Decoding Pearl Harbor:
USN Cryptanalysis and the Challenge of JN-25B in 1941

Timothy Wilford[1]

En 1941, les « Forces navales des États-Unis » ont tenté de dévoiler les plans de la marine japonaise en décryptant le principal code la marine japonaise, soit le JN-25B. Les auteurs traditionalistes estiment que les « Forces navales des États-Unis » ne pouvaient pas lire de JN-25B en 1941, alors que les auteurs révisionnistes estiment que le JN-25B était entièrement lisible. Cependant, un examen de la correspondance et des rapports de l'époque démontre que les « Forces navales des États-Unis » pouvaient partiellement décoder le JN-25B sur une base régulière depuis novembre 1941, mais on ne sait pas exactement dans quelle proportion on pouvait décoder le texte des messages. En outre, vers la fin des années 1941, les « Forces navales des États-Unis » interceptèrent plusieurs messages faisant allusion à une attaque japonaise trans-Pacifique contre les principaux navires ancrés au port. Les historiens qui étudient la controverse concernant Pearl Harbor doivent maintenant déterminer dans quelle proportion on pouvait décoder le texte des messages JN25B en 1941 au lieu de questionner la possibilité réelle d'un décryptage continue.

"We are reading enough current traffic to keep two translators very busy," explained Lt. John Lietwiler to the Navy Department in a letter dated 16 November 1941, in which he discussed

The author expresses his gratitude to Brian Villa, Professor of History at the University of Ottawa, who directed the graduate research from which this article is drawn.

American efforts to decrypt the principal Japanese naval code.' The Japanese named this code *Kaigun Ango – Sho D,* but in 1941 American cryptanalysts referred to it as the 5-Numeral Code or AN-1 Code, although it was later known in Allied wartime reports as JN25B. Lietwiler was co-commander of Station Cast, a United States Navy (USN) radio intelligence station located on the island of Corregidor in the Philippines. One of his primary responsibilities in late 1941 was the penetration of JN-25B. The Imperial Japanese Navy sent the bulk of its encrypted radio messages in this code and, needless to say, the Navy Department in Washington wanted to read these messages, despite its limited cryptanalytic resources. New evidence released by the National Archives II in College Park, Maryland, sheds light on the controversial question of how well the USN could read Japanese naval traffic in late 1941. Certainly, Navy cryptanalysts faced many obstacles in their quest to understand Japanese intentions in the Far East. Yet on the eve of the Pearl Harbor attack, USN cryptanalysts could partially read JN-25B, a code in which the Japanese transmitted numerous messages suggesting their intention to conduct a trans-Pacific raid against anchored capital ships.

Reading coded messages has always been a means of understanding an adversary's intentions. As early as the 1920s, the USN appropriated a copy of Japan's naval codebook, photographed it, and then used cryptanalysis to decrypt later cipher versions, or superencipherments, of the original code.' By 1926, the USN was decrypting Japanese naval messages sent in a naval code known to the USN as the "Red Book". After 1930, the Japanese navy used a new code, which the USN called the "Blue Book". Throughout the 1930s, the USN used cryptanalysis to recover new code and cipher values introduced by the Japanese navy. In 1939, the Japanese navy introduced a new principal naval code, known later to the USN as JN-25A. Although USN cryptanalysts solved this code by late 1940, the Japanese navy changed codebooks again on 1 December 1940. The new codebook, known later to the USN as JN-25B, became the object of much cryptanalytic effort. In 1941, the

---

[2] United States, National Archives II (NA II), Modern Military Records Branch (MMRB), Record Group (RG) 38, Crane – Inactive Stations, 370/27/23/7, Box 15, 3200/1 – *NSRS Philippines, Operations Summaries,* Letter dated 16 November 1941 from Lt. John Lietwiler, Fort Mills, P.I., to Lt. L.W. Parke, Navy Dept., Washington, p. 1. Lietwiler's letter to Parke may have been misfiled long ago in 3200/1 – *NSRS Philippines, Operations Summaries;* his letter likely should have been filed in 1300/1 – *NSRS Philippines, Assignment & Distribution.* The author originally found the Parke-Lietwiler letters at the National Archives II during his visit from 29 February to 3 March 2000, and immediately shared this evidence with Prof. Brian Villa, who helped direct this research. In March 2000, the author sent the Parke-Lietwiler letters, along with about 875 other USN/Station Cast intelligence documents from RG38, to Robert Stinnett, who returned the favour by supplying the author with copies of his 1941 Station H records, originally obtained through Freedom of Information Act (FOIA) requests. The author is indebted to archivists John Taylor and Barry Zerby, who provided great assistance in his search for documents at the National Archives II.3

Rear Admiral Edwin T. Layton, with Captain Roger Pineau and John Costello, *And I Was There: Pearl Harbor and Midway – Breaking the Secrets* (New York, 1985), 31-2.

