From AFIO's THE INTELLIGENCER
JOURNAL OF U.S. INTELLIGENCE STUDIES
VOLUME 25 • NUMBER 2 • Fall 2019 $15 SINGLE COPY PRICE

ASSOCIATION OF FORMER INTELLIGENCE OFFICERS
7700 LEESBURG PIKE, SUITE 324
FALLS CHURCH, VIRGINIA 22043
WEB: WWW.AFIO.COM * E-MAIL: AFIO@AFIO.COM

When Intelligence Made a Difference

— EARLY 20TH CENTURY —

Stealing the Japanese Codebooks
or
One Peek is Worth Two Finesses

by RADM T. A. Brooks, USN (Ret.)

The story of how U.S. Navy cryptanalysts broke Japanese naval codes prior to and during World War II has been told many times and in great detail. The complexity of the codes (and the Japanese language) and the brilliance of the cryptologists who broke them – and then re-broke them and re-broke them as the Japanese changed them – cannot be overstated. To the layman reading about the code-breaking exploits of Agnes Driscoll, Laurence F. Safford, Joe Rochefort, and the personnel of what came to be known as the U.S. Naval Security Group bordered on the miraculous. How were they able to accomplish this almost impossible feat in an era long before the advent of the computer? The answer, of course, is sheer force of intellect... and incredible dedication.

But they did have a little help—particularly at the beginning. A part of the story, which is not commonly known, concerns the ability of the Office of Naval Intelligence (ONI) to steal copies of the Japanese naval codebooks (and copies of diplomatic cryptographic material as well) and provide them to the Navy's fledgling cryptanalytic effort during the period from 1920-23 through as late as 1939.

In Captain Wyman Packard's semi-official history of ONI, *A Century of Naval Intelligence*, he relates the story of an ONI team from the District Intelligence Office (DIO) Third Naval District in New York City breaking into the One Madison Square offices of the Japanese Inspector of Naval Machinery (a Japanese "purchasing mission" attached to the New York City Japanese Consulate and headed by an undercover Japanese naval officer), opening the safe, and photographing the Imperial Japanese Naval Codebook of 1918. Because of the primitive nature of photocopying at the time, the process required break-ins on five consecutive nights.[1]

The break-in described by Captain Packard, and also highlighted in Jeffrey Dorwart's book, *The Office of Naval Intelligence*,[2] took place in May 1929. Both authors relied on the somewhat self-aggrandizing diaries of LCDR Glenn F. Howell, USN, who was the District Intelligence Officer at the time. Howell's diary (and thus both Packard's and Dorwart's books) leave the impression that the 1929 break-in was the first and perhaps the only such break-in conducted by ONI to obtain copies of Japanese naval codebooks. Neither impression would be correct. The 1929 break-in was but one of many conducted by ONI-led teams against the Japanese consulate in New York City. Most of these break-ins also involved the FBI and the New York City Police.

The precise date of the first break-in and codebook recovery is not known, but it clearly was between 1920 and 1923. CAPT Laurence Safford who, as a Lieutenant in 1924 headed the Navy's first organization dedicated to cryptanalysis, in his semi-official *A History of Communications Intelligence in the United States – with emphasis on the U.S. Navy*, places it in "about 1922."[3] John Prados, in his epic work *Combined Fleet Decoded*, places it in "about 1921"[4]. Edwin Layton, in his *And I was There*, says the break-in occurred in "Spring 1920."[5] None of the authors cite a source, so "the 1920-23 timeframe" is probably as definitive a date as can be determined.

Very deliberately, ONI kept no records of the break-ins and information concerning them comes from personal recollections and writings of a number of the people who were involved in early U.S. Navy intelligence and cryptanalytic efforts against the Japanese. In his book, *Surreptitious Entry*, Willis George, who headed the Third Naval District break-in teams immediately prior to and during the opening years of World War II, relates that he was cautioned that break-ins were illegal and that, if caught, he was on his own. His guidance went along the lines of "get us codebooks but please don't tell us how you got them." In his book

1. Packard, Wyman H. *A Century of U.S. Naval Intelligence*, Washington D.C., Dept. of the Navy, 1996, p.282.
2. Dorwart, Jeffry M, *The Office of Naval Intelligence: The Birth of America's First Intelligence Agency*, Annapolis MD, U.S. Naval Institute Press, 1979.
3. SRH-149: Safford, Laurence F., *A Brief History of Communications Intelligence in the United States, with Particular Interest in the United States Nav*. Re-printed by Navy Cryptological Veterans Association, 1982, and re-published as an NCVA Special Publication Fall 2004, p.24.
4. Prados, John, *Combined Fleet Decoded*, New York City, Random House, 1995, p.76.
5. Layton, Edwin T., RADM, USN, *And I was There*. New York City: William Morrow and Co.,1985, p.31.

he claims that DIO teams conducted more than one hundred break-ins and retrieved codebooks of several nations other than the Japanese, strongly implying that this included the codes of Vichy France and Franco's Spain.[6] Consular break-ins and safe-cracking appear to have been a thriving industry in New York City prior to World War II!

