Agnes Meyer Driscoll vs. the Enigma and the Bombe

Colin Burke

ABSTRACT**:** **D**ocuments in Britain's National Archives/ Public Record Office and in the U.S. National Archive's Record Groups RG457 and RG38 indicate that in mid-1941 the United States Navy's codebreaking organization, OP-20-G ignored an opportunity to gain full knowledge of Britain's anti-Enigma methods and machines. Spending a year and one-half working on what it felt was a unique and much more effective method– but one that failed--OP-20-G's, staff, at a critical time in U.S.- British relations ,did not inform America's decision makers of Britain's willingness to share its crypto-secrets . As a result, American leaders believed that England's GC&CS had deliberately withheld vital information that would have allowed the development of an independent American attack on Naval Enigma. That belief lasted

throughout the war and caused friction between the two nations. Other consequences of OP-20-G's mid-1941 decision were to delay the adoption of the British Bombe and its allied methods and to waste perhaps six months of the vital time of the new team of cryptanalysts and engineers assigned, in early 1942, to develop an American Bombe.

KEYWORDS: OP-20-G, Enigma, Driscoll, Denniston, GC&CS, Bombe, Safford, Wenger, Weeks, Currier, Engstrom, catalog, Banburismus, hot-point, cold-point, Tiltman.

Introduction: A Fragile British-American Crypto-Alliance

By the end of World War II Great Britain and the United States had forged uniquely close relationships--even among their intelligence agencies.[1] Much had to be overcome to achieve the long-lasting

---

[1] Robert Louis Benson, *A History of U.S. Communications Intelligence during World War II: Policy and Administration*, U.S. Cryptologic History, Series IV, World War II Vol 8, Center for Cryptologic History, National Security Agency,

collaboration, however. Distrust that arose between their cryptanalytic agencies in 1941 and early 1942 was one of the significant obstacles. The American Navy's belief that Britain withheld vital Enigma information remained a sore-point–even after the two nations' intelligence agencies had carved a record of more than three years of cooperation.

The American Navy's interpretation of the events of 1941-2 was incorrect. To paraphrase Shakespeare: The fault lay not only in Britain but in the offices of the American Navy's cryptanalysts. A critical August 1941 decision by the navy's top codebreaker to ignore a generous British overture was at the center of the problem, but several months of tension-filled contacts between cryptanalysts in America and England preceded it. The tensions were, to a great degree, caused by fears that naive politicians and diplomats were endangering their nations' greatest secrets.

Distrust had marked British-American crypto relations before

Ft. Meade, Md., 1997.

World War II. In the years before the United States became a belligerent suspicion stood in the way of cooperation. However, beginning in 1940 the leaders of both nations prodded their codebreakers to eliminate or ignore barriers to a partnership. Despite resistance from those worried about security, the pressures from the top led to an historic exchange of vital cryptanalytic methods and machines in early 1941--almost a year before the United States formally entered World War II.

As the two nations continued their earlier exchanges of intercepts and methods for Far Eastern problems, in February 1941 four American cryptanalysts traveled to England's codebreaking center (GC&CS) at Bletchley Park. They brought more than half a ton of their country's most precious code and cipher breaking documents and machinery. In exchange, the British codebreakers gave the Americans a tour of Bletchley's secret rooms and informed them of Britain's cryptanalytic methods and achievements. Of importance, they told the Americans of progress against all of Britain's European foes.

The British revelations included their greatest secret: the techniques and machines they were using to attack Germany's Enigma-

based encryption systems. The Americans even saw the Bombes, the only devices capable of quickly penetrating the newest versions of the Enigma machines. There were promises of a flow of more information when secure communications links between England and America were established.

That seeming openness and the expectations of continued full cooperation were not a prelude to harmony, however. The early 1941 Bletchley exchange became an irritant. Throughout the war, there were accusations that the British failed to keep the promises they made during the visit. Many Americans interpreted the assumed failure of Bletchley to share more Enigma information during 1941 (and the first half of 1942) as an indicator of something more ominous: a British desire to dominate German military communications intelligence, making the United States a near blind dependent.

The resentment over the assumed failure of the British to supply information on Germany's most secret machines was especially strong within the American navy's codebreaking agency, OP-20-G. Its officers' discontent surfaced as early as mid-1941 and continued in various forms

and intensities throughout the war. The convoy crisis in the Atlantic intensified the concerns, ones that reached upwards within the navy's' hierarchy. Then, when Bletchley seemed to lose any hope of reading the German's Atlantic U-boat Enigma messages at the beginning of 1942, the American navy felt doubly betrayed. Its representatives heatedly protested that England had and continued to withhold vital information needed for the development of an American Enigma attack; and, the American codebreakers felt the promise that Bletchley would soon again be able to read the U-boat transmissions was worthless. By mid-1942, the American army's codebreakers joined the protest.[2]

Frictions caused by the interpretations of the 1941 visit's agreements continued-- despite the attainment of unprecedented fellowship between the two countries in1942 and 1943. During those

---

[2] Bradley F. Smith, *The Ultra-Magic Deals: And the Most Secret Special Relationship 1940-1946*, Novato, CA, Presidio Press, 1993; NARA, RG457, HCC, NR4384, Box 705, 'History of the Bombe Project, 24 April 1944'; Dundas P. Tucker, (Laurance R. Safford) "Rhapsody in Purple," *Cryptologia*, 6 #3, (July, 1982), 193-228.

years, interaction on Japanese problems had deepened and by the summer of 1942, England was providing the American Navy the requested details of its Bombe attack. Bletchley would soon trust the Americans with operational work on the German U-boat Enigma systems. As well, in autumn 1942, the navy and the British signed a relatively broad sharing agreement. After some tense moments at the end of the year, England forged understandings with the American army. At mid-year 1943, the signing of the BRUSA pact settled many remaining issues with the American army. [3]

Yet, problems remained. The memories of the events of 1941 at times inflamed them. In a very important report to the Director of Naval Communications in April 1944, for example, the three leaders of OP-20-G's successful 1942-1943 Bombe development effort responded to

---

[3] Ralph Erskine, "The Holden Agreement on Naval Sigint: The First BRUSA?" *Intelligence and National Security*, 14 #2 (Summer 1999), 187-197. However, frictions continued throughout the war. For an insight into some of them: PRO HW3/93', Eric Jones Comments on Nigel DeGrey's Official History, November 23, 1948'.

some worrisome questions about the history of the navy's Enigma projects. They cited the failure of GC&CS to supply promised information about its Bombe-based anti-Enigma methods and technologies in 1941 and early 1942. That caused, it was implied, the American navy to be powerless during the critical months of U-boat attacks in 1942--although it had begun its own anti-Enigma program in late 1940.[4]

---

[4] NARA, RG457, HCC, NR4584 Box 705, 'History of the Bombe Project, 24 April 1944'; and, NARA RG38, CNSG, Library, Box 104, 5720/205, "American Cryptanalysis of the German Naval Enigma," 7 July 1944, OP-20-GY-A to OP-20-G-1 states (partially incorrectly, as will be shown):

> "Prior to the outbreak of war with Germany, the nature of the German machine employed by the Atlantic U-boats was known in that the British had supplied this Division diagrams of the wiring and wheels of the device, together with a description of the way in which it moved. Beyond this and some few examples of plain text, nothing was known as to the usages of the device nor the method in which keys could be recovered. At that time a small group of Civil Servants, headed by Mrs. P. (sic) Agnes Driscoll, were

A Opportunity to Change Cryptanalytic History

That and similar reports were not on the mark. Somehow, those OP-20-G officers, historians, and, more importantly, the American naval leadership of the early 1940s, remained unaware of a generous overture by the British in summer-1941. Knowledge of it could have changed the American navy's view of early British-American relations. Its acceptance might have altered the history of the navy's battle against Enigma.[5]

---

conducting preliminary research on the problem. It was then known that the British were conducting a successful attack, but the details of it were unavailable to the American Navy, due to the reluctance of the British to disclose the same"

[5] Earlier works on the history of the beginnings of the British-American crypto relationships are: Stephen Brudiansky's, "The Difficult Beginnings of U.S.-British Codebreaking Cooperation," *Intelligence and National Security*, Summer 2000; and, Lee A. Gladwin's , "Cautious Collaborators: The Struggle for Anglo-American Cryptanalytic Co-operation, 1940-43, in, David Alvarez (ed.), *Allied and Axis Signal Intelligence in World War II*,, London, Frank Cass, 1999, 119-

In August 1941, the American navy's lead cryptanalyst disregarded a British proffer of detailed knowledge and even, eventually, a copy of the only machine that 'conquered' the Enigma, the Bombe. Embedded in the invitation was a willingness to supply specific information on the many techniques required to maximize the Bombe's powers.[6]

Others in the American crypto and intelligence communities of the time were not informed of the British openness, at least in enough detail to allow the recognition of its significance for 1941`s interaction and for the relationships during the remainder of World War II.

---

145. Budiansky's book, *Battle of Wits*, New York, Free Press, 2000 also discuss the relationship. These works do not mention the navy's chief codebreaker nor the critical refusal discussed below.

[6] PRO HW14/45 and 46, 'Denniston report(s)', September 5, October 31, December 1, 1941, February 15, 1942. The offer of a Bombe could not have been immediately fulfilled as the British were quite short of such machines. However, technical designs and information on methods could have been and were provided.

An amiable reception of the British invitation would have led to earlier familiarization with the detailed logic and the technology of the Bombe and to a better understanding of all German Enigma systems. It might have cut as much as one year off the time that it took the United States navy to establish its own workable Bombe program. Knowledge of the offer in the intelligence community (and of its rejection) could have reduced the emotionally tense complaints of the Americans in 1941 and 1942 and hastened the onset of the cooperation and trust of the later years of the war.[7]

Politics, Personalities and Independent Cryptanalysis

The disregarding of the invitation to Bletchley's secrets cannot be

---

[7] Bradley F. Smith, Op. cit. Also informative is, Ralph Erskine, "Churchill and the Start of the Ultra Magic Deals," *International Journal of Intelligence and Counterintelligence*, 10 #1 (1997), 57-, and, his, "The Holden Agreement on Naval Sigint: The First BRUSA?", *Intelligence and National Security*, 14 #2 (Summer 1999), 187-197. The 'official' American history of the two nations' communications intelligence relationships is, Robert Louis Benson, Op. cit.

explained away as simply the result of ignorance of the cryptanalytic importance of the British Bombe and its allied methodology. Nor, can the navy's response to Britain's contact in August 1941 be treated as just the result of a faith in the anti-Enigma method OP-20-G was developing. Personalities, America's lack of intercept and analysis resources, the state of Britain's technology, tangled communications (especially within the American Navy) and, importantly, the politics surrounding the United States' involvements in Europe played central roles.

A Woman With Ambitions

OP-20-G's chief codebreaker, Agnes Meyer Driscoll, although burdened with physical problems stemming form an auto accident, was a mature and experienced cryptanalyst when she turned away from the overture by the operational head of Britain's Bletchley Park, Commander Alastair G. Denniston. She was fifty-three, intelligent, well educated, and had spent a quarter century working on codes, ciphers, and encrypting machines. She already knew something of the Bombe attack on Enigma and was receiving data on German systems from England as

early as March 1941. Denniston told her more during his August 1941 visit to the navy codebreakers' Washington headquarters.

A first generation American and a very attractive daughter of a mid-western intellectual, Driscoll had been able to attend a fine liberal arts college and Ohio State University. Her college majors reflected her talents in areas that underlie successful codebreaking: mathematics, music, and foreign languages.[8] One of the many unknowns about her is why she decided to leave the Midwest and her family. After graduation, she spent seven years as a teacher/administrator in a city in Texas. Then, she decided to move and, perhaps, to change careers. Although Amarillo was an urban center, it could not provide enough intellectual and cultural support for an energetic, inquisitive, and artistic

---

[8] For the latest attempt to overcome the lack of documentation concerning her life and career, see, Robert Hanyok, "Still Desperately Seeking "Miss Agnes": A Pioneer Cryptologist's Life Remains an Enigma," *NCVA Cryptolog*, Fall 1997, 22-. Also, Ray Schmidt, "First Lady of Naval Cryptology," as in, NCVA, *A History of Communications Intelligence in the United States with Emphasis upon the United States Navy*, Denver, Co., 1982, 44-45.

single lady. She was adventurous and somewhat of a workaholic.

Perhaps that is why Agnes, with a secure job and nearly thirty years old, made an unusual choice: In 1918, she and her sister were among the first to enlist as navy Yeomanetts. Although the navy granted her the highest possible entry-level rank, Yeoman, her decision to join the navy's new women's corps must have caused Agnes some anxiety. No long-term career or personal guarantees came with the enlistment papers.

There is no indication that she or her sister joined because the navy had promised them a posting to the exciting wartime city, Washington, D.C. However, the navy assigned them there where she and her sister worked in the navy's censorship corps in the office of the Director of Naval Communications. The job was rewarding, partially because it had ties to intelligence work and to the navy's newly expanded Code and Signal Section, the predecessor of the navy’s cryptanalytic group, OP-20-G. Although she began her enlistment with the uninspiring formal title of "stenographer," she was soon performing more stimulating and important tasks than taking dictation. She met all

the challenges and soon received the highest rank for a woman in the navy, Chief Yeoman. It appears that by the end of the war she was engaged in cryptologic work within the Code and Signal section.

That assignment was fulfilling and she gained respect as at least a fledgling cryptologist. Despite the cutbacks at the end of the war, her supervisors asked her to continue as a civilian employee, probably working on the construction of the navy's own codes. She liked the work, was well paid, and she soon accepted offers that brought her into contact with the best of America's codebreakers. She quickly became part of the nation's small and interconnected cryptologic community. During the next few years, she was at Riverbank Laboratories, Herbert Yardley's Black Chamber, and Hebern's Electric Code Company.[9]

While with Hebern, she learned much about the new electric enciphering machines of the era. Part of her job with him, and the navy, was to find the cryptologic weaknesses of such devices and the failings

[9] U.S. Navy Historical Center, Operational Archives, SRH355, "Naval Security Group History to World War II, Part 1," 28-35.

of all of the latest mechanical encryption machines.[10] As early as 1921, she made a successful attack on a new mechanical device that would serve as a basis for some later Japanese machines. In the mid-1930s, she 'solved' at least two of the Japanese navy's new cipher machines. [11]

---

[10] She probably worked on the early and simple version of the commercial Enigma machine and it is likely that she knew of the U. S. Coast Guard's successful attack against the Swiss Enigma's code wheel wiring in the late 1930s. Elizebeth Friedman headed the Guard's efforts. The Swiss machine seems to have been a quite simple commercial version that yielded to traditional attacks. NARA RG457, HCC, NR1737, Box 705, 'Enigma Conferences, Theory'. Useful for the range of Enigma devices is, David H. Hamer, Geoff Sullivan and Frode Weirod, "Enigma Variations: An Extended Family of Machines," *Cryptologia*, 22 #3 (July, 1998), 211-. A German Abwehr agents' Enigma, called Orange by the SIS during WWII, was stecker-less and was broken through hand methods and rather traditional approaches. NARA RG457, HCC, NR3809, Box 1283, "Tour of Duty Report of Capt. Roy Johnson." During WWII the U.S. Army's SIS built a complex catalog for an attack. NARA RG457, HCC, NR2804, Box 950, 'Eggs Catalog'. The report mentions a less sophisticated British catalog for the same problem.

[11] As supplied by Robert Hanyok, Memorandum for Commander Raven (from L.

One of the First Professionals

Despite her career options she remained close to the navy and became a central figure in its and the nation's other formal surges into codebreaking. She was in contact with cryptanalysts in the army and, importantly, Mrs. Elizebeth Friedman who had become the Coast Guard's chief codebreaker. Even with her ties to the nation's capitol, Mrs. Driscoll would always list her legal address as Westerville, Ohio, and would never purchase a home in Washington--although she became a permanent resident of the District of Columbia.[12]

In 1924, just as Driscoll married a Washington lawyer and as the navy formalized its code work, she became Lieutenant Laurance Safford's expert codebreaker and began a long tenure as the instructor of

---

Safford) 3 February 1944, "History of Japanese Cipher Machines," p3, item 8. The machine was made by Damm who later sold his rights to Hagelin

[12] Driscoll's employment history is documented in the '201' file held by Robert Hanyok. Driscoll became a very well paid civil servant as well as a member of the Washington community.

the first generation of naval cryptanalytic officers. Those who the navy assigned to Safford's new Research Desk in Naval Communications never forgot "Miss Agnes."