USN had three cryptanalysis centres working on Japanese naval codes: OP-20-GY at the Navy Department in Washington, Station Cast (COM16) at Corregidor, Philippines, and Station Hypo (COM 14) at Pearl Harbor, Hawaii.' Both OP-20-GY and Station Cast were dedicated to the solution of JN-25B, while Station Hypo was directed to decrypt an infrequently used Japanese naval code. David Kahn offered the following estimate of USN staffing: "Of the Navy's total radio-intelligence establishment of about 700 officers and men, two thirds were engaged in intercept or direction-finding activities and one third – including most of the 80 officers – in cryptanalysis and translation."[5] Indeed, Station Cast employed three translators, whereas Station Hypo employed seven. Furthermore, the USN exchanged code groups with its British counterparts.

With these cryptanalytic resources, limited as they were in the peacetime forces, the USN attempted to penetrate messages transmitted by the Japanese navy. The USN also decrypted Japanese diplomatic traffic (notably J-19 and PURPLE), but arguably the most important object of USN cryptanalytic effort in 1941 was the decryption and translation of Japanese naval messages transmitted by radio. Although actual 1941 USN decrypts or work sheets are unavailable, recently declassified USN correspondence, along with credible secondary sources, tell the story of American naval intelligence on the eve of the Pacific War.

Historians have variously interpreted the cryptanalytic abilities of the USN in 1941. In 1962, Roberta Wohlstetter, author of *Pearl Harbor: Warning and Decision,* focussed upon the value of diplomatic traffic: "The only markedly effective branch of Intelligence during 1941 was cryptanalysis. The messages decoded and translated from MAGIC provided vital data for predicting Japanese inoves."[6] Regarding Japanese naval codes, Wohlstetter asserted that these codes were virtually unreadable by the USN: "Of the naval traffic intercepted, Rochefort testified that his unit was able to decode and understand about 10 per cent. Neither unit [COM14 and COM16] had been able to break any high-priority naval code."' Wohlstetter mentioned that only Commander Laurance F. Safford, head of OP-20-G, believed that COM16 could partially read JN-25 by November 1941, but Wohlstetter accepted the majority of congressional testimony that suggested JN-25 was largely a mystery to USN cryptanalysts.[8] For Wohlstetter, MAGIC was the only viable source of cryptanalytic intelligence, but one that failed to serve as a warning signal because of the deluge of misleading information or "noise."

In 1967, David Kahn, author of *The Codebreakers,* explained that the Japanese never sent any encoded messages revealing their intentions at Pearl Harbor: "Why, then, did it [cryptanalysis] not prevent Pearl Harbor? Because Japan never sent any message saying

---

OP-20-G was divided into three sections: OP-20-GX (direction finding), OP-20-GY (cryptanalysis), and OP20-GZ (translation and dissemination). See David Kahn, *The Codebreakers: The Story of Secret Writing,* c. 1967, 1996 (New York, 1996), 11.

[5] Kahn, *The Codebreakers,* 10.

[6] Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford, CA, 1962), 169. See also page 171. 7 *Ibid.,* 31.8

Ibid., 41 n82.

anything like `We will attack Pearl Harbor."9 Kahn fell silent upon the subject of JN-25 decoding, but discussed the Navy's access to MAGIC diplomatic intercepts. He explained that Admiral Husband E. Kimmel, Commander in Chief of the Pacific Fleet, received enough MAGIC intercepts by late November1941 to know that war was possible, but emphasized that any forewarning of the Pearl Harbor attack was not possible.