But how many break-ins and code recoveries were there between the original 1920-23 period and the attack on Pearl Harbor? While there is no way to arrive at a definitive answer, Layton makes reference to break-ins and recovery of crypto materials in 1926 and 1927, and Safford makes reference to break-ins as late as 1938-39. He refers to the safe which yielded the codes in 1920-23 as "a never-failing source of supply for effective and reserve diplomatic ciphers and keys."[7]

The Japanese Imperial Navy code of 1918 came to be known as the "Red Book" code and remained in effect through 1930. It allowed the U.S. Navy to monitor Japanese fleet exercises and obtain information on Japanese tactics, ship capabilities, and construction plans. But the most important impact of possessing the codebooks was the fact that it compelled the U.S. Navy to create a communications intelligence capability within the Code and Signals Section of the Office of Naval Communications (ONC—also known as Op-20). Under the cover title of "Research Desk" and referred to as Op-20G, this organization was initially headed by then-LT Safford.[8]

Safford highlights the importance of the crypto materials obtained in the break-ins of the 1920s and the resultant ability to read the "Red Book" codes:

1. It was the determining factor in establishing the Research Desk in the Code and Signals section (January 1924).
2. It was a constant incentive to build up a radio intelligence organization to exploit our possession of this code.
3. It assisted our early efforts to a great degree when our cryptanalytic force was very small and inexperienced....
4. It showed us... that we must have qualified Japanese linguists....
5. It gave us invaluable information concerning Japanese Navy and Japanese war plans....
6. It forecast Japanese intentions of conquest....
7. It was useful, even after supersession, giving a probable vocabulary of later codes....[9]

Safford's appreciation of the value of the Japanese Navy codebook purloined in 1920-23 is best summarized by his observation, "If we had been faced at the beginning with the task of solving the cipher plus an unknown code, it might have been too much for us and, at least, it would have slowed our early efforts."[10]

In 1930-31 the Japanese changed their codes. The old 1918 code known as the "Red Book" was replaced by an entirely different code, which came to be known as the "Blue Book." Safford states that no "cribs" (aids such as stolen codebooks) were ever available for the Blue Book[11] and that it had to be solved by brute-force analysis. Layton confirms that no break-ins were conducted to assist in solving the Blue Book codes – allegedly because relationships between the Director of Naval Communications and the Director of Naval Intelligence were so strained that ONC refused to ask ONI for assistance.[12]

Nonetheless, the Blue Book was laboriously reconstructed and, by the mid-1930s, Op-20G analysts, led by Ms. Agnes Driscoll, had effectively broken it.

Captain Ellis Zacharias, a Japanese language officer who rose to be the Deputy Director of Naval Intelligence, in his book *Secret Missions; The Story of an Intelligence Officer*[13] tells the story of entertaining the Japanese Naval Attaché while an ONI team broke into the attaché's apartment to search for a code machine, which they thought might be kept there. Because the break-in team would be searching for cryptographic material or machines, Zacharias enlisted the aid of LT Jack S. Holtwick, a remarkably talented cryptologist who was working on Japanese codes at the time. He would be assisted by a Navy Chief Electricians Mate. Both would be disguised as electricians who had come to the apartment to fix a problem with the lights – a problem which they had created over the preceding week by periodically removing the fuses servicing the apartment. Armed with powerful searchlights,