She had much more on her work-list than the exploration and teaching of methods. An early 1920s theft of an important codebook was the beginning of twenty years of intellectually and physically demanding attacks on Japanese numeric codes. The stressful Japanese challenges were one of the reasons for Driscoll's periodic bouts of weight loss and returns to Ohio to recuperate.[13]

The newly married Mrs. Driscoll devised craftsman-like ways to strip-off the numbers the Japanese used to disguise their codes and she found workable techniques to identify the meaning of the emerging code groups. She also took the lead in the navy's successful attacks against Japan’s encryption machines of the 1930s. She may have been

---

[13] Robert Hanyok's picture file for Driscoll and her family reveals Agnes’ physical ups-and-downs. Family interviews have led Hanyok to believe that Driscoll’s frequent returns to Ohio were for recuperation as well as for tending to family responsibilities.

party to the exchanges between the army and navy that, some claim, helped William Friedman and his colleagues to use statistical techniques, as well as probable word methods (cribs) to conquer Japan's most secure diplomatic cipher machine, Purple, in late 1940.[14]

There are indications that Agnes worked on the systems of other countries and that she was aware of the development of crypto technologies throughout the world. For example, OP-20-G purchased an early 1920s version of the commercial Enigma. Agnes also shared in the information one of her officers brought back from a 1932 trip to survey the world's manufacturers of cryptologic machinery, including the factory making the Enigma encryption machines. She probably knew of that conquest of an older version of an Enigma device by Elizebeth Friedman's Coast Guard team in the late 1930s. [15]

---

[14] According to Robert Louis Benson, the first solution to the Purple machine was on September 27, 1940. Robert Louis Benson, Op.cit., 27, fn 48. NARA RG457, HCC, NR1737, Box 705, 'Enigma Conferences and Theory'.

[15] Joseph Wenger made the trip enroute to his naval assignment. His reports on Enigma show knowledge of models with irregular stepping and mention that

The Japanese code crises never went away, however. The Imperial Navy kept changing its codes, increased the number of systems, frequently replaced the books of numbers used to hide code groups, and improved its cipher machines. There was more than enough work for the few civilians and officers assigned to Safford's Washington center during the decade before World War II.

A Cryptanalytic Team with Commitments

Driscoll and her boss, Laurance Safford, became, if not a team, a fixture

---

OP20G purchased an early 1927 model. As supplied by Robert Hanyok: 'Attache Reports', June-August 1932. On the Coast Guard attack, RG38, Radio Intelligence Publications , Box 171, RIP606, Enigma Series 4, Wiring Recovery.

On Driscoll's direct experience with the more complex machines of the 1920s and 1930s, including European devices: L.F. Safford, Memorandum for Lt. Commander Raven, "History of Japanese Cipher Machines," 3 February 1944, NARA RG457, HCC, NR 2344, Box 808, supplied by Robert Hanyok. Driscoll had worked on machines with irregular stepping patterns. 'G's" Jack Holtwick had created a device to aid in the discovery of the wiring of enciphering wheels. U.S. Navy Historical Center, Operational Archives, SRH355 Op. cit., 225.

at the crypto center. Driscoll's sister joined them.[16] Safford was the first regular naval officer to commit his career to cryptology. That meant that he and Driscoll continuously worked closely together for more than a decade and one-half. They seem to have become of the same mind about cryptanalytic methods and about the politics of military intelligence.

In their early years, they were less than enthusiastic about statistical 'scientific' methods in codebreaking and about the then revolutionary electro-mechanical tabulating machines that were the computers of the 1920s and 1930s. The two codebreakers did become more receptive, however. By the late 1930s, they began to realize that the times might call for new methods and machines. Nevertheless, neither took the lead in OP-20-G's sometimes-disappointing surges into advanced statistical, automated cryptanalysis. [17] They never altered their

---

[16] Federal '201' Employment file.

[17] U.S. Navy Historical Center, Operational Archives, SRH355, Op. cit., 80; and, Colin Burke, *Information and Secrecy:: Vannevar Bush, Ultra and the Other Memex*, Metuchen, NJ, Scarecrow Press, 1994. Also, James Debrosse, *The Secret*

views about the nation's and the navy's role in intelligence, however. They always sought an independent codebreaking capability and they wanted a strong and self-sufficient naval crypto-service. Although often willing to share with the country's other codebreakers, they were also defensive of boundaries and secrets.

Their devotion to OP-20-G's work came at high personal cost. Critical challenges often called for months of continuous work. One of

---

in Building 26, New York, Random House, 2004. This essay was originally written before the Debrosse work and before the appearance of NSA FOIA Case 53567, (R. Hanyok) " Madame X: Agnes In Twilight, "The Last Years of the Career of Agnes Driscoll, 1941-1957," Cryptologic Almanac 50th Anniversary Series, nd. np .

As discussed below, despite Driscoll's mathematical training, she does not seem to have conceived of cryptanalysis through the lenses of abstract mathematics or emerging techniques such as formal group theory. There is no evidence that she explored the newer approaches, such as those put forward by Lester Hill. See his, "Concerning Certain Linear Transformation Apparatus of Cryptograph," *American Mathematical Monthly*, 38 # 3(March 1931), 135-154.

the most important and frustrating tasks came during what was perhaps the worst period in Driscoll's life. In 1939, the Japanese made profound changes in their secret communications systems. A new high-level naval code went on-line--just as America's military became convinced that conflict in the Pacific was unavoidable.

That new JN-25 code appeared a few months after Driscoll had returned to work from more than a yearlong convalescence. She had been in auto accident in 1937 that killed two people and gravely injured her. Both jaws and a leg were broken. Because of her religion, she refused newer medical treatments and she could not resume her duties at 'G' until September 1938. After her return, she remained crippled and, according to some accounts, in need of physical assistance.[18]

Returning to 'G's' downtown Washington headquarters, she was shifted from her work against cipher machines to head the attack on JN-.25.[19] Although she and her team were able to make some inroads, they

[18] U.S. Navy Historical Center, Operational Archives, SRH355, Op. cit., 160.

[19] U.S. Navy Historical Center, Operational Archives, SRH355, Op. cit., 255.

faced repeated disappointments because of continued changes to the system, ones that nullified earlier cryptanalytic progress. Only a small percentage of JN-25 was readable by late 1940. While some thought that OP-20-G's resources should be focused on direction finding and the type of message traffic-analysis that did not require decryption, there was a hope that the methods Driscoll's team developed would, with constant and repetitive effort, turn '25' into a major source of intelligence. [20]

Then, there was a startling decision. In October 1940, Safford gave the Japanese problem to a new small team of relatively inexperienced reserve officers who had arrived in Washington as the navy prepared for war. The new '25' group, and the tiny crews within the navy's Pacific interception centers, did important work, but Japan's major naval code remained essentially unreadable a year later.[21]

---

[20] She seems to have been given formal charge of the JN-25 problem in November 1939. Prescott Currier headed the attack before then. U.S. Navy Historical Center, Operational Archives, SRH355, Op. cit., 400.

[21] The brilliant article, Frederick D. Parker, "The Unsolved Messages of Pearl

A New and Unknown Enemy: Why Now?

A year after World War II began in Europe and as national priorities shifted, Safford ordered Driscoll and three others to take on other challenges: the German navy's codes and ciphers.[22]

The exact when, who, and why of the decision to divert the navy's most experienced codebreaker from the critical Japanese problem are unknown. On one hand, given the growing involvement of the American navy in the Atlantic and the fears that England might be

---

Harbor," *Cryptologia*, 15 #4 (October 1991), 295-, is highly informative on progress against JN-25..

[22] U.S. Navy Historical Center, Operational Archives, SRH355, Op. cit., 400, on the assignment to the German problem. Laurance F. Safford and J. N. Wenger, SRH-149, *U.S. Naval Communications Intelligence Activities*, Aegean Park Press, 1993, 16, gives only 3% of OP-20-G cryptanalytic capability and 0% of its translation effort to German and Italian naval messages in Dec. 1941. This is in some conflict with War Diary entries that cite Driscoll heading a rather large staff in the early years of World War II. Her team, GY-5, had 14 people, all civilians. That was the same size as the Italian naval team.

defeated, it seems a far-sighted and militarily justified decision to replace the small group that had explored some German problems with Driscoll's new team. So was the diversion of much of the navy's direction-finding capability to the Atlantic problem.

However, in some ways the reassignment of Driscoll and her group appears at least ill timed. The very limited ability of the navy's intercept and message processing teams in 1940 meant they could not provide Driscoll with the number and range of messages typically needed to unravel any type of crypto-system. Many of her previous conquests had been based on her adversaries' errors--such as sending messages on readable systems or issuing enough messages on a new system to give codebreakers the 'depth' needed to uncover encryption algorithms. Locating such errors called for intense radio monitoring[23]

That and other vital resources were missing--although Driscoll

[23] At the end of 1941 'G' was intercepting only 20% of the relevant traffic and had to ask Britain to send all the Atlantic intercepts for the past year, which GC&CS did. TNA/PRO HW14/45 Denniston message, December 1, 1941, 'Your CXG 105'.

was facing a great cryptanalytic challenge. The navy did not realize that it had asked her to defeat one of the most advanced encryption machines of the time. The 1940's naval Enigma was a far more difficult target than earlier versions of the device and the German navy was an even more cautious crypto-foe than that nation's army, air force, or intelligence agencies.[24].

Agnes began her assignment in late 1940 with almost no information about the German system–she did not even know it was using an Enigma. Furthermore, there was no heritage of successful

---

[24] The Germans had made their military and naval Enigmas more and more complex and the navy had developed more secure procedures, but some of its subdivisions did not always follow best practice.. A successful attack on the early 1940s Enigmas demanded knowledge of: the internal wiring of each enciphering wheel (as many as 8); the turnover cogs on each; the nature of the machine's keyboard-wheels linkages; its reflector wheel; the wheels (three) selected for the message; their order of placement in the machine; their starting positions; the positions of the slip rings on each wheel; and, the setup of the stecker (plugboard) which further transformed the plain-text The navy's 'fourth wheel' of 1942 added another challenging complication.

American work in any agency on the military or naval Enigmas. A small 'G' group under Wesley Wright had labored on some German naval systems during 1940 but abandoned their frustrating assignment in November because of a lack of progress. They had little to pass on to Driscoll except puzzlement over a new and very complex system they had yet to identify.[25]

Driscoll also experienced great frustrations. Six months into her new assignment, in spring 1941, she could report only that "D1" had finally been determined to be a complex machine cipher (she did not name Enigma) and that a solution to it might be possible.[26]

The lack of progress was predictable.[27] There had been no

---

[25] NARA RG38, Library, Box 130, 5750/1, OP20-GY, War Diaries.

[26] War Diaries. Op. cit., note that her May 1, 1941 pronouncement See below.

[27] The OP-20-G War Diary reports about Driscoll's progress during the period May 1941 through January 1942 are puzzling. On October 1, 1941, they report that "a method of solution [was] determined," but the Enigma is not mentioned by name at the time nor are the British cited. It was almost a year after the Bletchley exchange that the Enigma is mentioned by name and it is announced that a

captures or thefts of naval Enigma system documents; Driscoll did not have a copy of a modern military Enigma or its encryption wheels; and, even if Safford had tasked her to do fundamental research rather than produce useful intelligence, she did not have the needed advanced technological aids.[28]

The navy had only a handful of what had become rather old-fashioned electro-mechanical tabulators.[29] Its very ambitious program of the mid-1930s to create super-fast electronic statistical machines had

---

"method of solution [is] determined and being tested.", War Diaries. Op. cit. Some cryptologic help may have been obtained from the seizure of a large number of German diplomatic codebooks by the FBI in San Francisco in March 1941. NARA RG38, CNSG, Library, Box 77.

[28] Jack Holtwick, in, U.S. Navy Historical Center, Operational Archives, SRH355, Op. cit., 400, quoted that, "Heretofore, they [German naval systems] have resisted attack, but it is hoped that the employment of our best talent will produce results."

[29] NARA RG38, CNSG, Library, Box 104. Serious discussions between OP-20-G and IBM concerning advanced machines did not begin until the outbreak of war.

been starved to near death. Using private funds, OP-20-G was just restarting it in late 1940.[30] There was even little physical space for Agnes' crew; OP-20-G's few rooms were badly overcrowded with people and files.

The minimal resources allotted to Driscoll's group might stand as evidence that her reassignment was the result of Safford's negative reaction to complex political and ideological forces outside of the navy having dictated "G's' policies. Safford's interpretation had some justifications. Agnes' diversion from the systems of what the navy's operational men then considered the great threat, Japan, was perhaps the result of a shift of national and diplomatic priorities by the nation's politicians--rather than being the product of a rational assessment by the navy's highest line officers. The navy may have resented what they saw as political interference in their domain.

However, the problem of minimal resources might have been the result of a decision by lower-level communications intelligence officers,

---

[30] Colin Burke, *Information and Secrecy*, Op. cit., Chpt. 9.

such as Laurance Safford, who wanted the nation to have an independent Axis codebreaking capability but did not have the power to wage a full-force attack. Just a few years after the creation of the new American Enigma group Safford, despite his awareness of Britain's earlier cooperation on the Japanese problems, became a spokesman for those who deeply feared the results of dependence on Britain for cryptanalytic methods and materials. The formation of Driscoll's new group during the period of the navy's reluctance to participate in exchanges with England suggests a desire to quickly find a unique 'G' solution in order to fend-off any pressures to rely upon Britain's codebreakers .[31] There is another possibility--an ironic one: The Driscoll group may have been created to help prepare for a contemplated exchange of crypto-secrets with Britain; and, to be able to quickly exploit the methods to be brought back from England.[32]

---

[31] Dundas P. Tucker, Op. cit.

[32] The timing of the formation of her group suggests a combination of motivations. Established one month after the orders to begin to prepare for the exchange of codebreaking information with Britain (see below). the group may

There is no way to resolve the ‘why’ of the shift of cryptanalytic talent to the Atlantic problem and the ‘why’ of minimal resource allocation. No one has found documents that allow historians to determine if Driscoll and other valuable codebreakers were assigned to the German problem only because of unwelcome orders from the White House. It also remains unclear how much Driscoll and Safford knew of the president's determination to give the European war the highest priority As well, there is no smoking gun proving that Safford's drive for independence was the cause of the reassignment.

Forcing a Perhaps Unwelcome Crypto-Alliance

However, it is certain that pressure was coming from on high in the United States and Britain and that it was reshaping intelligence policy in general. Beginning in early 1940, Britain's critical military situation led to overtures to the United States for more supplies and technical aide.[33]

---

have been created in response to those orders, and, to the desire to develop an American capability before more had to be revealed to the British.

[33] FOIA, Robert L. Benson, "The Origins of U.S. - British Communications

By summer, Britain was directly encouraging exchanges of cryptanalytic as well as the most precious scientific secrets.[34] President Roosevelt and his advisors, including his chief 'spy,' William Donovan, were receptive.[35]

Roosevelt soon bent many neutrality rules. In late summer, he approved an exchange of highly sensitive military/scientific

---

Intelligence Cooperation (1940-1941), *Cryptologic Spectrum*, 7 #4 (Fall, 1977), 5-, is the authoritative article. Although Benson was an 'insider', it seems he did not see some of the documents later found in the Public Record Office (PRO) HW series. See, also, his NSA volume, Op. cit..

[34] Bradley Smith, Op. cit,, 49;TNA/PRO HW14/8 letter to England 11-4-40; TNA/PRO HW14/45 Memorandum of 11-22-40; NARA RG457, HCC, NR2738 Box 940, 'Chronology of the Correspondence Between SSA and the London Office of GCCS; NARA RG457, HCC, NR4565, Box 1413, 'Sinkov Papers'.