By the 1990s, however, Kahn, drawing upon more recent sources, admitted to some USN decryption of Japanese naval codes. He wrote in 1991 that the Navy's poor IN-25 reading ability "was due less to Japanese cryptographic superiority than to the navy's insufficiency of cryptanalysts" and that "no reference to a raid on Pearl Harbor ever went on the air, even coded."[10] Underscoring his point, Kahn stated that "JN25b messages intercepted before the attack, but solved after the war, show that even if that naval code had been fully solved and those messages read before 7 December, they would not have foretold the attack."[11] In 1996, he explained that "Rochefort's attack on Japanese naval codes had achieved some minor successes in late October and November, but he could read only about 10 per cent of the naval traffic, and much of this consisted of weather and other minor systems."[12] Kahn also asserted that "Cavite [Station Cast] was spottily reading JN25 messages – which revealed nothing about Pearl Harbor – until December 4, when the superencipherment was suddenly changed."[13]

In 1967, Ladislas Farago adopted a similar view of USN cryptanalysis in *The Broken Seal.* Farago argued that USN cryptanalysis was not particularly effective by late 1941 and that "dependence on traffic intelligence had become crucial."[14] Drawing upon some of the sources used by Ellis Zacharius in *Secret Missions,* he decided that Japanese naval codes failed to yield important information to USN cryptanalysts.[15]Farago offered the following explanation:

> The FLAG OFFICERS code was lost and Rochefort's team of cryptanalysts was making no headway whatsoever in its effort to solve its replacement. Op-20-G did succeed in keeping the old IN series open and was, in fact, using its twenty-fifth variant, solved a few months before. But it was yielding only routine information, mostly of an administrative nature, with very little operational or tactical intelligence.[16]

For Farago, JN-25 had been understood by OP-20-G, but not well enough to provide complete textual information. Like most discussions of this topic in the 1960s, Farago's

---

Kahn, *The Codebreakers,* 4.

[10] David Kahn, "The Intelligence Failure of Pearl Harbor," *Foreign Affairs* 70.5 (Winter 1991/1992), 144, 147.

11 Ibid., 147.

[12] Kahn, *The Codebreakers,* 47.

" *Ibid.*

[14] Ladislas Farago, *The Broken Seal: The Story of Operation Magic and the Pearl Harbor Disaster* (New York, 1967), 269.

[15] For comparison, see Ellis M. Zacharius, *Secret Missions* (New York, 1946), 258.

16 Farago, *The Broken Seal,* 268-9.

account was rather general and necessarily based upon limited primary sources owing to the security-classification of such sources at the time. Nonetheless, Farago later offered important new testimony concerning code recovery, which will be later discussed, in his postscript to the paperback edition of *The Broken Seal.*

Gordon Prange and associates also asserted that cryptanalysis failed to unlock the secrets of Japanese naval codes in their epic work of 1981, *At Dawn We Slept.* Prange emphasized the decryption of Japanese diplomatic traffic, but explained that the USN had no working knowledge of JN-25: "In Safford's unit, Op-20-G, tension was `at an all-time high.' The `First Team' of experts sweated over the Japanese fleet JN-25 code.' For Prange, only call signs could have been read because the actual text of Japanese messages could not be decrypted.[15] Seemingly, Prange's treatment of cryptanalysis was more conservative than that of Farago.

Yet in 1982, John Toland explained in *Infamy* that the Dutch had broken Japanese codes and made their intelligence available to the Americans. Toland failed to broach the subject of USN decryption of Japanese traffic, but relied upon testimony to show that forewarning of the Pearl Harbor attack, as deduced by Dutch cryptanalysts operating in the Netherlands East Indies, was provided to Washington in a timely fashion. Toland produced testimony from key Dutch military personnel: "... during a meeting in 1943 Vice Admiral Conrad E.L. Helfrich of the Royal Netherlands Navy expressed wonder that the Americans had been surprised at Pearl Harbor. The Dutch, Helfrich said, had broken the code and knew that the Japanese were going to strike Pearl Harbor."[19] Nonetheless, Toland did not produce any decrypts of Japanese traffic and limited his discussion of message reading to the USN's interception of Tokyo's "East Wind, Rain" Execute message (allegedly sent in a plain-language weather broadcast), which meant Japan would declare war against the United States.[20]

