devices were manufactured. For several years this device formed the basis of the Strip Cipher System, which carried a large part of the secret and confidential communications of the Army, the Navy, and the State Department. In the Army it still serves as the back-up system for Converter M-134 C (Sigaba) and as the primary system for Posts, Camps and Stations as well as for circular messages to military attaches. In the Navy and in the State Department it is still used to a considerable degree for secret and confidential traffic.

e. Throughout the years mentioned, in my capacity as Head Cryptanalyst and later as Director of Communications Research, many problems in 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 practical and satisfactory answers thereto. Some of the items that may be mentioned here are the following:

(1) In 1941, as a result of my special study of the manner in which Army and War Department cryptographic communications were then organized, I evolved and developed the idea of the "Cryptonet" system, which has worked in a highly satisfactory manner in practice.

(2) The studies and development of Converter M-209, over 100,000 of which were produced and distributed in the Army and Navy.

(3) The "Stop-gap" or temporary-expedient system of double-loop key-tape encipherment of teletype transmissions.

(4) The "one-time tape" or Sigtot system.

(5) The development of voice security equipment, including the "Sigsaly".

(6) The development of the "Synchronous Polarity Reversal System" of Cifax, which is based upon an important modification (by Lt. Colonel Rosen) of the principles disclosed in my (secret) patent application (Serial No. 478,193) filed on 3 June 1943.

f. I also was a member of the Ad Hoc Committee, consisting of two Navy and two Army members, appointed in 1944 by the Joint Communications Board to look into the matter of communications security in all non-military departments and agencies; the work of this Committee resulted in the establishment by President Truman of the Cryptographic Security Board, consisting of the Secretaries of the State, War and Navy Departments.

3. My principal contribution in the communications intelligence field, directly applicable to our operations in World War II, was in connection with the solution of the Japanese cipher machine (purple system) employed by the Japanese Foreign Office in its highly secret communications with its Embassies and Legations. As Principal Cryptanalyst in the years 1939-1941 I was in charge of the cryptanalytic staff that studied this problem from February 1939, when the first traffic in that machine appeared, until September 1940, when we were able to hand in the first translations. By careful analytical reasoning, long and arduous study of the external cryptographic phenomena exhibited by the messages, by correct reasoning, and a wide knowledge of cryptographic mechanisms we were able to fathom the mystery underlying the functioning of the Japanese machine and to construct, without ever having seen the original itself, machines which would duplicate the functions of the Japanese machine. So far as I am aware, this is the first time in cryptanalytic history that a machine of such cryptographic complexity was completely reconstructed by pure analysis.

As to the importance of that solution I need only refer to the disclosures of the current Joint Congressional Investigation of the Pearl Harbor Attack by the Japanese and to certain statements contained in the Chief of Staff's letter to Mr. Dewey. While the 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. I do not believe that this machine was solved by any other cryptanalytic organization. We know that the very competent British organization failed in its efforts to solve this problem, for we gave them the solution and a machine in January 1941. Nor did the German cryptanalytic staffs who attempted it gain any success.

During the succeeding years, 1941-45, the Agency accomplished many feats in cryptanalysis, too numerous to mention. The diplomatic communications of many countries were read, some almost in toto; the

secret communications of the Japanese Army and Air Force were read to a considerable degree, contributing greatly to our victory in the Pacific. In my capacity as technical adviser to the Chief of the Agency, and having Staff Supervision over all the technical operations of the Agency, I was always consulted by him and acted as advisor to all Chiefs of Divisions and Branches in these operations. 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.

4. From my earliest days of duty in the Office of the Chief Signal Officer I have taken a deep interest in the preparation of texts for use in training military personnel in cryptography and cryptanalysis, and the War Department has published a series of such texts which were written and prepared entirely by me. I regard the writing of this literature, which was extensively used at the various Army Signal or Communications schools, and in the Army Extension Courses, as one of my very important contributions to the war effort. I believe that this material represents an important contribution to the science of cryptology, because for the first time its basic principles and techniques, hitherto scattered in a most chaotic, disorganized manner in foreign literature, were set forth in a scientific, logical, orderly and clear manner; and consistent, adequate and scientific terminology used in this work. Upon them were also based a long series of graded exercises, with approved solutions, also prepared by me, which were used in conjunction with the texts by thousands of enrollees in the Army Extension School, in the various schools throughout the Army during the war, in the special schools in cryptography and cryptanalysis at Fort Monmouth (later at Vint Hill Farms Station), and at Arlington Hall Station itself, to train thousands of new employees. All or most of these texts were also used by the U. S. Navy, the U. S. Coast Guard, the Federal Bureau of Investigation, and the Department of State; copies were also officially furnished the Canadian and British Government.

It was at my suggestion that the War Department, on 11 October 1930, formally established the Signal Intelligence School in Washington, for training Regular Army officers in signal intelligence operations. I served as the Director of that School, in addition to my other duties, organized the 2-year course given, and directly supervised the instruction. The fact that of the nine Army graduates (there were two officers from the U. S. Coast Guard and they also worked in the cryptologic field later) seven came to occupy top-level positions in communications intelligence and communications security work during the war.

In addition to the foregoing, numerous technical papers were written by me in my spare time; these were usually published by the War Department as secret or confidential documents, or they appeared

as articles in the Signal Corps Bulletin (restricted). Two of the most important of these works are entitled "Analysis of a Mechanico-electrical Cryptograph", in which I set forth the basic principles and techniques in the solution of cryptograms produced by electrical rotors in cascade, and "The Index of Coincidence", a revision of an earlier paper under the same title, in which there appears for the first time in cryptologic literature applications of statistical theory and techniques, later to become of great importance.