[35] Bradley Smith, Op. cit., 14. Donovan's close ties to British intelligence and his ambitions to create, even in World War II, a 'central' intelligence agency may well have led military officers such as Safford to suspect any proposal involving Donovan.

information. In addition, by then Britain had been informed (but not by America's cryptanalytic agencies) in general terms, of America's progress against all types of crypto challenges. At the same time, high-level military and diplomatic representatives were making rather specific commitments about sharing intelligence. At home, the administration began applying pressure on the army and navy's communications/intelligence divisions to formulate plans for the transfer of crypto knowledge and technology.[36]

As England's scientific wizards were preparing to leave for the United States, America's cryptanalysts began to detail their response to what they thought England was offering: a full entry into its cryptanalytic secrets.[37] In mid-summer 1940, the Americans did not yet know what treasures the British held, but some of the nation's cryptologists had hunches about England's German and Japanese

---

[36] 'Chronology of the Correspondence', Op.cit.; NARA RG457, HCC, NR4565, Box 1413, 'Sinkov Papers'.

[37] TNA/PRO HW14/8, November 5, 1940, 'to Hopkinson'.

capabilities.

By September 1940, the planning was intensifying. Although the army and navy crypto groups were in legally separate agencies, they held combined meetings. The American Army's Signal Intelligence Service (SIS) and OP-20-G proceeded under the assumption that they were to have a great degree of latitude in deciding what the United States was to reveal and receive.

The discussion among the army and navy's representatives began with a sense of common purpose and with consensus about the issues. As well, there was pride in what were regarded (at least hoped-for) as American triumphs: the entry in the Japanese diplomatic Purple system; the conquest of JN-25; and, the solutions to important German diplomatic codes.[38] Meanwhile, preparations in England proceeded at a

---

[38] On the 1940 acquisition of part of a German one time pad for the GEE diplomatic system, NARA RG457, HCC, NR4692, Box 202, 'IBM Role at the Army Security Agency'. On the later reading of the Floradora and OTP codes, NARA RG457HCC,NR246, Box 832, Annual Report of the Chief Signal Officer, FY 1942-1943 and, Cecil Phillips, "The American Solution of a German One-

slower pace and there was little coordination between her policy makers and her cryptanalysts. GC&CS' leaders remained worried about sharing any German or Italian secrets. They were quite concerned that any American visitors would be a version of Herbert Yardley:

> "…we are entitled to recall that America sent over at the end of the last war the now notorious Colonel Yardley for purposes of cooperation. He went so far as to publish the story of his co-operation in book form."[39]

The British were also fretful about the security of America's code systems, especially those used by the State Department. They had not proven to be much of challenge to England. Its cryptanalysts correctly guessed that other nations knew what America's diplomats were

---

Time -Pad Cryptographic System (G-OTP)," *Cryptologia*, 24 #4,(October 2000), 324-332..

[39] TNA/PRO HW14/8, "The Director (Personal)," November 15, 1940. Yardley had led the American codebreaking Black Chamber after WWI. After it was closed in the late 1920s, Yardley published a book revealing many of its crypto-triumphs.

communicating.

From Consensus to Suspicion

Unfortunately, by the time Driscoll's German Atlantic group began its work harmony had turned into discord--at least among America's crypto and intelligence agencies. Within days of its formation, the OP-20-G Atlantic problem's team became a behind-the-scenes but important participant in heated conflicts over the proposed British and American cryptologic exchanges--ones that Laurance Safford soon condemned as a "sell-out" by the Roosevelt administration. Britain's negative response to a request the American Navy sent to in England in July 1940 may have shaped Safford's attitude. The navy asked for virtually all information on Britain's own naval communications and cryptologic systems, as well as for all it then held on German and French devices and codes. Important, Safford's request was on a non-reciprocal basis because the Americans then felt they were not allowed to share their secrets with Britain.[40]

---

[40] NARA, RG38, CNSG, Inactive Stations, Box 54, 3200/1, GCCS Cryptology, General, Kirk to Sir Archibald Carter, July 9, 1940. "Notes on OP20G" (supplied

However, the initial September 1940 American army-navy meetings had begun with optimism and congeniality. The cryptanalysts then believed that Britain was offering full information on Axis and Soviet systems. The Americans agreed among themselves to provide some information about foreign systems but concluded they were not to reveal the secrets of their own nation's communications structures. Both services were willing to exchange intercepts with the British, and mutual respect and a desire for consensus suppressed an explosive issue, at least for a time.[41] William Friedman's army codebreakers, who then

---

by R. Erskine) written British crypto-visitors include the observations that when Driscoll discovered a joint 1943 British-American effort against the new Japanese naval attaché enciphering machine, Coral, she declared that ‘someone should be court-martialed’, indicating that she continued to have, as did Safford, a deep dislike of any work with the British codebreakers.

[41] NARA RG457, HCC, SRH391, "U.S. Cryptologic History: American Signal Intelligence in North West Africa and Western Europe," by George Howe; 'Chronology’ Op. cit. ;TNA/PRO HW14/45 , ‘to CSS’ November 26, 1941.

dealt mainly with diplomatic systems, were anxious to share all their cryptanalytic successes and failures. However, the inter-service group recommended that any disclosure of methods await specific agreement by Laurance Safford and the naval communications hierarchy.

The navy's approval did not come. Safford and his boss, Leigh Noyes, the Director of Naval Communications, refused to reveal any cryptanalytic conquests, including the imminent one the army would consider its own, the defeat of Japan’s diplomatic cipher machine, Purple.

Noyes continued to voice his objections through October 1940, protesting even when pressures from the Secretary of War were propelling Friedman's group to take an independent course and when the Secretary of the Navy made more than suggestions that OP-20-G's cooperation was expected.[42]

Although he tried, the discontented Noyes was unable prevent a

[42] 'Chronology’ Op. cit.; NARA RG457, HCC, NR6565, Box 1413, 'Sinkov Papers’; TNA/PRO HW14/8 'to Hopkinson’, November 5, 1940.

higher-level commitment to the 'exchanges.' In November, a final promise was made to send American codebreakers on a mission to England. The cryptanalysts were quickly informed. The army's team, to be led by William Friedman, responded immediately. His men drew up a complete gift-list. Hardware had a prominent place on it. Copies of the Purple machine which were under construction (using navy funds and facilities) were to be included in the over one-half ton of equipment and papers that divulged American world-wide military and diplomatic cryptanalytic capabilities.[43] There was an underlying expectation of full reciprocity, although the army composed a detailed schedule of what they sought from England.

The Navy Resists

---

[43] One of the first of those army gift-lists, of October 25, 1940, contained some intriguing phrases, ones which suggest that the navy had decided to give only minimal cooperation. Appended to several of the items was the mention that the navy had supplied them. This also suggests that the army was in the lead on the project and was dragging the navy along. Memorandum to Assistant chief of Staff-G-2, October 25, 1940.

The navy's intelligence group responded differently. First, the head of the naval intelligence division informed the British that he and the army demanded (despite the higher-level promises) an unambiguous answer to what was meant by the phrase "pretty free exchange" in the latest descriptions of the intentions of the British codebreakers. He firmly stated that unless there was a guarantee of complete exchange with regard to Italy, Germany, Japan and Russia the army, as well as the navy, might withdraw. He went further. Even if the British made that guarantee, he said, the navy was not going to send any of its cryptanalysts on the exchange trip. The excuse, a quite thin one, was that the navy had no one available. The navy was resisting involvement in what it considered a politically motivated operation.[44]

Unknown to the navy's highest officials and to the White House, the British codebreakers did have reservations–despite the desires of their political leaders. They were not planning to reveal all--unless

[44]TNA/PRO HW14/8 November 5, 1940. Noyes seems to have understood that the two nations had agreed that Britain was going to supply an Enigma (perhaps two).

forced to by persistent American demands. Extremely worried that America's diplomats and politicians could not keep secrets, there were recommendations that Bletchley withhold the progress on German and Italian military ciphers from any American visitors. It was recommended that if an American expert did arrive at Bletchley, "steps [should] will be taken to steer him away from our most secret subjects." To avoid alienating America's leaders, GC&CS drafted an ambiguous message concerning the proposed exchanges. [45]

Meanwhile, knowledge of the American navy's own resistance reached the top of the United States' government--there was another immediate and strong reaction. Unambiguous orders were sent to the navy and army: The British were to be trusted; the Americans were to share all their secrets and machines; and both services were to send representatives. By mid-December, OP-20-G had to signal its compliance and raced to catch up with the well-prepared army team.

---

[45] TNA/PRO 14/45 November 22, 1940, from Major General F. G. Beaumont-Nesbitt.

'G' wanted both groups to depart together as soon as the British provided safe passage. However, the navy's acquiescence was not capitulation.

Safford remained convinced that his nation had been "sold-out" and that OP-20-G had little to learn from GC&CS. Neither he nor Driscoll expected to find much of value in England. His last minute selection of rather junior people for his team reflected that.[46] In contrast, the army quickly promoted its two top civilian codebreakers to high military rank to ensure the British would respect and trust them.[47] While

---

[46] It was not until the day after Christmas that Prescott Currier was notified that he was to go. He was not told why. The other member of the navy's delegation, Robert Weeks, was also a last minute selection. Another reserve officer, Robert Ely, a Philadelphia lawyer, had been the first choice. Ely, however, was not recalled to 'G' until late June 1941. Then, he became one of the first members of the second Enigma team formed in 1942 (see below). Prescott Currier, "My "Purple" Trip to England in 1941," *Cryptologia*, 20 #3 (July 1996), 193-. On Ely, U.S. Navy Historical Center, Operational Archives, SRH355. Op. cit."

[47] On the British view of the trip, including a mention that the Americans "would welcome" machines in exchange, and the reluctance to reveal Enigma, TNA/PRO

the men tapped to represent the navy prepared for their late January departure (unexpectedly on Britain's showpiece new battleship, the King George V), Safford fumed, perhaps hoping that Driscoll's work would, as she strongly hinted, lead to a major discovery--one that America could keep to itself and one that would provide an independent power over the German naval systems. That might convince the American policy makers that the nation had little need for further ‘exchanges’.

On the Verge of Independent Methods, She Thought

Driscoll encouraged that hope; although she had just begun her effort. She may have been optimistic out of ignorance. America’s codebreakers were unaware of the extreme difficulties that Poland’s and England's many talented codebreakers had faced for over a decade to make significant inroads into German military encryption systems.

HW14/45 December 18, 1940; November 22, 1940. On Friedman and Sinkov, NARA RG457, HCC, NR4565, Box 1413, 'Sinkov Papers’, memo of December 26, 1940. The British were concerned that American civilians were not subject to the kind of severe punishments faced by military men.

Driscoll began her effort assuming that the best German systems and enciphering machines would be only a little more complex than earlier commercial Enigmas.[48] Soon, her belief that she was confronting a rather typical enemy, a simple electric code wheel machine, and her realization that the navy would be unlikely to provide continuous help (in the form of thefts or the capture of machines, enciphering cylinders, documents, or expensive analytical machinery) led Driscoll to an historic commitment. She decided to base the American attack upon approaches that needed little equipment, little knowledge of German systems and operational procedures, and that would be as free as possible of a dependency on German communications or cryptologic errors. Her most lofty goals were to make the American attack independent of Britain and of all but intercepted messages. Important, an American attack had to be 'economical.' She and Safford did not envision the navy ever providing 'G' with expensive equipment or a

[48] NARA RG457, HCC, NR1737, Box 705, 'Enigma Conferences', cites the attack against the Swiss Enigma.

large staff.

Typically, Agnes Driscoll left few papers concerning her Enigma work. In addition, there are few mentions of her 1940-1942 projects in the technical documents and histories written by her associates.[49] There are, however, allusions to several naval Enigma attacks that she worked on after the war began. They all used ‘catalog’ methods.

Digression: Traditions and Catalogs

An explanatory digression is necessary for those of us unfamiliar with codebreaking traditions and language. Codebreakers develop their own

---

[49] Although Driscoll may have made some cryptanalytic advances before she left the Enigma problem in 1943, there is no direct mention of her and her work in the many detailed reports on Enigma methods written after the Enigma problem was turned over to a new group within OP-20-G in 1942. It is impossible to tell which of the methods described in those reports originated solely with her. See, for example, the Radio Intelligence Publications series in NARA RG38, Boxes 169-171. In addition, although a 1942 OP-20-G policy was to keep a daily war diary recording work and accomplishments, no Driscoll diaries have been found. Parke memorandum, January 6, 1942, as supplied by Robert Hanyok.

special lexicons, ones that vary over place and time. The term, ‘catalog attack,’ which was used to describe Driscoll’s anti-Enigma method, does not have a precise meaning. It does not point to specific procedures and much of its value as a descriptor has been lost. Important, various ‘catalog attacks’ were in use long before the development and application of formal statistical and mathematical cryptanalytic methods.

The term, ‘catalog attack,’ covered a wide range of methods, but all shared common elements. Some, with the help of allied techniques, allowed cryptanalysts to determine the internal nature of an enemy’s encryption machine; but the term most frequently referred to methods applied when the inner workings of an enciphering machine (such as the wiring of its wheels) were already known. With that knowledge, cryptanalysts used quite effective ways of finding some of an encryption machine’s settings for a particular message. Using infinite patience, all the settings might be identified–at least for simple machines.[50] When

[50] A German analyst claimed that he had devised a catalog attack in 1944 that could have found all the major settings for the German naval Enigma. See,

cryptanalysts found the set-ups, a message could be easily deciphered.

Catalog attacks ran from those untrained laymen intuitively understand to highly complex methods that even experienced codebreakers find hard to describe. In simple catalog attacks, the first and laborious step was to take a plain-text word that was likely to be found in any message and encipher it at every possible setting of a copy of the machine being attacked. At each encryption of what some called a 'crib', a clerk would record the results. Although the term 'catalog' was usually associated with manual methods, such as the use of file cards or paper books, by the late 1930s some mechanization had appeared.[51] Of importance, the more complex an enciphering machine,

---

(FOIA) "Report of Interrogation of Lt. Frowein of OKM/4 SKL III, His Work on the Security of the German Naval Four Wheel Enigma," 21 June 1945, as supplied by Ralph Erskine. Frowein's attack is explained in a later note.

[51] In the 1930s Polish cryptanalysts had built semi-mechanized catalogs for their sophisticated attacks on Enigma "cycles" and "females." See, Andrew Hodges, *Alan Turing: The Enigma of Intelligence*, London, Unwin, 1983, 172. NARA RG457, HCC, NR4584, Box 705, 'Bombe History' folder. The "October 11" draft

the more entries any catalog required. Various devices were invented to overcome the great problem of searching through large catalogs. By the mid-1940s, modified tabulators, film-based machines, and motorized analogs of the apparatus being attacked helped speed catalog creation, as well as searching.[52]

In one type of crib-based catalog attack, analysts inspected encrypted messages for a possible crib. When they thought a crib was located, the codebreakers tried to match its encryption against entries in the catalog that pointed to settings. A match led to a further test to see if the suspected proper machine setting produced a sensible decryption of

---

of the Bombe history indicates that the U.S. Navy had been informed of the Pole's methods after the U.S. entered the war and by at least 1943 understood how the Enigma's enhancements had undermined the Pole's catalog attacks.

[52] The term 'catalog' was most frequently used in a low-tech context. However, for various types of traditional catalog attacks the Poles had a built the cyclometer, the British constructed their "Baby," and, during 1943, the Americans built their M8 and later attached it to scanning devices. TNA/PRO HW3/64 'Squadron-Leader Jones' Section'; NARA RG457, HCC, Box 584 'M7'.

the remainder of the message—or, if it had been a useless match because of a misleading crib.

Even automation could not make a traditional catalog attack cheap, timely, or error free. Simple versions of early Enigma-type machines, with only three wheels and no letter-changing plugboard, called for nearly 120,000 catalog cards for just one crib.[53] Even when a catalog was tabulator-based, looking through it was a time consuming and mind-deadening process. (A full catalog for the naval Enigma of the 1940s would have contained trillions of cards.)[54]

A significant drawback of usual crib-catalog methods was the probability of false matches. Short cribs with few letters had a high

---

[53] This is based on a hypothetical Enigma with only three wheels (total) with a possibility of six wheel orders and approximately 18,000 starting positions of the three wheels. A plugboard (stecker) would have added perhaps over a hundred million more.