In 1985, Rear Admiral Edwin Layton and associates returned to Farago's position, but discussed the potential value of cryptanalysis. In *And I Was There,* Layton asserted that USN intercepts of Japanese radio traffic had *"potential* intelligence value as clues to Japan's operational intentions, *including* indications that an attack force of carriers was heading for an unknown target."[21] Layton carefully supported his position with SRN intercepts dating from 14 to 29 November 1941, which demonstrated that the Japanese navy was being placed on a wartime footing complete with a Strike Force, "Combined Fleet Battle Plan," and fuel-supply network.[22] Yet Layton offered no clear indication of how much information USN cryptologists gleaned from these intercepts of Japanese traffic, other than explaining that such traffic was 10% readable in 1941. Nonetheless, Layton offered readers a tantalizing

---

[17] Gordon W. Prange, with Donald M. Goldstein and Katherine V. Dillon, *At Dawn We Slept: The Untold Story of Pearl Harbor* (New York, 1981), 464.
[18] *Ibid.,* 425.
[19] John Toland, *Infamy: Pearl Harbor and Its Aftermath* (Garden City, NY, 1982), 317-8.
[20] *Ibid.,* 286-7.
[21] Layton, et al., *And I Was There,* 231.
[22] *Ibid.,* 232, 548.

piece of information concerning intelligence-gathering: Lt. Cmdr. Alwin Kramer, a naval intelligence officer with OP-20-G, went about New York City in early 1941 stealing Japanese code books from diplomatic offices.[23] Kramer, employing the "direct method" of code breaking, made photo-prints of these Japanese codebooks for OP-20-G. According to Layton, exactly which codes Kramer was able to secure remains unclear. In general, Layton's account contributed important evidence to the debate over USN methods of intelligence recovery, but stopped short of definitive answers.

In contrast, James Rusbridger and Eric Nave offered definitive answers in their work of 1991, *Betrayal at Pearl Harbor.* The authors alleged that British cryptanalysts obtained enough intelligence from Japanese intercepts to predict Pearl Harbor, a feat not duplicated by the USN. Rusbridger and Nave explained that the Far East Combined Bureau (FECB) at Singapore, Britain's main intelligence unit in the Pacific, provided Churchill with foreknowledge of a long-range Japanese attack on American forces. Churchill, however, failed to share this important intelligence with Roosevelt. Rusbridger and Nave supported some of their arguments by citing USN intercepts (SRNs) as proof of what the FECB must also have intercepted.[24] The authors showed some misunderstanding of the JN-25 Japanese naval code as they failed to delineate the "A" version of the code from the later "B" version, and confused code types (encipherment) with additive types (superencipherment).25 Rusbridger and Nave provided testimony and letters to support certain points, but very little hard evidence to support their claims.

Frederick Parker, an historian with the National Security Agency (NSA), reaffirmed Layton's view in his well-researched account of 1994, *Pearl Harbor Revisited.* Parker, building upon the position he adopted in his 1991 article, "The Unsolved Messages of Pearl Harbor," explained that USN intercepts revealed Japanese plans for a trans-Pacific raid on capital ships moored in shallow waters, but that these intercepts were not readable by USN cryptologists.[26] Regarding JN-25B decryption, Parker explained that a lack of resources, particularly translators, prevented the USN from fully reading Japanese traffic: "Little if any of the COMINT provided by Station C [Corregidor] came from cryptanalysis. Because Washington could not supply current code group meanings, Station C was not able to read messages in ... JN-25, or in several of the minor naval codes."[27] Parker held to the view that all available USN decryptions were made in 1945-46, thereby concluding that the United States had no foreknowledge of Pearl Harbor. Parker's work constitutes one of the most meticulous examinations of these intercepted Japanese messages.

In 1995, John Prados expanded the debate over USN cryptanalysis *in Combined*

---

[23] *Ibid.,* 284.

[24] James Rusbridger and Eric Nave, *Betrayal at Pearl Harbor: How Churchill Lured Roosevelt into World War II* (Old Tappan, NJ, 1992), 138, 146.

[25] *Ibid.,* 86, 115, 145.

[26] Frederick D. Parker, *Pearl Harbor Revisited: United States Navy Communications Intelligence, 1924-1941,* United States Cryptologic History, Series IV, World War II, Vol. 6 (Washington, DC: Center for Cryptologic History, National Security Agency, 1994), 35, 43, 48. See also Frederick D. Parker, "The Unsolved Messages of Pearl Harbor," *Cryptologia* 15.4 (Oct. 1991), 295, 298.

