(U) Cryptologic Almanac 50th Anniversary Series

(U)Madame X: Agnes Meyer Driscoll and U.S. Naval Cryptology, 1919 - 1940

(U) Of all the pioneer American cryptologists that we remember - William and Elizebeth Friedman, Herbert O. Yardley (founder of the American Black Chamber), and Joseph Rochefort, whose codebreaking exploits contributed to the Midway victory - one, Agnes Meyer Driscoll, remains something of a mystery. The mystery is all the more ironic when we consider the range and number of her accomplishments as a pioneer cryptologist, and that she was a woman working in the mostly male domain of naval cryptology.

(U) She was born on 24 July 1889 in Genesco, Illinois, to Dr. Gustav F. and Lucy Andrews Meyer. In 1911, she received an A.B. from Ohio State University, having majored in mathematics, music, physics, and foreign languages. Her curriculum was atypical of women's education in the post-Victorian era. After college, she moved to Amarillo, Texas, where she taught in various high schools. By 1918, she was the head of the mathematics department at Amarillo High School. However, events were soon to change her career completely.

(U) In April 1917, as a result of the unlimited U-boat campaign and the revelations of the Zimmermann Telegram, the United States declared war on Germany. By early 1918, the U.S. Navy found that it had a serious personnel shortage as the war soaked up the pool of available manpower. To fix this problem, the secretary of the navy, Josephus Daniels, made the far-reaching decision to allow women to enlist. A large number of American women answered the call to arms. Among them was Agnes Meyer, who resigned her position in Amarillo and enlisted in the Navy on 22 June 1918.

(U) She began as a Chief Yeoman (F), the highest rank that could be achieved by a woman. ("F" stood for female, to distinguish it from the male Yeoman.) She was assigned to Washington, D.C., and worked in the Postal and Cable Censorship Office reviewing telegrams and letters for compromises or indications of espionage activity. She later was transferred to the Code and Signal Section of the Director of Naval Communications (DNC), which was responsible for developing the operational codes and ciphers for the U.S. Navy. At war's end, women were offered the opportunity to be discharged with an option to accept a civilian position within the Navy Department. In mid-July 1919, Agnes Meyer took the offer and began working as a civilian in the same section.

(U) Shortly after being hired by the navy, she was invited to spend some time at the famous Riverbank Laboratory in Geneva, Illinois. This was the same place where William and Elizebeth Friedman had begun their cryptologic careers. Later in 1920, she spent about five months at Herbert O. Yardley's Cipher Bureau (more popularly known as the "Black Chamber") in New York City. Yardley's bureau took on trainees from other government offices, so this was not unusual. In addition, Yardley's greatest successes were against Japanese systems; therefore, it is possible that the foundation for her later cryptanalytic exploits may have begun while at the bureau.

(U) Interestingly, during this period the navy's communications intelligence effort was, for the most part, still an idea. Some theoretical studies had been done before, during, and after the war, but an organization designed explicitly to intercept, decrypt, and report intelligence from the radio traffic of other navies did not exist. Much like the army, the navy's cryptologists were producing systems to protect its own communications. So Miss Meyer spent the next year working with the head of the Code and Signal Section, Lieutenant Commander William Gresham, on the development of a device known as the "CM" or the Communications Machine. In 1921, this device, which was a sort of mechanical cipher device based on a sliding alphabet system, became one of the navy's standard cryptographic systems for most of the 1920s. In 1937, in belated recognition for her work, Congress awarded Agnes, along with Gresham's widow, $15,000.

(U) That same year, Miss Meyer's career in cryptographic development took a curious turn. She had responded to a publicized challenge to decipher a supposedly invulnerable cipher message produced by a machine. She solved it, much to the chagrin of the machine's developer, Edward Hebern. Hebern had invented the first cipher machine to use a rotor and had submitted it to the navy for consideration. He thought that Agnes might help him design a better device, and in 1923 he hired her away from the navy as a technical expert. Ironically, her place in the navy was filled temporarily by Elizebeth Friedman. Despite her best efforts, the Hebern machine could not provide the cryptographic security promised by its designer. In 1924, an evaluation by William Friedman revealed the severe shortcomings of the machine. The Navy lost interest and Hebern's company folded. Agnes returned to Washington and the navy.

(U) Circumstances for Agnes had now changed. For one thing, she was now married. Her husband was Michael B. Driscoll, a lawyer for the Department of Commerce. More importantly, for Mrs. Driscoll the Navy had created a cryptanalytic mission in the Code and Signal Section, known as the Research Desk. Lieutenant Laurance Safford was in charge, and he was assisted by one cryptanalyst (Driscoll) and two clerks. For the next 18 years, Safford and Meyer would work together in establishing what eventually became OP-20-G. He organized the intercept and analytical efforts, while she provided the cryptanalytic and technical base for the navy's COMINT effort. Like the Black Chamber, and later the army's codebreaking efforts, the navy concentrated on Japanese communications. This emphasis on Tokyo's communications seems to have originated in

both the availability of Japanese messages and a feeling that the potential existed for conflict between Japan and the United States over China, colonies, and trade.