[54] Statisticians of the 1990s were still debating how many combinations, with higher estimates replacing older calculations. See, Ray A. Miller, "The Cryptographic Mathematics of Enigma," *Cryptologia*, 19 #1 (January 1995), 65-.

probability of pointing to incorrect settings. However, it was very difficult to find long suitable cribs. Furthermore, a great and fundamental burden of a crib method was the difficulty of telling if the crib was present in a message. How could one know that DXCETBY, for example, really was the encryption of the word, ADMIRAL? Analysts could only know that through intimate and up-to-date knowledge of the communications system under attack; and, that was what the American navy and Agnes Driscoll did not and might never have. [55]

Applying the Proven

There were many levels of sophistication and power in catalog attacks. Some, like one the British explored as early as the 1930s, went beyond the brute-force test of rather obvious cribs, and approached being a ‘statistical’ attack. The British based that early method on the use of a single letter, the one most frequently used in German text, 'E'. An ‘E’

---

[55] By December 1941 the interception of German U-boat traffic by the Americans had improved and they were using traffic analysis Robert Louis Benson, *“A History,” Op. cit.*, 46.

catalog was also close to being a method of plain-language recognition, but not quite.

In a full plain-language attack, the codebreakers ran an intercept through all possible encryption settings. At each setting, the analysts examined the decryption to see if its content matched the known statistical distribution of letters or words in an enemy's language. If the distribution reached a scientifically determined probability threshold, the analysts identified the setting as a candidate for the proper machine set-up.

Although a crib-free, plain-language method was attractive, such an independent and ‘scientific’ or ‘statistical’ attack was a technical impossibility in the 1930s and early 1940s. It demanded machines with very complex and very fast circuitry. Such technology did not exist and would not for many years. The British had longed-for but could not envision building such a sophisticated device in the mid-1930s. The American navy's attempt at a plain-language anti-Enigma device constructed during the last years of World War II, the Bulldozer, had to rely on much experimental electronic and electro-mechanical

technology, and even then, it was only minimally useful. The American army codebreakers' mid-1940s high-technology attempt also had limited results.[56]

The letter 'E' catalog was a compromise, but still a demanding one. Analysts had to match intercepted messages to the strings of

---

56 NARA, RG457, HCC, NR4645, Box 600, 'Cryptanalytic Equipment for Enigma Problems--Bulldozer'. Ferner and Small of the army's SIS worked on the mathematics and logic of a multiple high-frequency letter attack for the huge 003 relay bombe. NARA, HCC, NR3175, Box 1009, "Cryptology of the Yellow Machine, 11-1-43, Capt. Roy Johnson," 45; Lee Gladwin," Bulldozer: A Cribless Rapid Analytical Machine (RAM) Solution to Enigma and its Variations," *Cryptologia*, 31,# 4,(October 2007), 305. The formidable challenge of a plain language attack on Enigmas simpler than the one used by the German navy is illustrated in the article by Heidi Williams, "Applying Statistical Language Recognition Techniques in the Ciphertext Only Cryptanalysis of Enigma," *Cryptologia*, 24 #1 (January 2000), 4-17. The article shows that although using 1990's techniques and fast microcomputers, Enigma remained a major challenge. The article also includes a useful list of works on modern plain language techniques.

already enciphered 'Es,' a time-guzzling task because they had to test entire messages against the master strings. Then, the cryptographer had to identify the places, if any, where an adequate number of matches occurred. The longer the strings being matched the more reliable the test of adequacy. However, long strings presented a techno-challenge when technicians attempted to automate the process. Scanning technologies, even sophisticated film based versions, were imperfect.[57]

There were other advanced cryptanalytic methods emerging in the 1930s. Driscoll may have taken some steps to extend the reach of various statistical procedures, such as those the army's William Friedman had formalized. Those were quite different from traditional catalog attacks. She had previous experience, for example, with the

[57] In the case of Enigma, the absence of ‘E’ might be tested because the Enigma never allowed a letter to be encrypted as itself. On ‘E’ tests, TNA/PRO HW14/45 'Copy to Denniston' December 12/13, 1941, [from Hastings]. When first researching Driscoll’s efforts it was thought that she may have explored an ‘E’ attack in mid-1941 because she was a compiling frequency statistics. However, it now seems that the American ‘E’ came much later and was probably the product

Index of Coincidence and she had probably used such techniques to understand how enciphering wheels were wired and where they were placed in encryption machines--at least in basic versions of the devices. By the late 1930s, after years of hesitation, she had also become accustomed to using tabulating machines and by then saw them as invaluable to code, if not cipher, breaking.

However, the best evidence points to Driscoll placing her faith in her versions of the more familiar 'catalog' techniques; but Agnes' were ones much less understandable than the intuitively obvious simple crib or plain language attacks. Her favored 'catalog' method had always relied upon the creation of a huge and complex file of code wheel output (for individual wheels and combinations of them) so that an analyst could search for which wheel combinations and initial positions could have (or could not have) produced sequences of pairs of enciphered-plain text letters. Such a catalog could answer, with much labor, what machine set-ups could produce a crib-text series like A-C, then B-O, then X-W, then Y-E, then Z-O, and then, D-K. If the chain

---

of the new Enigma team established in 1942.

was broken at any point before its end, the pathway being explored was eliminated from consideration.

Such a complex version of a catalog could be extremely useful because it was not bound to a single crib--but it demanded the application of much tedious analysis and labor-intensive and very time-consuming searching.[58] Even its compilation required enormous resources and much mind-numbing effort.

In the last months of 1940, and during the first quarter of 1941, OP-20-G did not have the crypto-essentials for building such a complex catalog or even for a successful simple crib-based traditional catalog attack. Driscoll and her crew began their work without knowing the technical details, or even the identities, of the systems they were confronting.

---

[58] A simplified catalog method that may have begun under Driscoll called for almost one million entries and would have demanded days to search for just one 'key'. See NARA RG38 Radio Intelligence Series , Box 170 RIP 605 #5, "HYPO–General Nature and Projected Use," Ely, March 1943 and 605 #5, articles on the letter 'E' methods.

They Almost Came Home Empty Handed

In early 1941, just as Driscoll's group was launching into its daunting tasks, the two OP-20-G officers selected for the GC&CS exchange mission, Lt. Weeks and Lt. Currier, boarded the King George V for what became a several weeks stay in England.

Prescott Currier had been a noncommissioned officer, after that, a civilian employee at 'G'. Then, in December 1940, the navy recalled him to active duty. He continued to work with Driscoll on JN-25, although he was in charge of efforts against other Japanese problems. He was especially valuable because he was fluent in Japanese. However, neither he nor his naval traveling partner, Robert Weeks, was mathematically trained, and neither considered themselves polished cryptanalysts. Another reserve officer with a mathematical background, who would play a major role in 'G's' future rounds of German naval work, Robert B. Ely, had been assigned to the exchange team, but Weeks took his place at the last minute.[59]

---

[59] Currier went on to have the responsibility for many important Japanese

Weeks and Currier regarded their army partners on the exchange trip as the true, deeply experienced, crypto-professionals. They were only partially correct. For example, the army had scheduled America's most practiced codebreaker, William Friedman, to go but at the last minute, he became 'ill' and the electrical engineer, Leo Rosen, who had recently joined the army's crypto team as a civilian employee, replaced

---

systems during World War II. Weeks left 'G' for a long and significant naval career. See, NSA, Oral History Collection, OH-1972-02, "CAPT Prescott Currier, USN, Ret.," and, Prescott Currier, "My "Purple" Trip to England in 1941," *Cryptologia*, 20 # 3(July 1996), 193-. Currier was not, it seems, asked any questions about the trip to England during the NSA Oral History interview. There are some hints that Ely was the first in OP-20-G to formalize ideas for an American bombe during 1942. NARA RG38, CNSG, Library, Box 104, 5720/205, "American Cryptanalysis of German Naval Systems," 7 July 1944, states that Ely, assigned to the task by Raven just after Pearl Harbor, designed a bombe-like machine on his own. This is a puzzling statement because of the March 1941 visit by Weeks and Currier, Driscoll's previous knowledge of the Bombe and because Turing's report on Enigma was sent to the American's in late 1941..

him. The second man, ‘Abe’ Sinkov, who had been with the group for a decade, was also a civilian. He was one of the young men Friedman hired when he created the army's revamped cryptologic branch in the early 1930s.[60] However, neither he nor Rosen had significant experience with German military systems.[61] In fact, none of the army's codebreakers had yet spent much time on any German army or air force challenge.

Although they did not have the impressive crypto-credentials of a Friedman, the British gave the four Americans the best they could offer. They elegantly housed them a few miles from GC&CS's headquarters at Bletchley Park. The mansion of the president of the Anglo-American Oil Company (he was also a director of the Suez Canal Company)

---

[60] TNA/PRO HW14/45 'to Denniston' January 12, 1941; NARA RG457, HCC, Box 1413, CBIB22 AHA 100b, 'For Adjutant General’, January 24, 1941.

[61] However, the SIS team was part of the international cryptologic community and had contributed to major works in the field. They, like Driscoll were aware of the earlier commercial Enigma. Rouse Ball, *Mathematical Recreation and Essays*, New York, MacMillan, 1939. Andrew Hodges, *Alan Turing: the Enigma*, New York, Simon And Schuster, 1983, 163.

became the Americans' home. A stenographer was at hand and the mansion's staff made sure that food rationing was not a problem. All that was luxurious compared to the stringency faced by the British stationed at Bletchley. Throughout the war, they faced shortages of everything. A pencil sharpener was rare; paper was scarce; copying equipment was on the dream list; and, their temporary wooden buildings, the Huts, were near primitive. Many of the staff were billeted to the cramped homes of local residents.

To hide their links to the United States, which was not yet at war, the four Americans wore civilian clothes. The British assigned two large automobiles and drivers to them. There was an important reason for two cars.[62] Reflecting the legal and bureaucratic separation of the American army and navy's crypto-services and, perhaps, difference in the promises the British had made to them, the army and navy teams

[62] TNA/PRO HW14/9 'from GC&CS', December 20, 1940; Prescott Currier, "My "Purple" Trip, Op. cit.

traveled separately.[63]

The Americans did feel welcome. Moreover, they thought the British were fulfilling all promises. That was not quite true. The original British enthusiasm for openness had diminished as security considerations reemerged. The Americans were unaware that permission to learn of Britain's Enigma capabilities had been withheld until, literally, the last days of their scheduled stay. They were also unaware they had been shown through technical centers only, not ones producing operational knowledge.[64]

---

[63] TNA/PRO HW14/45 'to Travis', February 1, 1941.

[64] TNA/PRO HW14/9, February 24, 1941; HW14/12 February 24, 1941; HW3/93 'C to Churchill and return', February 26-27, 1941; HW14/45 'Weeks to Commander Denniston', March 3, 1941. There have been varied dates given for the length of the Americans' stay. The PRO documents, especially the one cited below concerning the behavior of one of the army's team on the return trip to America, suggests the departure date was close to March 5, 1941. Weeks signed his pledge March 3, 1941. The date of the report of the American's behavior on board the return ship, in conjunction with the date on a receipt for documents received by Weeks dated March 19, 1941, indicates that OP-20-G communicated

They came close to boarding their homebound ship without learning of the methods of attack against Enigma and some other major Axis military systems. They almost missed learning of the existence of the Bombe! In addition, what they finally did see was not as impressive as would be imagined from the post-1970's common image of the famed Bletchley Park of 1944 and 1945.[65]

Nevertheless, they learned enough to prevent them from thinking that their hosts were not honoring any earlier agreements. Prescott Currier concluded that reciprocity was fulfilled and that the trip was more than worth the dangers he had faced when a German aircraft attacked his ship in the English Channel. At the end of his weeks at GC&CS, Currier thought he had been "shown everything"--and that the

---

about secret materials with Bletchley during the early months of 1941.

[65] A thorough yet non-technical description of the methods used at Hut 8, including Banburismus and the Bombe is : NARA RG457, HCC, NR4685, Box 940, “The History of Hut Eight, 1939-1945,” by A P. Mahon. It is a remarkable and highly valuable document.

exchange had been open and equal.[66]

In turn, the British felt that Purple (the machine used to read Japan's diplomatic messages) was highly valuable and soon began to think that the demeanor of Currier and Weeks indicated it would be safe to reveal Bletchley's greatest secrets to OP-20-G. On the day the Americans were first shown the Bombe, Bletchley's operating head, Alastair Denniston, wrote to the leader of British intelligence, "C," that, "Complete co-operation on every problem is now possible and we are drafting plans for its continuity when they return to U.S.A." [67] The British began developing a system for special telegraphic communications and courier services to link liaison officers.

---

[66] Joseph Wenger later concluded that the British had been forthcoming in this period. See the discussion below. NARA RG38, 'Wenger Memorandum for OP-20-G' May 13, 1944, as supplied by Ralph Erskine.

[67] TNA/PRO HW1/2 'To Director', 3-3-1941. Also relevant is, David Kahn, "Britain Reveals Its Bombe to America From the Archives," *Cryptologia,* 26 #2, (April 2002), 50-54.

Knowledge Without and With Restrictions, and an American Secret

The American army and navy teams had transported a great deal to England. They presented copies of the Purple machine, methods to attack other Japanese codes and ciphers, knowledge of German diplomatic systems, and much more to GC&CS--importantly, without restrictions on their use.[68] The Americans also revealed, in general terms, their plans to soon build what they saw as revolutionary code and cipher breaking machines, including what they termed, "electronic" ones. Rosen, among the four Americans, was the expert on such things. He and the navy's men may have engaged in a bit of puffery about this, leading the British to expect to encounter more sophisticated machines, and more of them, than they saw when they visited the United States

---

[68] 'Chronology' Op. cit. ,September 9, 1940; NARA RG457, HCC, Box 1127, ,Robert L. Benson, "The Origins". Op. cit.; NARA RG457, HCC, NR3813, Box 1296, 'Sinkov Report'. The British did continue quite open interchanges of methods and intercepts in the Far East.

later in the year.[69]

Of more significance for the future of British-American relations, the navy's representatives seem to have kept the British unaware of Mrs. Driscoll's German naval project. In turn, the American visitors remained unaware that the British thought little of most of what the four Americans presented to them--with the exception of Purple.[70] Yet, all the 'gifts' were graciously accepted. The GC&CS staff was careful not to be too gracious, however. For example, out of fear of providing the Americans with a bargaining chip, they did not reveal their admiration for the United States' outstanding tabulator company, IBM. They did not want the Americans to know they viewed IBM as a possible manufacturer of English designed and controlled new crypto technology.[71]

---

[69] TNA/PRO HW14/46 'Denniston memorandum U. S. agencies', 1942.

[70] TNA/PRO HW14/45 'Denniston Report', September 5, 1941; TNA/PRO HW14/59 'Memorandum on U.S.', November 30, 1942.

[71] TNA/PRO HW14/45, 'to Denniston', August 5, 1941.

Bletchley's courtesies had to be restricted--at least until the importance of Purple was recognized by the government. It had taken major efforts for GC&CS to receive permission from Prime Minister Churchill to unwrap the means of attacking Enigma. Arguing that England would probably have to depend on American help in the future (especially for the Japanese problems) and that bitterness would result if the Americans learned of the Bombe and its methods after their aid was secured, a plea had been sent to London in late February to allow tours of the most secret crypto-methods huts at Bletchley. The fabled "C," had passed the request to the Prime Minister on the twenty-sixth. Churchill gave his approval the next day. That was less than a week before the Americans were scheduled to leave.

Moreover, unlike the American cryptanalytic gifts, that approval came with some severe restrictions. GC&CS was to show the visitors the new technology and methods, not the ‘results’. In addition, they were to hold as top-secret what they saw and learned. They were to describe their findings only verbally and only to only their immediate superiors who, themselves, were expected to keep the secret. The

Americans had to promise to refrain from putting the knowledge to any use before they contacted GC&CS and it gave its approval.[72]

The Right Place at the Wrong Time for the Bombes

By the third of March 1941, the American navy's men were visiting the building where Alan Turing, later to be famous as a mathematician and as the inventor of the British Bombe, was refining his attacks on the naval Enigma system. The army's two representatives were allowed into some of the Bletchley centers working on German diplomatic, air force, and army codes and ciphers. All four Americans, apparently, visited the building housing the Bombes.[73] It also contained an earlier

---

[72] TNA/PRO HW14/9, February 24, 1941; HW14/12 February 24, 1941; HW3/93 'C to Churchill and return', February 26-27, 1941; HW14/45 'Weeks to Commander Denniston' , March 3, 1941.