[27] *Ibid.,* 48.

Fleet Decoded. Prados offered the first public account of the intelligence activities of Station Cast at Corregidor since the publication of Dwayne Whitlock's article, "Station `C' and Fleet Radio Unit Melborne (Frummel) Revisited."[28] Prados also systematically described the principal stations of the USN radio intelligence network. Moreover, he criticized Rusbridger and Nave for failing to provide sufficient evidence to prove that the British and the Australians were reading JN-25.[29] Prados, working mainly from official military histories, adopted the position of both Layton and Parker, declaring JN-25B to be beyond the grasp of USN cryptanalysts owing to inadequate resources: "In 1941 the JN-25(b) cipher continued to resist efforts to break into it. Station Hypo's assistance could have been useful had it been brought into the attack. It was not."[30] As well, Prados described JN-25B as "a cipher that Cast actively attacked, but that only slowly yielded its secrets."[31] Prados provided a good survey of the existing literature and available sources, but ultimately defaulted to the traditionalist view of USN cryptanalytic achievements in 1941.

Robert Stinnett, however, offered a revisionist account of USN cryptanalysis in *Day of Deceit,* a book published in 1999 after seventeen years of archival research. He stated that the USN had the ability to solve four principal Japanese codes by the autumn of 1941: Code Book D (JN-25), the Call Sign Code, the Ship Movement Code (SM), and the Merchant Marine *Shin* Code (S).[32] Stinnett analyzed Station Hypo's communication summaries (COMSUM 14s), finding that seven reports issued between 4 September and 16 November 1941 demonstrated Japanese code-reading ability, a feat not repeated again until 19 December 1941, well after the Pearl Harbor attack.[33] He also produced a message dated 29 November 1941, from Lt. Rudolph Fabian to Roosevelt's naval aide, which suggested that Station Cast was reading the Ship Movement Code.[34] Nonetheless, Stinnett, who conducted extensive research in several branches of the National Archives, found no reliable evidence "that establishes how much of the 5-Num text could be deciphered, translated, and read by naval cryptographers."[35] Stinnett largely relied upon the same cryptologic sources as previous authors, but decided that Japanese traffic was largely readable prior to the Pearl Harbor attack.

Yet the range of possible historical interpretations may be redefined through an evaluation of USN cryptanalysis as practised in 1941. Such an evaluation must consider capability, resource allocation and application. Indeed, an examination of key letters and

---

[28] John Prados, *Combined Fleet Decoded: The Secret History of American Intelligence and the Japanese Navy in World War II* (New York, 1995), 210-5. See also Dwayne Whitlock, "Station `C' and Fleet Radio Unit Melbome (Frummel) Revisited," *Cryptolog* 14.2 (Spring 1993): 1-19. Whitlock, who served as a traffic analyst at Station Cast in 1941, asserts that neither traffic analysis nor cryptanalysis provided any foreknowledge of the Pearl Harbor attack.

[29] *Ibid.,* 171.

[30] *Ibid.,* 175.

[31] *Ibid.,213.*

[32] Robert B. Stinnett, *Day of Deceit: The Truth about FDR and Pearl Harbor* (New York, 1999), 70-2.

[33] *Ibid.,* 133-4.

[34] *Ibid.,* 73.

[35] *Ibid.,* 324 n18. See also 348 n32.

message-intercepts, particularly those previously unavailable to historians, suggests that the USN could partially read Japanese naval traffic on the eve of the Pacific War.

Certainly, Japanese naval codes offered great challenges to USN cryptanalysts in 1941. The USN, working with limited resources, intercepted Japanese despatches mainly encrypted in five principal codes from the *Kaigun Ango,* a collection of 29 Japanese naval codes: the Japanese Fleet General Purpose System, the Japanese Minor Purpose System (for construction activities), the Merchant Vessel-Navy Liaison System, the Merchant Vessel-Navy 5-Letter Cipher, and the Japanese Naval Attaché Cipher.[36] Apart from these principal codes, the Japanese infrequently sent messages in the Japanese Navy Flag Cipher (AD code), an administrative code that had been a prevalent in the late 1930s before the introduction of JN-25. The cryptanalysis unit of OP-20-G, known as OP-20-GY, directed Station Hypo to work on the AD code, one that was never broken because its traffic volume was insufficient for successful decryption.