(U) The first break for the Research Desk was the exploitation of the current Japanese Navy's operational code, known as the Red Book. Actually, the code book itself had been snatched and copied by the Office of Naval Intelligence. The problem for Mrs. Driscoll was recovering the cipher systems used to encrypt the code groups. At first, the Japanese used relatively simple additive or transposition systems. But within a few years a dozen systems were being used with multiple keys. Surprisingly, though, very few of the decrypted messages were translated since the Research Desk lacked enough Japanese linguists.

(U) The breakthrough paid off in 1930 during the Imperial Japanese Navy's Grand Maneuvers. OP-20-G analysis of the exercise indicated that Tokyo had developed a good insight into American naval planning, specifically War Plan Orange, which called for Pacific Fleet operations near the Japanese home islands. Critical to this was Mrs. Driscoll's cryptanalysis. For the maneuvers, Japan had issued a new cipher and daily changing keys for the Red Book. However, she was able to exploit the system. Her breaks, and the input from traffic analysis by the U.S. naval team on Guam, secured the place that cryptology held in the U.S. Navy.

(U) In December 1930, the Japanese navy went to a new code - the Blue Book. This system entailed over 85,000 code groups that were further enciphered. The immense difficulty in recovering the Blue Book was that both the cipher and the code groups had to be recovered simultaneously. There were no cribs or translations available. Critical to Mrs. Driscoll's breakthrough was the insight into the difference in the groupings of the code values. Her success also was important since this particular effort was one of the first times that IBM "tabulating machines" were used to keep track of cipher and code groups.

(U) Mrs. Driscoll's successes were not limited just to paper codes and ciphers. Sometime before (or in) early 1935, she began the attack on one of Japan's early machine cipher systems, the M-1, or Orange, used by its naval attaches. The machine was derived from earlier ones like the Kryha or Hebern. Mrs. Driscoll developed a manual method of decryption which used a diagram on cross-section paper against which she slid the recovered cipher sequence. This breakthrough led to a pair of controversies, though.

(U) The first involved a dispute with the cryptanalysts in the army's codebreaking unit, the Signal Intelligence Service (SIS). That group, under Frank Rowlett, had been working on the Japanese Foreign Ministry's cipher device known as the Red machine, which was similar to the Orange machine. Rowlett's breakthrough came at about the same time as Mrs. Driscoll's. Later, navy apologists would claim that the SIS benefited from technical information provided by OP-20-G. The army denied this and claimed they had received no

help from the navy. The controversy is almost impossible to settle. Both service cryptologic units were extremely reluctant to share any information with the other. Technical exchanges often were made with one side not knowing what the other was working on. The degree of cooperation often hinged on the personalities involved. Safford was not friendly to the SIS. On the other hand, later OP-20-G commanders, such as Joseph Wenger, were far more accommodating.

(U) The second issue for the navy stemmed from its interpretation of Japanese naval cryptologic trends. The success against the Orange machine convinced many in OP-20-G that the future lay in machine systems. Anticipating this, the navy had one of Mrs. Driscoll's associates, (then) Lieutenant Jack Holtwick, work on an analog device to replicate the Orange machine and possible future modifications. However, the Japanese navy remained wedded to paper codes and ciphers. The only machine it produced was the 1940 successor to the Orange machine, codenamed Coral by the Americans. (In fact, except for a few new machine systems, notably Purple, Jade, and Green, Japanese cryptography used mostly manual paper systems.

(U) In 1937, Mrs. Driscoll was involved in a serious traffic accident in which her jaw and leg were broken. After more than a year of convalescence, in which her leg never properly healed and forced her to walk with a cane, she returned to OP-20-G. At least one source claimed that, upon her return, she appeared to have undergone a personality change. This observation is disputed by other members of OP-20-G and close relatives. Perhaps the best argument against this "change" was that the navy charged her with breaking the new general-purpose code, eventually known as JN-25.

(U) In June 1939, the Japanese navy had introduced the new code. It was an extremely complicated system: it involved three separate codebooks, a 300-page book of random additives, and an instruction book. The original codebook, designated the "A" by OP-20-G, contained over 30,000 five-digit groups that represented numbers, place-names, and other meanings. A key characteristic was a self-check system for groups. When all of the digits of a group were added, the total was divisible by three. By late 1940, after a little over a year, some progress had been made. A few thousand of the additive groups had been stripped away, and over 500 of the code groups themselves had been recovered. The navy could read some standard format messages, such as weather reports, but the bulk of the messages remained to be discovered. With the navy's best codebreaker leading the attack, there was hope for an eventual success.

(U) However, in October 1940 Mrs. Driscoll was moved off the JN-25 problem and assigned a team to work on German naval systems. This curious move, which ultimately benefited neither effort, was the result of a division in policy within OP-20-G. The move would also signal the end of Agnes Driscoll's cryptanalytic successes.

[(U//~~FOUO~~) Robert J. Hanyok, Center for Cryptologic History, 972-2893s, rjhanyo]

Almanac 50th Anniversary Series

Content Owner: Feedback

Web POC: Feedback

Last Modified: by nsr
Last Reviewed: February 28, 2003
Next Review: 365 days