[73] Both Sinkov and Rosen later denied that they learned about the Bombes during the trip. Rosen went further and claimed that no Bombe information was given to the army before the SIS designed its own Bombe in 1942 . Their statements do not ring true. The transcript of NSA's Oral History interview with Rosen contains contradictions, which lead to the conclusion that Friedman's group learned much

Bombe look-alike machine, Baby, which generated Enigma encryptions at high speed for some of GC&CS's own earlier catalog attacks.[74]

Weeks and Currier spent much time with Turing. He described the naval Enigma and various related transmission systems. Although critics later stated the Americans were not given enough information,

---

about the Bombe from the British. See, NSA, Oral History Interview, OH-16-84 with Leo Rosen, 26 August 1984. Ralph Erskine has cited documents that also undermine the claim that Sinkov and Rosen were excluded from knowledge of the Bombe in early 1941. Ralph Erskine, "What Did the Sinkov Mission Receive from Bletchley Park?" *Cryptologia*, 24 #2 (April 2000), 98. In addition, the SIS' foray into the construction of a fully electronic Bombe, beginning at least as early as April 1942, and the construction of a prototype fully electronic commutator based on the British "two way" design soon afterwards, suggests that much information came from the British and /or OP-20-G. Letter to the author from Joseph Eachus, April 24, 1989.

[74] NARA RG457, HCC, NR964, 'Turing's Treatsie on the Enigma', 141. TNA/PRO HW14/45 'Weeks to Denniston', March 3, 1941. TNA/PRO HW14/45 'Report on American Visit', March 3, 1941; TNA/PRO HW3/164 'Squadron-Leader Jones' Section'.

what they were told was considerable.[75] However, they may have come away without being impressed as they might have been. If they had arrived a few weeks later, they would have encountered and taken home a brighter view of the British effort against the naval Enigma. In March 1941, the British introduced them to a developing project, not a finished effort. The Americans must have been disappointed to learn that one of Turing's most promising methods, Banburismus, then depended on capturing documents and would always require the daily interception

[75] The critics receive support from Ralph Erskine's, "What Did the Sinkov Mission Receive", Op. cit . The TNA/PRO documents he cites do not reflect the gift of enough for a full attack on Enigma but they show that Currier, Weeks and, later, Driscoll, were told much. As a result of the visit, Driscoll knew, for example, of the double turn of the middle wheel, the role of bigrams, the nature of stecker-settings and that several reflector wheels were a possibility. She thought she knew enough to proceed on her own with only a modicum of additional information from GC&CS. In addition, NARA RG38, CNSG, Library, Box 104, 5720/205, "American Cryptanalysis of the German Naval Enigma," 7 July 1944, OP-20-GY-A to OP-20-G-1.

and costly and tiresome processing of great numbers of messages.[76] Also, his description of his complex way of turning very hard-to-find long cribs into 'menus', which were needed to give the Bombes enough logical power to select only the most likely Enigma settings, might have overwhelmed the non-mathematical navy men. Turing must have mentioned that regularly finding adequate cribs was difficult.

The Bombes were, themselves, an overwhelming, if not fearsome, sight. They were huge and noisy although ingenious high-speed automatic and near instantaneous plain-cipher, comparing electro-

---

[76] Ralph Erskine, "The First Naval Enigma Decrypts of World War II," *Cryptologia*, 21, # 1 (January 1997), 42-. Ironically, the major capture that allowed the 1941 victory over the naval Enigma, the Lofoten Raid, took place on March 4, 1941 a few days before the Americans departed. A useful chronology of the captures in 1941 is in F H. Hinsley, *British Intelligence in the Second World War: It Influence on Strategy and Operations, Vol. One*, London, Her Majesty's Stationary Office, 1979, 337. A useful compilation on England's program is, Ralph Erskine and Michael Smith (eds.) *Action This Day*, London ; New York : Bantam, 2001.

mechanical devices whose metal cabinets had a forbidding look. The Bombes had complex circuitry to test matches between cribs and enciphered text. Turing may have explained that the latest Bombe was able to overcome the Enigma's letter-changing plugboard settings with more ease than the first version of the device--making it much, much more powerful than any previous crib testing methods. He would have had to admit, however, that all types of Bombes were costly and demanded extensive manufacturing facilities.

Turing would have found it impossible to avoid underlining that the German naval Enigma was, yet, unconquered.[77] He explained there

---

[77] The naval Enigma posed special problems and had been read only intermittently in 1940. The best of the available crypta-methods depended on the near regular acquisition of up-to-date documents and mistakes by the Enigma operators, as well as systematic errors such as retransmissions of Enigma messages on systems the British could read. Information from such sources did not begin to flow into GC&CS until April 1941, a month after the Americans had departed. On the chronology of the acquisitions see, Ralph Erskine, “The First Naval Enigma Decrypts” Op. cit., 42. Also useful for an understanding of the Naval ‘E’ is his, "Naval Enigma: An Astonishing Blunder," *Intelligence and*

were not enough Bombes on-site for a stand-alone attack or for successful attacks based only on errors in the use of the Enigma. The methods that allowed the expensive Bombes to work (especially in the period when only a few Bombes were available) relied, to some extent, on old-fashioned cryptologic craftsmanship, including the theft of documents. GC&CS was even planning the seizure of German trawlers to obtain information.[78]

The results from those captures, which allowed the British to read the naval system for much of the remainder of 1941, did not come until the Americans had left.[79] If they had stayed longer, they would have seen even more progress. Mid-year saw the beginning of other

---

National Security, 11 #3 (July 1966), 468-473.

[78] David Kahn, *Seizing the Enigma: The Race to Break the German U-boat Codes, 1939-1943*, Boston, Houghton-Mifflin, 1991, 117.

[79]81. The navy was informed of the breakthrough into the Naval Enigma. NARA RG38, CNSG, Library, Box 104, 5720/205, "American Cryptanalysis of the German Naval Enigma," 7 July 1944, OP-20-GY-A to OP-20-G-1.

important breaks into naval Enigma. By August, a regularized operation against it was finally in place but most German naval systems were still to be conquered.[80]

If the Americans' visit had been in April, May, or late summer, OP-20-G's representative might have carried back a very positive recommendation, one that neither Driscoll nor Safford could ignore; learn all about and use the Bletchley attacks. In contrast to the OP-20-G men's experience, the American army's Sinkov and Rosen saw a bright crypto-scenario. They learned of the long-time success against the Axis diplomatic and air force ciphers, as well of more recent entries into various German army networks.[81]

---

[80]. A. P. Mahon, Op. cit., 48. Useful on how weaknesses in German procedures aided their allies, Ralph Erskine, "Kriegsmarine Short Signal Systems—and How Bletchley Park Exploited Them," *Cryptologia*. 23 #1 (January 2001), 65-92.

[81] Although the army men may not have taken notes on the Bombe, they came away with much information about diplomatic and military systems and soon knew of the wiring of the military Enigmas. NARA RG457, HCC, Box 1413, 'General Marshall's Letter to Field Marshal of 23/12/42'.

All four visitors seem to have taken advantage of the time they had to explore the nature of the Bombes. Although crude compared to later versions, they were innovative and, at least, psychologically stunning. Currier and Weeks did not take notes, assuming that the Sinkov and Rosen, the more experienced cryptanalysts, would be much better at recording the details of the Bombes and related methods.[82]

However, the navy's representatives did not leave empty-handed or depressed. More British offerings appeared. Weeks and Currier received a paper model (analog) of a naval Enigma machine; specifications of the wiring of the machine's eight code-wheels; and, there were assurances that when enough copies of real Enigmas became available the American navy would receive one. Alan Turing supplied additional special material. Moreover, there were promises that England

---

[82] Prescott Currier, "My "Purple" Trip, Op. cit. There may have been a significant misunderstanding. Robert L. Benson, Op. cit., suggests that Sinkov and Rosen were not allowed to take notes during the visit. See NARA RG457, HCC, NR3873, Box 1296 'Sinkov Report'. Alastair Denniston, see below, did send keys to OP-20-G during 1941.

would exchange much more in the future, including information about Germany's mistakes when using Enigma systems. Lt. Weeks also carried away a large packet of documents concerning Russian, Vichy and Italian codes, German merchant marine ciphers, bare-bones documents on many German naval systems and, perhaps, some old 'keys' to allow 'G' to practice Enigma decryption using the paper Enigma they had been given.[83]

Not a Pretty Sight: The First Bombes

However, what Weeks and Currier received did not impress the American navy's chief codebreaker: GC&CS' machines and methods could not meet Agnes Driscoll's standards and vision. The trip to England had revealed that the British thought that the Enigma was not going to yield to any simple or inexpensive solution. Bletchley's Enigma attacks demanded a huge work force, and very costly

[83] Ralph Erskine, 'What Did the Sinkov Mission Receive', Op. cit.. See also, TNA/PRO HW14/45, 'List' March 19, 1941.

equipment. Even the Bombes needed much assistance. Although an engineering marvel, the Bombes were not truly electronic and not flexible enough to complete an attack on their own. Worse, because they were difficult to manufacture, there was a shortage of them in 1941. In addition, the few Bombes the Americans saw (4, perhaps 6, at most) were rather crude. The first model of the type that printed its results did not arrive at Bletchley until the end of March and that Jumbo would never be as reliable and handy as the simpler Bombes.[84] More importantly, without the support of large amounts of time, labor-intensive calculations, and cytological skullduggery, the Bombes could not overcome the trillions of possible Enigma settings.

The original electro-mechanical Bombe, with its sets of noisily whirling commutators (complex electric analogs of Enigmas' code wheels) had begun its work at Bletchley less than a year before the American's brought their 'exchanges'. The British Bombes of 1940 to

[84] NARA RG457, HCC, NR3175, Box 1009, 'Cryptanalysis of the Yellow Machine'.

early 1941 were relatively unrefined mechanisms, and GC&CS had to use them in a brute-force way for many months. A massive set of many Enigma analogs linked together, the Bombe matched a complex form of plain to cipher pairs at each of the thousands of its commutators possible positions. It did not perform an automatic test to identify the code wheels used for a message, nor for their order within an Enigma. That meant a need for a separate run for each suspected wheel combination and placement. With a minimum of sixty possible combinations and orders of wheels for simplest Enigma systems, using the Bombes alone proved overly time consuming. Furthermore, the first Bombes were not cutting-edge examples of automation or electronics. Although Alan Turing had envisioned using fast electronic tubes when he designed the device, practicalities dictated reverting to the older electrical relay technology. Another limitation of the early Bombes was that they did not automatically stop and record the commutators' positions when they sensed one of the possibly true matches between the complex 'crib' and the Bombe's output. The machine's commutators continued to spin for some time after a 'hit'. When the machine finally

stopped, its operators had to feel the relays in its circuits to identify the correct positions. Then, they had to crank it back to where it had sensed a match before they restarted it. Unless the operators did that, a Bombe might miss the next possible ‘hit’.

That original Spring 1940 machine, which had taken several months to construct at Britain's tabulator company, BTM, was not very efficient at testing for the setting of the Enigma's ‘stecker board.’ The ‘stecker’ (a plugboard) vastly increased the number of combinations that had to be eliminated to find a correct machine setup. It was not until August 1940 that BTM delivered a Bombe with a very important automatic test device, the ‘diagonal board’. That board helped turn short or weak cribs into much stronger and more discriminating ones.

Furthermore, the British put that new Standard Bombe to work on air force, not naval, traffic because they knew enough about the air force's systems to make the bombe operationally useful.[85] Unfortunately, even the Standard was slow. Britain’s engineers had to restrain the

[85] TNA/PRO HW3/164, 'BP Bombes'.

speed of its some thirty spinning commutators because the electrical relays that sensed a hit were quite ‘sticky’ and sluggish.[86]

The GC&CS’ experts may have told the American visitors that the first Bombe had taught GC&CS many lessons about the limits and expense of cryptanalytic technology. For a while, Bletchley had to run the Bombes against most Enigma code wheel combinations and placements. That proved much less than efficient and the British realized the consequences of the Germans increasing the number of wheels for use in Enigmas, or adding new communications networks: the combinations to test would amount to the unmanageable level of thousands per day.

In 1940 and 1941, running just sixty wheel combinations was too much for GC&CS. With set-up times included, each Bombe run took almost one hour. Even though the later Bombes tested as many as three wheel combinations at once, without Alan Turing's amazing logical tricks with cribs, his Banburismus, and a steady flow of long and

[86] Later Bombes had 3 banks of 36 wheels and could run three jobs at a time.

reliable suspected words, the Bombes could be of limited help against the German navy's advanced systems.

A Demanding Scientific Aid

The modern statistical Enigma attack Turing devised, Banburismus, was also expensive and dependent. However, since late 1940 it had seemed that Banburismus would become Bletchley's savior. While his colleagues were besieging the government for the funds needed to build at least five dozen more significantly improved Bombes (and calling for the takeover of BTM, Britain's version of IBM) Alan Turing had been putting the finishing touches on the ideas for his method to reduce the number of wheel combinations that had to be tested on the Bombes (or by hand-methods) by as much as a factor of ten.[87] Some hoped they

[87] TNA/PRO HW14/8 'Need for Spiders', November 20, 1940; TNA/PRO HW25/1 C.H. O'Alexander, "Cryptographic History of Work on German Naval Enigma," 1946. Bletchley used its own non-Bombe crib-letter/cipher letter catalog attack once the stecker and probable wheels had been identified and when no code wheel turnovers were expected, NARA RG457, HCC, NR3175, Box 1009, 'Cryptanalysis of the Yellow Machine', 79. The American army used a

could turn his advanced method into a substitute for the Bombes.

Banburismus, although sophisticated, demanded much human and tabulator time. Its powers depended on the knowledge of the codes (bigrams) the Germans used to help tell each other how to set up an Enigma for a message. Changes to them threatened disaster because they were so complex that even Turing's crew had been unable to deduce them until mid-1941. Much else made the early 1940's Banburismus a less than sure-fire and proficient attack. Alterations to other German procedures, or to the Enigma itself, would have made it an impractical if not useless method.[88] It was also a resource-devouring

---

similar attack later in the war. NARA RG457, HCC, NR2136 Box 782, "Group II Machine Catalog."

[88] It would prove ineffective against the new "four wheel" naval Enigma. Additionally, the method took so much time that by mid 1943 it was thought best to shift to a reliance on more Bombes and the enhanced knowledge of cribs. However, Banburismus was used through, at least, 1943. TNA/PRO HW25/1 C.H. O'Alexander, "Cryptographic History of Work on German Naval Enigma," 1946. A. P. Mahon, Op. cit., 22, 31, 48, outlines Banburismus' use and states

approach. The method needed several hundred of a day's messages sent on an Enigma system under attack. Those messages had to be recorded on a medium that facilitated running each message against all others while calculating statistics (much like those of Friedman's Index of Coincidence analysis) at each step. Without high-speed electronic machines, that required dozens of people and the use of many tabulators.[89]

Banburismus was not even in full swing when the Americans visited Bletchley in early 1941 and it remains unknown if their hosts

---

that the bigram tables, which super-enciphered the Enigma indicators, could be deduced on a regular basis after mid-1941 through information gained by other means of attacking the systems such as “EINSing..”

[89] A . P. Mahon, Op. cit., 20, also explains how it became more economical to add Bombes rather than continue the use of Banburismus. In the United States, the navy had Vannevar Bush design a optical-electronic machine for its IC testing, the Comparator, which ran messages against each other. A readable description of Banburismus is found in, Hugh Sebago-Montefiore, *Enigma: The Battle for the Code*, London, Weidenfled and Nicolson, 2000, 328-335.

told them of the failures of other Enigma attacks. It is unlikely that the British reviewed the entire list of methods they had examined but found valueless.

A Too Secret, Secret?

The four Americans visitors let the British know they valued what they had learned. They signed ironbound oaths of secrecy just before they left for the United States in the first week of March 1941. They were pleased with the way GC&CS's had treated them, and Britain's crypto-leaders thought they had achieved their own goals.

However, trouble came, immediately. It was over what had been one of the major reasons for Britain's hesitancy to reveal anything about their 'Ultra' secrets, security.[90] British intelligence quickly informed GC&CS that one of the men from the American army's team, despite his oath, talked about his work so much on the British ship to Scapa that its officers knew what he had been involved with during his visit to

[90] TNA/PRO HW14/13 'intelligence to Denniston', March 10, 1941.