6. George, Willis, *Surreptitious Entry*, Boulder CO: Paladin Press, 1990.
7. Safford, p.27.
8. The famous "Black Chamber" State Department-Army cryptologic effort headed by Herbert O. Yardley was able to break the Japanese Diplomatic codes prior to the negotiations for the 1921 Naval Disarmament Treaty. This allowed U.S. negotiators access to the Japanese negotiating strategies. While the U.S. Navy played no role in this cryptanalytic effort, senior U.S. Navy leaders were aware of the impact that our ability to read the Japanese codes had on the U.S. achieving a very favorable agreement. Knowing this, senior U.S. Navy leadership was probably favorably disposed to the creation of a navy cryptanalytic effort in 1924 after Japanese naval codebooks had become available.
9. Ibid. p.204.
10. SRH 305, *The Undeclared War; History of R.I.* (Radio Intelligence) 15 Nov 1943, p.3 as cited in Layton, p. 33.
11. Safford, p.28.
12. Layton, p. 48.
13. Zacharias, Ellis M. *Secret Missions: The Story of an Intelligence Officer*, Annapolis MD, U.S. Naval Institute Press, 2003 pp.180-82.

the pair entered the apartment and, accompanied the entire time by the Japanese attaché's servant, searched every nook and cranny of the apartment looking for "a problem in the wiring" while the Japanese attaché enjoyed cocktails in Zacharias' apartment. Having completed their search, one of them made a show of taping some wires while the other went downstairs and replaced the fuses. They then declared the problem fixed, which indeed it was, and departed, having determined that there was neither coding machine nor cryptographic material in the apartment.

Some Folklore
(True or not, it makes a good story)

Willis George was the head of the ONI break-in team in New York City. One night George's team was assigned to break into an unidentified office and, in the process of so doing, broke a window. There was no time to replace the window prior to the office opening in the morning. What to do? An enterprising member of the team went out and captured one of the city's ubiquitous pigeons. The break-in team finished its work and then locked the pigeon in the office and departed. The next morning the tenant came in, discovered the pigeon fluttering around in the office, and concluded that the dumb pigeon had broken the window and flown into the office.

Although Holtwick had not been able to obtain the attaché's crypto machine, he and Ms Agnes Driscoll were later able to construct a machine which was capable of breaking the Japanese attaché codes.[14] Safford states that our subsequent ability to read those codes was aided by break-ins at the New York City Japanese Consulate as late as 1939.

The job of solving Japanese diplomatic codes was assigned to the Army's Signal Intercept Service under and its brilliant cryptanalyst William F. Friedman, while the Navy was to focus on Japanese naval codes. Friedman's team had solved the Japanese "Red" code machine[15] by the mid-1930s with substantial Navy help – to include purloined key lists, etc. from the "magic safe" in New York City. But in 1939 the Japanese changed to a new and much more complex machine code dubbed "Purple." By 1940 Friedman had solved this code as well in a brilliant effort, which Safford characterized as, "...the masterpiece of cryptanalysis of the war era."[16] Navy cryptanalysts helped the Army recover keys to the Purple system, but the successful assault on the Purple code was an Army achievement.

However, by the winter of 1940-41 the volume of Purple traffic had become too high for the Army's translators who were forced to ask for help from the Navy. It was decided that the task of decrypting and translating the Purple code would be divided. Navy would take odd-numbered days and Army would take even-numbered days. Thus, it came about that it was a Navy team that decrypted the key last section of the famous "14-part message" on 7 December 1941. While many sources state that the successful breaking of Purple was a joint Army-Navy effort, it really was not. It was a U.S. Army success. Navy helped. There is no evidence of ONI "black bag" jobs having contributed to the successful attack on the Purple code.

The story of U.S. Navy successes in obtaining/breaking Japanese naval codes would not be complete without observing that the Japanese were doing the same thing to us. In the 1930s they managed to solve our fleet systems, then being encrypted by the commercially available Hebern Coding Machine. They succeeded in breaking all of our diplomatic codes, to include the high-level State Department "Grey Code." This was accomplished by the Japanese Secret Police repeatedly breaking into the U.S. Consulate in Kobe, Japan, opening the Consul's safe, and photographing the codes/ciphers.[17] They similarly stole British codes by way of break-ins, while, at the same time, British Intelligence was conducting break-ins to obtain various foreign cryptographic material.

The U. S. was not the only nation that recognized that "a peek is worth two finesses."

Rear Admiral Brooks was a career Naval Intelligence Officer. He served as Director of Naval Intelligence from 1988 to 1991.

14. Layton, p.79.
15. Not to be confused with the "Red Book" Japanese naval code. The Red Book was a classic book code while the Japanese diplomatic Red Machine was a machine-generated cipher system. There was no similarity between the systems other than the fact that it was decided to use the color "red" to describe them both.
16. Safford, SRH 149, p.25.
17. Layton, op.cit. pp.47,48