England. Security problems continued. In the next months, there were incidents that made the British regret opening Bletchley's doors. For example, GC&CS received a letter in plain language from the American army asking for a Bombe although, the British thought, they had an agreement never to put such things to paper.[91] The American State Department was regarded as a an intelligence 'sieve' and when a long newspaper article appeared describing the plans of the head of the American OSS to start a new intelligence/covert operation in England,

[91] Ralph Erskine believes that the June 1941 request for a Bombe may have come from OP-20-G. Driscoll's refusal in August, Safford's later statement that 'G' never wanted a bombe, and the many attempts by the SIS to launch its own Bombe and other Rapid Analytic machine programs ,well before it could even intercept German messages, helped to convince this author that the request came from the American army. This is supported by the Denniston memoranda concerning the visit with Driscoll. The army's electronics man, Rosen, was well aware of the need to speed up the Bombes in spring 1942 and was regarded by the British as America's expert in applying electronics. On Rosen as the expert, From Travis, for OP-20-G from G. C. & C. S., 13 May 1942, as supplied by Robert Hanyok.

"C" and his subordinates began to push even harder to prevent the Americans from doing anything with European crypto systems except technical "research."[92]

Keeping Some Promises and Keeping America in Its Place

Britain's needs helped overcome some its qualms. American aid was too valuable and its navy was too involved in the Atlantic for the British to cast aside Anglo-American intelligence cooperation. GC&CS decided to continue to fulfill all its promises. It responded positively to 'G's' request for recent Enigma settings (keys) in late May and early June 1941, although that request suggested the Americans were doing

---

[92] TNA/PRO HW1/6 'C to Prime Minister', June 24, 1941. The security concerns ran deep. Churchill wanted to inform the United States when it was known that U-boats were stalking American ships on a regular basis but "C" could find no possible way to do that. The Germans and Americans would know that such information came from Enigma radio messages. The American army's written request for a bombe and fears that it might pass on Ultra information to the State Department were also deeply worrisome. On relations with the SIS, HW14/45 'Denniston report', app August 5, 1941.

more than research.[93] Then, Bletchley did not protest when the Americans' finally let it be known they had begun work on the German naval systems–a decision that seems not to have been preceded by a prior notification.

'G's' July 1941's follow-up requests for more on Enigma and other Axis systems took some time to fulfill as the Germans had changed some of their procedures. GC&CS sent OP-20-G what Enigma keys it had and even sent a copy of the bigram tables that were vital to determining the indicators for Enigma setups. The Americans also received hints that a permanent entry in the naval Enigma was close-at-

[93] As supplied by Stephen Budiansky, RG38 "Washington and E. Traffic, Notes on Correspondence," nd. On materials sent to America, TNA/PRO HW 14/45 "D.D.M.I." July 8, 1941. There were continued security breeches, even by the American cryptanalysts. See, TNA/PRO HW 14/45, Denniston to Hastings, November 5 and 6, 1941. OP-20-G announced that it had begin its operations against Enigma in late May 1941 and in early June signaled that it was attacking one system. GC&CS responded with approval and sent requested information.

hand.[94] In addition, there was a flow of information about Japanese systems. There was one critical request the British cold not fulfill: they did not have copies of the requested physical Enigmas to send to America.[95]

---

[94] The German navy was in many ways more prudent than the other Axis services in its Enigma procedures, one reason for the difficulty of an attack on its Enigma. However, by late summer 1941, there were signs that the increased number of Bombes would compensate for that. For some examples of the German navy's infrequent but important lack of prudent use of its systems, Ralph Erskine and Philip Marks, "Naval Enigma: Seahorse and Other Kriegsmarine Blunders," *Cryptologia*, 28 #3, (July 2004), 211-241.

[95] The 'when' of GC&CS' fulfillment of all of the request for "all future German traffic on A. and all Steckers and keys not previously forwarded, " and much else, became central to the late 1941 disagreements discussed below. See, as provided by Stephen Budiansky, NARA RG38, Op. cit.; and. TNA/PRO HW14/45, 'list of items requested', and "Has series "A" anything in common with series "B." As late as mid-1942 GC&CS, was still making inquiries about sending an Enigma when enough were captured. TNA/PRO HW14/47, 'to Tiltman', June 6, 1942. The British were not trying to deceive the Americans by withholding a copy of

Despite Britain's cooperation, frictions continued, with both 'G' and the American army's code men. Soon, GC&CS dispatched its headman to Washington. Commander Alastair G. Denniston's mid-August 1941 tasks were to coordinate, appease, and control. A first step was to convince Friedman (at the Signal Intelligence Service, SIS) that England had no Bombe to spare and to prevent him from turning to the IBM factory to build one.

Another goal was to persuade the SIS' staff members that their efforts on European military work were currently unnecessary. England, Denniston claimed, would tell of methods and supply information as soon as the American army had any real European involvement. A last-gasp tactic England contemplated using, in order to mollify the army, was to offer to have some of SIS' mathematicians visit Bletchley. That would allow the Americans to feel part of the system and to save face.

---

the 'E' machine. Ralph Erskine has determined that GC&CS had no spare copies of Enigma during 1941. See, Ralph Erskine, "The Holden Agreement on Naval SIGINT: The First BRUSA?" *Intelligence and National Security*, 14 # 2 (Summer 1999), 196, fn 7.

Denniston hoped that he would not need to make that offer because there were deep security fears concerning the mathematicians the army might select.

Denniston's positive objective was to coax Friedman's group to concentrate its energies and, he thought, its vast technological resources on Japanese systems. However, he was surprised and disappointed after he toured the SIS' headquarters. It contained few tabulators, the Americans were not using them efficiently, and there was no sign of the more advanced machines that the Americans had alluded to in earlier communications.[96]

That disappointment was counterbalanced by what Denniston considered tobe SIS' acceptance of "advice" on European systems, a commitment to concentrate on Japanese problems, and its cancellation

---

[96] TNA/PRO HW14/45 'Denniston Report', September 5, 1941. At the time of the Denniston visit, Britain's army and navy codebreakers were in their old cramped headquarters. They had no room for new machines and were just beginning to order new equipment. Neither had moved to the large girls' schools they used for the remainder of the war.

of the request for a Bombe. As important, was ‘attitude’. Denniston came to consider Friedman's team as "our friends" who wanted to learn from and cooperate with (be subordinate to) GC&CS's codebreakers. Moreover, Denniston now concluded that Friedman was the real force in American cryptanalysis. Another result of the meeting was that Friedman and Denniston became close friends.[97]

A History-Making Rejection

In contrast was the outcome of the August 1941 meetings with the crew at OP-20-G. At the army's center, Denniston offered little and got much; at the navy's, he offered a path to his greatest prize and faced what was a

---

[97] On Denniston and the SIS: TNA/PRO HW 14/45 ‘Memorandum of August 5, 1941, “dear Eddie’ October 9, 1941, and ‘Hay Adams Stationary’ August 14-18, 1941. David Alvarez, *Secret Messages: Codebreaking and American Diplomacy*, University of Kansas Press, 2000, 119. Some background on Denniston is in, Robin Denniston, *Thirty Secret Years: A. G. Denniston’s Work in Signals Intelligence*, 1914-1944, Polperro Heritage Press, Clifton-upon-Teme, Worcesteshire , 2007.

near insult to GC&CS' capabilities.[98]

After Prescott Currier escorted him through OP-20-G's offices, Denniston met with the leaders of the naval communications section. He agreed to furnish more information on French and Italian systems and he established more procedures for secure communications with England.[99] A few days later, he had an intense meeting with Laurance Safford, probably admitting the American navy deserved special cryptologic consideration because its ships were virtually "at war" in the Atlantic.[100] Nevertheless, Denniston continued to press for a reaffirmation of what he believed the Americans had promised: to do

---

[98] On the visit with Driscoll, TNA/PRO HW14/45, 46, 'Denniston Reports', of September, October and December 1941. Especially, December 2, 1941. On rejection of the bombe see, also, Dundas P. Tucker, Op. cit. On the perceived attitudes of Safford and Driscoll, TNA/PRO HW14/46 memorandum of February 15, 1942 and HW14/45 'Hastings to GC&CS', December 12, 1941.

[99] TNA/PRO HW 14/45 'Notes on Conference Held August 14/15, 1941'.

[100] TNA/PRO HW 14/45 "Interrupted Conference with Commander Safford," August 18, 1941.

nothing more than “research” on European naval systems.

Denniston withheld voicing complaints about the information Currier and Weeks brought from England having been revealed to others besides Safford. When Denniston talked with Agnes Driscoll, it was clear that she had been privy to the secrets revealed to OP-20-G in mid-March. She must have been using the knowledge of Enigma’s wheel wirings, Denniston concluded, and she seemed informed of the Bombes and even Banburismus.

That did not anger Denniston too much. However, he was shocked when Driscoll announced that the American navy did not want a Bombe; did not want to use the Bombe; and thought little of the other British anti-Enigma methods Turing had revealed. Driscoll declared she had devised a far better approach. With a bit more work, she said, it could become operational. It was, she claimed, much simpler, demanded much less material than the Bletchley attacks, and would be better able to withstand changes in the Enigma systems. It would only need a few daily messages and very short common-word cribs–not the hard to find special ones the Bombe required. As well, the method did

not requite any revolutionary machinery. Driscoll emphasized that her attack was more effective than others in dealing with the problem of Enigma wheel turnovers after an operator encrypted only a few letters.

She showed Denniston a sample solution based on a short eight-letter crib. She believed that with less than two dozen people using her soon-to-be completed catalog, settings could be found within a few days.[101] Those were grand claims given Britain's need for hundreds of people and very expensive machines to penetrate Enigma systems.

Denniston remained composed--even though he felt insulted and although GC&CS' desire to control the Enigma problem was under threat. He could not dissuade Driscoll although he knew that GC&CS had made the great breakthroughs that were finally allowing a relatively constant reading of the naval Enigma.[102] He offered to provide more information about the Bombes and Turing's methods–to no use. His

---

[101] TNA/PRO HW 14/45 'Denniston to Safford' October 1, 1941.

[102] A. P Mahon. Op. cit.. This author believes that Safford and Driscoll knew of the successes against naval Enigma in 1941.

offer to give more about such things as the statistical Banburismus received a cold reception. He was willing to supply ‘G’ with a Bombe when one became available-- but Driscoll certainly did not request one.

Driscoll did not seem to listen as the prestigious visitor continued trying to convince her to drop her new ‘catalog’ work. Denniston explained that GC&CS had explored the same letter-pair catalog approach years before, unsuccessfully.[103] In addition, he may have cited Alan Turing's reasons for not relying upon an 'E' catalog, and why he dropped his plan to build an electrical machine fast enough to make a full ‘E’ attack worthwhile. He may also have explained why GC&CS was turning to a catalog variation using the word EINS--it was a less powerful but practical crib for secondary tasks that did not require much

---

[103] Britain, France, and Poland seem to have already explored most alternatives of the era. The Poles had used catalogs in various forms (their bombe was a version of an automatic catalog) but the changes in the use of the plug-board Enigma stecker invalidated their catalog attacks. NARA RG457, HCC, Box 705 'Bombe History' folder. Britain had used or explored many methods, including attempts at an ‘E’ catalog, a digraph catalog, and a plain language attack.

scanning or calculation.[104] Denniston may well have described the downfall of some of the attacks using the embedded indicators of Enigma machine setups.

He stressed that most catalog methods, when facing an adversary like the naval Enigma, could not solve enough of the machine's settings.[105] Like an 'E' catalog (and the EINS version) they might be

---

[104] On EINS A. P . Mahon, Op. cit., 21.

[105] A startling document has emerged in the TICOM materials searched by Ralph Erskine. TICOM-I-38 "Report on Interrogation of Lt. Frowein of OKM/4 SKL III, On His Work on the Security of the German Naval Four-Wheel Enigma," June 21, 1945. Frowein had been assigned to check the security of the naval system in the summer of 1944 after the German naval authorities discovered a suspicious pattern of U-boat sinkings. In his interview with allied investigators he claimed that he had found a method to read the four-wheel Enigma using rather traditional methods of determining the fast-wheel, then, using a large catalog of, the other settings of a machine. As a result, the Germans ordered that only double turnover wheels be used in the fast position because his method would not work with a multiple turnover wheel in the fast position. However, his method demanded a very long crib, an enormous catalog (some 4,000, 000) entries and

useful as ‘locators’ to find the starting positions of Enigma wheels once it was certain that the correct wheels, their internal wiring, their order in the machine and the steckers (plug-board settings) were known. Like the 'EINS' and the 'E' catalogs, any simple catalog methods were too weak to stand by themselves. He emphasized that only the Bombe, aided by strong and complex crib ‘menus,’ by labor-intensive methods such as Banburismus and by the exploitation of German procedural errors, could penetrate Enigma in a timely way.

Agnes Driscoll bent a little. She admitted that she was somewhat "stumped" in her quest to fully understand the Enigma. She had been unable to build a fully working Enigma from the paper analog and the other documents Currier and Weeks had brought to America. She voiced frustration over the double turnover of one of the Enigma code wheels. Then, she forcefully demanded clarifications of how it and a number of other Enigma components worked.

---

forbidding amounts of human and tabulator time if it was to be turned into more than a theoretical exploration.

Denniston agreed to her demands, without hesitation. He promised to send responses to all her questions and asked her to compose a list for him. He also promised to forward relevant codebooks when they were available. He pledged that a working naval Enigma would be sent when possible.

A Crypto Cold Shoulder

Following that, Mrs. Driscoll turned down an invitation to come to England to learn more about the British methods--as well as to inform GC&CS about hers. A visit was out the question, she said. Her auto accident made such a voyage impossible. She did not suggest that any of her crew take her place. Important, she did not invite a British expert to work directly with her.[106]

The meeting concluded with Driscoll reaffirming her faith in her approach; with her promising to quickly inform Bletchley Park of the details of her superior method; and, with her submitting that list of

---

[106] Soon, Britain informed Safford that as soon as Driscoll's work proved "in any way successful" that GC&CS wanted to send out one its it best men. TNA/PRO HW14/45 'To Washington' December 1 1941, 'Your CXG 105 of 27.11.41'.

questions to Denniston. The list was very specific and did not reflect what Leigh Noyes, the Director of Naval Communications, later asserted: OP-20-G had expected the British to supply everything about Enigma--without specific requests.[107] Importantly, Agnes' list did not include anything about the Bombe, its methods, Banburismus, or any other British attack. She was after just enough details about Enigma and the German naval systems (including its use of 'indicators') to allow her to further her own attack.[108]

A bit put-off, Denniston departed concluding that Driscoll was America's version of Dillwyn Knox, the rather crusty old English codebreaker of World War I who remained active at GC&CS, but who did not seem to fit into Bletchley's new way of doing things.[109]

---

[107]. TNA/PRO HW 14/45 'List' following Denniston report on August 18, 1941 meeting.

[108] Ralph Erskine, "What Did the Sinkov Mission Receive from Bletchley Park?" Op. cit., also contains the list of questions.

[109] Driscoll worked in a rather idiosyncratic way, one not in tune with large bureaucratic organizations. One member of 'G' mentioned that Driscoll has a

Safford's Trust

Denniston arrived in England convinced that neither Driscoll nor Safford were 'friends' of GC&CS or Anglo-American cooperation. Nevertheless, he kept his word. As a first step, he immediately established detailed procedures to register and track all communications with 'G' and the SIS.[110] He then had his technical people take scarce time to answer Driscoll's questions, sending them to America in October.[111] He also dispatched the specifications of Enigma set-ups and wheel wiring that Bletchley's crew had recently discovered. GC&CS later shipped copies of all the relevant intercepts for 1941. Moreover,

---

large and very disorganized closet full of message and solutions that others found valuable--but only after complete reorganization. U.S. Navy Historical Center, Operational Archives, SRH355, Op. cit., 160.

[110] TNA/PRO HW 14/45 "Dispatch of Packages for U.S. Authorities at Washington," August 28, 1941.

;TNA/PRO HW14/45, 'Hastings from Denniston' December 12, 1941; TNA/PRO HW 14/45, October 1. 1941, 'To Safford; ' and, 'dear Eddie', Op. cit..

Denniston made additional inquires about acquiring an Enigma for Driscoll. Then, he waited, and waited, for Driscoll's description of her method. Driscoll's failure to send the promised description frustrated Denniston. He wrote: "As to the famous Mrs. D., I have sent her nearly all she asked for and asked her to prove her method's success where we have failed. Our men can't believe it but of course if she can do it we shall send out a professor. We are on a good wicket at present but can't afford to neglect any side lines."[112]

As he waited for the detailed description, he prodded Mrs. Driscoll with a request for answers to three general questions. He hoped that her response would contain the long expected full methodological explanation.[113] While again waiting for a response, GC&CS sent a longer letter to Driscoll. It was a scathing criticism of what its author understood her method to be–and a not-too-guarded demand for the details Agnes had promised in August. The writer, mathematically

---

[112] 'dear Eddie', Op. cit.

[113] 'dear Eddie', Op. cit.

skilled, declared that even when the majority of the settings of an Enigma were identified her method would generate too many possible settings to explore. Even if she applied her attack when the wheels, their order in the device, and the ring settings were known, it would take 72,800 hours of work to specify a message solution.[114]

Undeterred, Agnes Driscoll continued working.[115] She made few, if any, attempts to contact or inform the British about her work. Her crew computed more statistics and began building the catalog(s)--even though, apparently, 'G' remained without a full understanding of how

---

[114] NARA RG38 CHSG, Library, Box 104, undated letter, "we were rather surprised to hear." It has been determined that Alan Turing wrote the letter. See, Jack Copeland (ed.) *The Essential Turing: The Ideas that Gave Birth to the Computer Age*, Oxford, Clarendon Press, 2004., 341-35 This work readjusts Lee Gladwin' conclusions in his,." Alan M. Turing's Critique of Running Short Cribs On the U.S. Navy Bombes," *Cryptologia*, 27 #1 (January 2003) , 50-54..

[115] About this time Frank Raven, a navy stalwart at OP-20-G, was put in charge of the Driscoll team but he would soon be switched to head the Atlantic traffic analysis section. War Diaries, Op. cit.

naval Enigma's special turnover mechanism was driven.

Driscoll did not leave a formal record of her special 1941 catalog attack. However, we know that since early 1941 she was working on a project to ease spotting Enigma code-wheel positions when they were at their special 'turnover' point using an enormous catalog. Another related catalog attack was mentioned at the close of 1942; but she probably began work on it was much earlier in the year. Central to 'G's' efforts, she and her crew were also building a file containing almost one million entries which would allow searching through different Enigma wheel combinations to 'locate', presumably, the starting positions of the Enigma wheels.[116]

---

[116] The information on the '17576' catalog and the turnover project was graciously provided by Ralph Erskine . Alan Turing encountered this on his trip to the United States in December 1942. Like other British comments about Driscoll's work, those in Turing's report were less than complimentary. "A Driscoll-Welchman-Chamberlain catalogue is being made for the 56 wheel orders with 17576 cards in each. There is a dwindling party headed by Mrs. Driscoll that wants to list the positions with a given pairing on separate pages according to B-wheel position. Mrs. [D] thinks that this will help when one is looking up

Another effort was likely a modification of her earlier attempts at a full Enigma solution-- it was first mentioned in mid-1942. Then, a description of the attack appeared in August 1942 after Driscoll had experimented with it for some time, aided by what was probably the paper analog of the Enigma. One of the navy officers assigned to a new and separate OP-20-G Enigma group described it in a memorandum. He was working on the reduced problem of 'locating' the code wheel starting positions of an Enigma after all the other settings of the machine had been solved. Driscoll claimed that her 1942 attack, like that of 1941, needed only a few intercepted messages, very short clear-text words, and the special German bigram encoding tables.[117] She again asserted that the method was especially valuable because it overcame

---

positions where there is a turnover, but it won't."

[117] NARA RG457, HCC, NR 2338, Box 808, J. H. Howard to Commander Engstrom, 21 August 1942. For a more complete description of what became known as the "click" process, see, NARA RG38 CNSG, Library, Box 102 5750/1, "The Number of Stories Expected from the Click Process." October 13, 1942.

difficulties caused by the erratic turnover of Enigma's code wheels.

The most direct though not complete description of the method she had proclaimed as ready in mid-1941 indicates she continued to think she was on the way to a complete solution of Enigma. The description came from that critical British expert who had heard of it second hand, probably from Denniston after his August 1941 trip to the United States. According to the expert (later identified as Alan Turing) Driscoll's attack began with a short crib and assumptions about how the letters in the crib were set-up on the Enigma's plugboard (stecker). By assuming the steckers, Driscoll obtained pairs of letters in unsteckered form. Using those letters she went through the twenty-six positions of the assumed fastest moving code wheel keeping constant a combination of the second, third and letter-reversing wheel –all treated as a unit. At each position of the assumed fast wheel, the analyst traced letter pairs in a large catalog of the output of the chosen combination of wheels. The goal was to specify the correct wheels and their positions. Any inconsistency in the emerging letter-pair chain could also lead to the

rejection of assumptions about the steckers and wheels.[118]

Whatever the nature of her 1941 work, it had Safford's full support. In late 1941, he approved her requests for more resources although she had admitted that one of her attacks had failed.[119] By the end of the year, her team had more than doubled and had some fourteen people.[120] They generated letter groups and punched them on tabulator cards, using precious machine time and manpower while Agnes awaited that physical copy of an Enigma.[121]

In mid-December 1941, six months after the Driscoll-Denniston meeting, , Agnes finally sent the British some partial information on her special method that she had so proudly alluded to in her conference

---

[118] NARA RG38, CNSG, Library, Box 104, nd., "we are rather surprised to hear."

[119] TNA/PRO 14/45 [Hastings] to Denniston December 13, 1941. This method was described as a "shortcut" to the turnover problem. See also, as provided by Stephen Budiansky, Op. cit.

[120] As supplied by Robert Hanyok, OP-20-G, War Diary, January 1942.

[121] TNA/PRO HW14/45, 'Denniston's reports and replies', December 2-13, 1941.

with Denniston in August. Despite 'G's' often -voiced protests that GC&CS was not giving full and open answers to its inquiries, Driscoll sent only cursory answers to the few questions Denniston had posed almost four and one-half months before.[122]

Driscoll again declared faith in her approach, but GC&CS had concluded that her method had "apparently failed." It could not, as she had claimed, overcome the problems analysts faced when Enigma's wheels moved before enough letters had been enciphered to allow identification of particular wheels. As a result, GC&CS began to have second thoughts about responding to Driscoll's demand for even more technical information.[123]

Meanwhile, something went terribly wrong.

Unraveling

The ties between OP-20-G and Bletchley began unraveling. Incorrectly,

---

[122] TNA/PRO HW 14/45, 'CXG 129', December 13, 1941.

[123] As provided by Stephen Budiansky, 'RG38', Op. cit. Also, TNA/PRO HW14/45, CXG.130, 'Copy to Commander Denniston, December 12, 1941'.

the navy accused Denniston of not truly sending his early October communications containing detailed answers to all but one of Driscoll's questions.[124] After that, emotions took hold. It did not take long for Safford's complaints that Britain was breaking its promises to push his superior, Leigh Noyes, into a series of the strongest protests against GC&CS, and to a reaffirmation of the powers of Driscoll's methods. Through November and into December, memoranda flew across the Atlantic. Noyes was very direct: Britain had broken its promises to 'G'; America had no use for the Bombe; if GC&CS finally cooperated

---

[124] Exactly what happened to the materials is uncertain but, as stated below, they were sent and were received at OP-20. 'dear Eddie', Op. cit. . See also, Ralph Erskine in, "What Did the Sinkov Mission Receive from Bletchley Park?," Op. cit. NARA RG38, CNSG, Library, 5750/41 , 'Noyes signaled that all was ok'. It should be noted that Denniston sent information to the American army's codebreakers at the same time and it was received. On that mailbag of Japanese army messages and related crypto information, NARA RG457, HCC, NR1920, Box 751, 'SIS Personnel, Organization and Duties 1937-1941', as cited by David Alvarez in, *Secret Messages: Codebreaking and American Diplomacy, 1930-1945*, University Press of Kansas, 2000.

Driscoll could have her method working on real problems.[125]

In comparatively measured responses, Denniston and his colleagues declared they had fulfilled all the agreements and were not holding back vital information. They asked why Driscoll had not responded as quickly as she had promised, why she was not fully sharing her secrets, and why the Americans had taken so long to signal them that they had not received Denniston's information on Enigma.

Noyes' next responses were heated—alienating and frightening to the British. The navy, he said, had never agreed to confine itself to Enigma "research." It had always intended to be "operational." He told the British liaison officer in Washington that what the navy wanted was the information on Enigma and the codebooks and machine that Safford and Driscoll had requested. Soon, the British began to worry about more than the navy's protests. GC&CS began to fear that Friedman's men were planning to work the German air force systems on their own and to

[125] For example, see, TNA/PRO HW14/45 '[Hastings] to GC&CS', December 2, 1941, HW 14/45 'CXG 115-117', December 2, 1941.

neglect the Japanese problem. The army denied such intentions.[126]

Then, and despite what would appear in the later histories of GC&CS - OP-20-G relations, Noyes apologized. On December tenth (and again on the twelfth) he declared that British explanations and actions since his outbursts had satisfied him and "everyone else."
In addition, OP-20-G finally discovered the missing October package within its own offices.[127] On the thirteenth, GC&CS received a cryptic

---

[126] See, as provided by Stephen Budiansky, RG38, Op. cit. However, Friedman's group made repeated surges to break free of dependence on Britain. For example, it did not inform the British of its summer 1942 decisions to view the Bombe plans sent to OP-20-G and to begin the design and construction of its own Bombe. NARA RG457, HCC, NR3815, Box 1283, ' Project 68003', Friedman to Bullock, September 14, 1942, 'Project in the Cryptanalysis of German Military Traffic in their High-Grade Cipher Machine'.

[127] Three days after Pearl Harbor, Noyes, responding to the answers from Denniston, informed the British representatives that he was "satisfied" concerning the 'missing' packets. On the October information: as provided by Stephen Budiansky, NARA RG38 , Op. cit.; also, TNA/PRO 14/45 'CXG 105-109', December 12. 1941, and 'CXG 127', December 12, 1941. NARA RG38,

yet pointed message from someone in the U.S. Navy Department:

> "Luke Chapter 15,v 9: And she found it. She calleth together her friends and neighbours saying: Rejoice with me for I have found the piece which was lost."[128]

Complaints, Yet Again

Noyes's repentance did not mean that all was well, nor that Driscoll had abandoned her cause.[129] Tensions escalated. Once again, there was a pointed American request for a copy of an Enigma machine. Then, while Roosevelt and Churchill were forging the unique alliance of their two nations, their crypto services began drifting apart–again. Dissensions within both nations' crypto-agencies had much to do with that. Word of those fritions and of the British-American misunderstandings must have reached above the levels of Denniston,

---

CNSG, Library, Box 104, on January 2, 1942, OP-20-G received a package containing the steckers for July 1941 from GC&CS.

[128] TNA/PRO HW 14/45, 'G. 199', December 13. 1941.

[129] TNA/PRO HW 14/45, 'CXG' 131, December 13, 1941.

Noyes, Safford, and Friedman. There had been some hints a few months before about changes within GC&CS, as well as within OP-20-G. In October 1941, Alan Turing and others at GC&CS had gone to the Prime Minister's level to protest the lack of resources at GC&CS.[130] There were demands for more Bombes.[131] In February 1942, there was a major reorganization at Bletchley and a new group began to serve as the representatives to 'G' and to Friedman's SIS. Denniston was "promoted' out of Bletchley. Soon, BTM was ordered to shift priorities to Bombe production--two factories and a thousand people were assigned.

At OP-20-G, hints of changes in priorities, attitudes, and people surfaced in late 1941. In November, there was a meeting between the

---

[130] The October 1941 letter requesting more people is reprinted in. F. H. Hinsley, et al, *British Intelligence in the Second World War: Its Influence on Strategy and Operations, Volume Two*, New York, Cambridge University Press, 1981, 655-657.

[131] TNA/PRO HW14/19 'Welchman request', Sept., 1941. See also, HW14/31, March 11, 1942.

cryptanalysts at ‘G’ and the team from the Massachusetts Institute of Technology (MIT) in charge of designing and building revolutionary optical and electronic ‘computers’ for OP-20-G. They had just begun their task and wanted to know what kind of machine each major cryptanalytic group desired. They spent much time listening to a description of Agnes Driscoll’s “special problem.”[132]

Despite that attention, when the meeting was over the MIT group was taken aside and told that, "her problem was not that important." [133] They must have believed that statement. The navy’s technical advisors did not attempt to design a machine for any traditional catalog method until a year later. It was another dozen months before it was delivered to ‘G’ –and in an altered form as a device to implement a letter ‘E’ attack.[134] A machine designed to perform the data-heavy tasks of a

---

[132] NSA FOIA RAM File, 'Notes of Meeting’, November 3, 1941.

[133] NSA FOIA RAM File, 'to Howard’, November 14, 1941.

[134]117. NARA RG38, Radio Intelligence Series, Box 170, RIP605 #5, ‘HYPO - General Nature and Projected Use–Notes on the Use of EEE—Sequence’, and,

Banburismus type attack received a much higher priority and work on its design began in early 1942. Meanwhile, new faces appeared at OP-20-G--old-timers were pushed aside. Joseph Wenger, the regular navy officer who had been the driving force for the modernization of 'G's 'methods and machines in the 1930s, returned to Washington. He came with plans and a new mind-set. He wanted the centralization of 'G' and the elimination of any fiefdoms. In addition, he urged cooperation with the British to solve what had changed from an imminent to an immediate problem, the U-boat challenge in the Atlantic. New

---

'Use of An All E Sequence', suggest that others in OP-20-G (not Driscoll) developed the final version of what they called a unique American "locator" and that a complex catalog HYPO attack was replaced with the simpler letter 'E' method. To this author's surprise, the documents on HYPO did not mention Mrs. Driscoll. The lack of interest in the machines for Driscoll supports the conclusion that little faith was being placed in Driscoll's other attacks. See Colin Burke, "Automating American Cryptanalysis, 1930-45: Marvelous Machines, A Bit Too Late," in David Alvarez (ed.), *Allied and Axis Signal Intelligence in World War II*, London, Frank Cass, 1999.

mathematically and university trained officers such as Howard Engstrom, soon joined Wenger in Washington. The SIS faced is own internal traumas as the failure to predict the Japanese attack on Pearl Harbor led to a disheartening outside investigation of the service.

Laurance Safford was the crypto-officer who took the brunt of much of the discontent over the state of American codebreaking. He was pushed aside when he lost an organizational tussle with Joseph Wenger. Safford's supportive Director of Naval Communications, Leigh Noyes, despite trying to fix relations with GC&CS, lost a more subtle battle to Joseph R. Redman. By February 1942, a new hierarchy was in charge at ‘G’ and the British looked forward, finally, to "cooperation." [135]

Losing Cryptanalytic Face

It seems that Agnes Driscoll’s crypta-cause suffered--although she

[135] TNA/PRO HW14/48, GC&CS memorandum of August 16, 1942.

remained in charge of an anti-Enigma group.[136] Meanwhile, Safford had to adjust to more than a not-to-well disguised demotion. He also had to admit that he had been wrong about the promised quick yet independent and efficient American Enigma solution. In early March 1942, after more meetings with British representatives, and after learning of the new and then impenetrable U-boat four-wheel Enigma system, Safford announced the failure of 'G's' early efforts: results had, at best, been "meager," he wrote. He informed his superiors (without naming Driscoll's efforts) that Enigma was not going to yield to an inexpensive or independent American cryptanalysis. He gave a very pessimistic assessment and stated that thefts, German errors, and cryptanalytic craftsmanship had been, and would be, the only ways into naval Enigma.[137]

---

[136] OP-20-G War Diaries. OP. cit., show Driscoll with more than a dozen people continuing with her project.

[137] Louis Kruh, "Why Was Safford Pessimistic About Breaking the German Enigma Machine in 1942?," *Cryptologia*, 14 #3 (July 1990), 253-. William Friedman, who had directed part of his team to develop a "statistical" attack on

However, Wenger and the leaders of a new and separate OP-20-G German team he had created had more faith in cryptanalysis and GC&CS, and they were more devoted mathematical and technological cryptanalysts than Driscoll. As a result, they were cooperative when they met with the latest British crypto representative who had rushed to Washington in April 1942.

What became rather cold relations between Agnes Driscoll and Wenger's group may have been a consequence of their new attitude toward the British-–especially after she learned that 'G' might fully open its arms to England.[138] Driscoll did not surrender, however. She

---

Enigma in 1942, came to a similar conclusion after his return from a visit to Bletchley Park. His report, "Enigma Operations at GC&CS" NARA RG457, HCC, Box 1126, stressed that Enigma would not yield to "pure cryptanalysis."

[138] Documents from April 1942 meetings indicate that the Americans had learned much about earlier Enigmas and the British methods since August 1941. This supports the idea of Denniston providing more information in 1941 than later alleged by 'G' The questions asked of the British experts at the time were aimed at special features of the new four wheel naval Enigma. However, (see below)

persisted. She or an ally in 'G' gained the ear of the new Director of Naval Communications, Joseph Redman, who the British had thought would be a loyal friend. Although Leigh Noyes had declared in December that the navy was satisfied with British efforts, in early 1942 Redman sent a blistering message to England that restated all the older demands and accusations.[139] He wanted a copy of an Enigma, even if it had been damaged. He wanted GC&CS to provide all available information on minor German systems–all of which, he reiterated, were due in exchange for the American gifts of early 1941. Then, the peacemaker GC&CS sent to America, John Tiltman, had to endure an embarrassing harangue by Agnes when he attended a joint OP-20-G/-SIS Washington conference in spring 1942. Driscoll's accusations tested Tiltman's patience, as did confrontations with Redman that

---

questions later put forward by the new OP-20-G Enigma team under Engstrom suggest less than full communications between it and the older American group.

[139] NARA RG38, 'LEPPERT' March 5, 1942, as supplied by Ralph Erskine John F. Clabby, *Brigadier John Tiltman: A Giant Among Cryptanalysts*, Ft. Meade, Md, Center for Cryptologic History, National Security Agency, 2007, 38,58.

continued into the postwar era.

Meanwhile, Wenger's new American Enigma group under Howard Engstrom and Robert Ely was taking a very different course. Its members may not have been aware of Redman's March 1942 demands, and they may have been the victims of a breakdown in communications in OP-20-G. The information on Enigma GC&Cs sent since the Weeks-Currier trip in early 1941 seems not to have been passed on to the Ely-Engstrom team. Why else would a history proclaim that, shortly after being assigned to the task in spring 1942, "Ely evolved the basic concept of a device which was subsequently discovered to be identical in principal with that which the British at that time were employing in England."[140]

While Ely and his team were reinventing the Bombe, wasting perhaps six months time, they asked for all the things Driscoll had ignored in August 1941. They gave Bletchley's costly approach a major

[140] NARA RG38, CNSG, Library, Box 104, 5720/205, "American Cryptanalysis of German Naval Systems," July 1, 1944.

compliment: they demanded that GC&CS send a Bombe, not a copy of an Enigma, and that GC&CS give them full knowledge of the methods that made it successful.[141]

At the same time, they inexplicably bowed to Britain's earlier wishes and signaled they would not establish their own operational system.

Starting Over Again

GC&CS, with an overly taxed workforce, and facing defeats in attempts by two groups to devise revolutionary types of Bombes to conquer the new U-boat Enigma system, was unable to send a Bombe to Washington. The British were so hard-pressed that they found it

---

[141] NARA RG457, HCC,NR3815, Box 1283, 'Project 68003', 'Questions Handed to Col. Tiltman', April 24, 1942. The British seem to have been sincere in their promise to send a Bombe as they did expect their new types to be ready by June 1942. However, they were pessimistic about success against the four-wheel 'E' and foresaw having to make 336 Bombe runs for each problem because they could not deduce wheel orders. NARA RG38, Radio Intelligence Series, RIP403, Box 169, 'For Tiltman from Travis', April 21, 1942.

difficult to produce copies of blueprints of any of the Bombe types for the Americans.[142]

With the U-boats dominating the Atlantic, and GC&CS unable to penetrate the new four-wheel Enigma, 'G' decided to launch its own Bombe development project; but its new leadership had still not committed to a separate operational program.[143] Despite that spring 1942 decision to begin a design effort, the Americans did not gain enough knowledge from the now completely cooperative England to

---

[142] On the problems of the teams working on the British high-speed Bombes, see the various reports in, TNA/PRO HW14/59 and HW3/93. On the difficulties of supplying blueprints, NARA RG457, HCC, NR3815, Box 1283, 'Project 68003', CXG 550 From Travis, July 27, 1942.

[143] As mentioned above, Friedman's group decided to establish its own program a few months later and without asking for British permission. See, NARA RG457, HCC, NR3815, Box 1283, 'Project 68003'. On grand plans for British Bombes in which any wheel could be used to represent any other, War Diaries, Op. cit., Eachus, "Cold Spot Method," app. August 1942.

begin final detail designs until late summer.[144]

There was something odd about the new American naval Enigma project. It was as if the Engstrom-Ely group could not communicate with Driscoll and her team as they continued to build her paper catalog. The new group had to ask the British questions about Enigma indicating they were unaware of some of the fundamentals that had been previously revealed to 'G'. They seemed not to know that in very early 1942 the British had sent a copy of Turing's marvelous report on the Enigma and his attacks against it.[145] That report contained useful

---

[144] Insights into the progress of the new 'G' Enigma group are in: NARA RG38, CNSG, Library, , Box 104 , 5750/205, "Easy Research to Date," July 24, 1942. It indicates that the new American team did not have full knowledge of the British Bombe design and logic but had learned enough to devise a quite similar approach. See below on the method and logic first used by the Americans and the question of the Turing "Treatsie" and the first American "hot point" design.

[145] For the sending of Turing's report see Stephen Budiansky: RG38, Op. cit.. also, NARA RG457,HCC, NR964, 'Turing's Treatsie on the Enigma', Box 201. This document was in the NSA files but the date of original receipt is not. It is assumed that it was this document or parts of it that was the "report" alluded to in

descriptions of Bombes and methods.

Although not as intense as before, the first half of 1942 witnessed a bit of yet another renewal of bickering and suspicion over "withheld" information–this time, ironically, about the Bombe and its allied methods.[146] The Americans were upset when they discovered that

---

the "Notes on E Correspondence." The Treatsie contains at least general explanations of most of the GC&CS Enigma methods including logical outlines of the Bombe including a description of something quite like the "cold point" or instantaneous test for steckers. That method and associated hardware looked for inconsistencies. The first American "hot point" design, in contrast, searched for possible correct settings. That "hot point" approach was not instantaneous but it did not require commutators that sent current in both directions and, thus, called for commutators with one-half the components. The SIS' Rosen, as noted above, also claimed that the army independently invented its Bombe.

[146] As before, mislaid and tangled communications between parts of the navy seem to have compounded the problems. NARA RG457, HCC, NR2723, Box 1283, 'Project 68003', "Questions Handed to Col. Tiltman, April 24, 1942," and, 'For OP-20-G From G.C. & C. S. XT 685', May 15, 1942. Also revealing is:, "Easy Research to Date," July 24, 1942', Op cit..

their first design for a bombe (one planned to be electronic) used a very inefficient logic to test the Enigma stecker (plugboard) setting. After several months of work, in July 1942, they switched to the British approach that was twenty-six times more powerful.[147] Despite the investment of millions of dollars and the take-over of a major 'computer' company (thus acquiring the talents of the National Cash Register Company's Joseph Desch), OP-20-G did not have a truly operational four-wheel Bombe until late summer 1943. By that time, the Atlantic crisis had greatly eased and GC&CS was regaining its power

---

[147] NARA RG38, Radio Intelligence Series, RIP, Box 171, "American Hot Point Method," August 1942. The British "cold point" test of the diagonal board was instantaneous while the American "hot point" design called for scanning all twenty-six positions at every Bombe position. Thus, the British Bombe was more efficient in testing steckers. "Easy Research to Date," Op cit.. The "Easy" document also explains one of the reasons why OP-20-G decided to abandon its plans for an electronic Bombe, one that was to perform one-half million tests a second. The savings using the cold point test meant that a non-electronic Bombe would be almost as fast.

over the U-boat Enigma. Although both the American and British four-wheel Bombes contributed to a near constant reading of the U-boat's Shark system from late 1943 to the end of the war, they came too late to play a dominant role in winning the Battle of the Atlantic.

The delayed appearance of the American Bombes may have been the reason for the reappearance in 1943 and 1944 of complaints about British openness– complaints with a new twist. When asked to write an official history of the American Bombe project Joseph Wenger and his colleagues restated the old theme of Britain's withholding of vital information. However, what the British had withheld, they claimed, was not what Driscoll had sought. It was what she had refused when Denniston visited in summer 1941. Supposedly, the British gave all she had needed but kept information on the Bombe and its methodologies to themselves. In mid-1944, in a private response to an inquiry about Redman's March 1942 protest, Wenger penned a reinterpretation of what had happened in 1941, as well as a slap at Mrs. Driscoll's attack..

> "Unfortunately there must have been a misunderstanding on Captain Redman's part, or else he was misinformed

> concerning the nature of the 'E' problem. In the first place, the British had supplied us with a paper model that was entirely adequate for our purposes at that time. Furthermore, by no stretch of imagination could the mere possession of a German cipher machine have enabled us to read any of the German traffic. We were in possession of ample information concerning the machine itself. What we lacked (emphasis added) and were anxious to obtain was more information concerning the Bombes and the British method of solution."[148]

However, Wenger's views on Driscoll never appeared in the formal histories of OP-20-G.

Driscoll Steps Back

By fall 1942, many of Safford's fears had been realized. 'G's' Enigma work became somewhat of an appendage to GC&CS.[149] In return for the

---

[148] NARA RG38, 'Memorandum for OP-20-G', May 13, 1944, as supplied by Ralph Erskine.

[149] NARA RG457, HCC, NR4584, Box 705, 'Bombe History' for the renewed

secrets of the Bombes and the techniques and information to make them useful, the Americans moved to a new level of cooperation. Fall 1942 began an amazing era of intelligence sharing between the two nations.[150]

Agnes Driscoll? Typically, it is hard to trace her history after Safford's announcement of defeat. Her name does not appear in major documents, such as the critical and politicized 1944 report on the history of ‘G’s’ Bombe project. The navy seems not to have consulted her for that history, as there is no mention of Denniston's offer of August 1941, or of the details of the missing-package crisis of October.[151]

---

agreement to shift many of ‘G’s’ experts to Japanese problems and to rely upon n GC&CS for much Enigma cryptanalytic research.

[150] Friedman's group had begun a Bombe development program in late 1942, without giving full knowledge to the British, NARA RG457, HCC, NR3815, Box 1283, ‘Project 68003’, ‘Bullock to Friedman, 1-4-43’. The British reaction to the discovery that SIS was planning an operational machine (and not confining itself to research) was quite strong. See the Welshman memo of 5-43-43, TNA/PRO HW14/75.

[151] NARA RG457, HCC,NR4584, Box 705, 'History of the Bombe Project, 24

Driscoll's 'catalog' method evolved into the "click" process, which proved of some value to OP-20-G and to the British—but only as a 'locator'.[152] It seems that an 'E' catalog was made operational, but, again, only as a 'locator' to supplement the Bombes. At first, tabulators were used for 'E', then, the new analog photoelectric-electronic HYPO machine was put to work in late 1943 to reduce the load on the Bombes. Ironically, HYPO had begun as a machine for Driscoll's traditional catalog attack, not as an 'E' machine. [153]

April 1944'. At least one draft of the history contained a major error: "the British did not inform us of their work until after Pearl Harbor."

[152] NARA RG38, CNSG, Library, Box 102 5750/1, "The Number of Stories Expected from the Click Process," October 13, 1942, and, NARA RG38, Radio Intelligence Series, RIP, 603 Enigma Series 1, "Click Process." 'Click was, admittedly, only a 'locator'.

[153] Note that Hypo began as a machine intended to automate a catalog method for the 'four' wheel problem. Then, it was switched over to the 'E' attack. TNA/PRO HW25/1. HYPO was also used against an Abwehr Enigma and was put to a ninety hour run to attempt to see if the German Rocket (railroad) Enigma

There are hints that none of her other Enigma methods became central to OP-20-G although various traditional catalog techniques were explored and refined by the new Enigma group under Howard Engstrom.[154]

---

system had been changed. See NARA RG38 Radio Intelligence Series ,Box 170 RIP 605 #5, "Hypo–General Nature and Projected Use," Ely, March 1943 and 605 #5, articles on the letter 'E' methods. Also, NARA RG457, HCC NR1548, Box 600, CNO-TS-9 HYPO, 6-45. Other OP-20-G RAM machines were tested to see if they could function as 'locators'. NARA RG457 Box Box 583, 'IC, Tetra Tester, Ram2, ICKY'. On the railroad Enigma, David H. Hamer et al, "Enigma Variations: An Extended Family of Machines," *Cryptologia*, 22 #3 (July 1998), 21-. HYPO was also used on some Japanese problems. TNA/PRO HW25/1 C. H. O'Alexander, "Cryptographic History of Work on German Enigma Machine, " and, NARA RG457, Box 600, 'Cryptanalytic Equipment for Enigma', 'Hypo'. ' David H. Hamer, "Enigma Actions Involved in the Double Stepping of the Middle Rotor,:*Cryptologia*, 21 #1, (January 1996), 47-50.

[154] For an example of a catalog technique that appears much like Driscoll's, NARA RG38, Radio Intelligence Series, Box 170, RIP 603 #1, "Recovery of the Grundstelling," February 1943. However, in that report and in others in the RIP

Driscoll seems to have continued her efforts on the German problem until early 1943.[155] With a dwindling staff and with an OP-20-G stalwart, Frank Raven[156], again looking over her shoulder, she focused

---

series that explored 'catalogs', Driscoll was not mentioned. These reports also show the limits of traditional catalogs attacks-- due to the sheer size of the catalogs.

[155] The navy had already taken much of the German work from her group. NARA RG38, CNSG, Library, Box 104, 5720/205, "American Cryptanalysis of the German Naval Enigma," 7 July 1944, OP-20-GY-A to OP-20-G-1 shows that the bulk of the German cryptanalytic work had been assigned to the new group. Among them were men who later became famous in the American academy, such as W. V. Quine and W. R. Church. Church's research group discovered, in 1944, important rules the German were using that limited Enigma wheel choices. This discovery made the attack on Enigma much more efficient. A. P. Mahon, op. cit.,5.

[156] In mid-1942 Raven was regarded, by the new operational head of OP-20-G, Joseph Wenger, as the best Enigma expert at 'G'. RG457, HCC, Box 1386 NR4419/4420, 'Wenger Memoranda'. "American Cryptanalysis of German Naval Enigma", Op. cit. Raven had been placed in charge of Atlantic traffic

on more Bombe-related methods--with perhaps, little success.[157] The navy then returned her to work on Japanese systems two months before the team working on the new Coral enciphering machine problem finally reconstructed the device. At the end of 1944, she participated in what seems to have been the navy's first attempts at decrypting its intercepts of higher-level Soviet messages.[158]

---

analysis in February 1942. War Diaries, Op. cit.

[157] The December 1942 evaluation of a Driscoll project by Alan Turing was quite critical of her efforts to build a catalog to help identify "B-wheel" turnovers. Quotation is from the Turing report on his visit to OP-20-G and Dayton, supplied by Ralph Erskine, May 18, 2000.

[158] Cipher A. Devours and Louis Kruh, *Machine Cryptography and Modern Cryptanalysis*, Norwood, Mass., 1985, 249, does not mention Driscoll when discussing the attacks on major Japanese systems. The authoritative work by David Kahn, *The Codebreakers" The Story of Secret Writing*, New York, MacMillan Publishing Company, 1967, had no references to Driscoll after her work with Hebern in the pre-war era. However, Ralph Erskine has found evidence in OP-20-G documents (such as the War Diaries) in the NARA RG38 CNSG collection of her assignment to Coral in January 1943 and to the "Foreign

One thing is certain about Driscoll: She continued at OP-20-G and its successors for fifteen years after WWII. However, what she did after 1945 remains, typically, vaguely described. She died fourteen years after she retired in 1957.

Language" section in November 1944. On the reassignment to the Japanese attaché system, NARA RG38, CNSG, Library, Box 104, “American Cryptanalysis of German Naval Systems.” The late Cecil Philips who made the initial in-roads on the post-war Venona project had informed Robert Hanyok that Driscoll did some work on Russian problems but that her contribution was, at most, very minor. NSA FOIA 52567 “Madame X: Agnes in Twilight…,” Op. cit.