Meanwhile, OP-20-GY and Station Cast both worked on the Japanese Fleet General Purpose System – Code Book D, or *Kaigun Ango – Sho D,* known to the USN in 1941 as the 5-Numeral code or AN-1 code, but later known as JN-25B. This code carried the bulk of encrypted traffic for the Japanese navy. Kahn once estimated that JN-25B comprised "45,000 five-digit groups, enciphered by two volumes of 50,000 five-digit additives each.'" Just like the code's immediate predecessor, JN-25A, which the Japanese navy had used from 1 June 1939 until 30 November 1940,[38] each word in JN-25B was represented by a five-digit group, each of which was further enciphered by summing a five-digit "additive" using false addition (adding without carrying). For example, if the code word for the aircraft carrier *Kaga* is 01905, then its final super-enciphered form after summing the additive 00989 (using false addition) is 01884. Fortunately for USN cryptanalysts, when JN-25A changed to JN-25B on 1 December 1940, the additive groups, known collectively as Cipher 5, or Additive 5, stayed the same. This retention of the same additives aided recovery of the new JN-25B codebook. Nonetheless, the Japanese did change the additives used with JN-25B throughout 1941: Additive 5, or JN-25B5, was used from 1 December 1940 until 31 January 1941; Additive 6, or JN-25B6, was used from 1 February until 31 July; and Additive 7, or JN-25B7, was used from 1 August until 4 December.[39] The extent to which USN cryptanalysts read JN-25B at this time has previously been unclear because original decrypts were never publicly released.

USN histories and document collections offer various estimates regarding JN-25B code recovery in 1941. In the *Naval Security Group History to World War II* (SRH-355),

---

[36] NA II, MMRB, RG457, SRH Series, 190/36/11/4, Entry 9002, Box 120, SRH-406, *Pre-Pearl Harbor Japanese Naval Despatches, 7.*

[37] Kahn, *The Codebreakers,* 563.

[38] Stephen Budiansky estimated that JN-25A comprised about 30,000 code values and that the first additive groups also numbered 30,000. See Stephen Budiansky, *Battle of Wits: The Complete Story of Codebreaking in World War II* (New York, 2000), 7.

39 Stephen Budiansky, "Too Late for Pearl Harbor," *Naval Institute Proceedings* (Dec. 1999): 50-1; Stinnett, *Day of Deceit,* 331-2 n36; SRH-406, foreword, 7; NA II, MMRB, RG457, SRN Series, 190/36/26/4, Entry 9014, Boxes 144 to 147, SRN-116741. Hereafter, SRNs will be cited only by their numbers.

Captain J.S. Holtwick explained that "On 4 January 1941 it was reported that about 2000 values had been recovered out of 33,000 possible, in the 5-numeral code (JN-25)."[40] Parker assessed the importance of SRH-355 as follows: "This manuscript, which has been turned over to the National Archives, would have been listed as a primary source if all the documents uncovered by Holtwick could be examined by other historians."[41] A code recovery report dated 4 January 1941 likely would have likely concerned JN-25B, the system then current. Furthermore, the quote of 33,000 possible code values is reasonable given that the code's "divisible by three" garble check, which allowed Japanese operators to check the reliability of code reception, made only 33,333 code groups usable.[42] Yet contemporaneous OP-20-GY status reports offer the following estimates of code group recoveries made throughout 1941: 300 code groups by 1 April; 1100 by 1 June; about 2000 by 1 August; 2400 by 1 October; 3000 by 1 November; 3800 by 1 December; and 6180 by 1 January 1942.[43] These estimates conflict with the single estimate offered in SRH-355 and suggest that the USN had only recovered about 3000 to 4000 code values in the weeks preceding the Pearl Harbor attack. However, even if about 1000 code values represented numbers, which already constituted important intelligence considering their use in reporting ship positions, weather, dates and schedules, the remaining code vocabulary of 2000 to 3000 word groups could have permitted the reading of pattern naval messages.

Additive recovery and message reading ability have also been variously interpreted. Certain OP-20-GY status reports suggest that less than 10% of JN-25B7 additives had been recovered by December 1941.[44] Parker, an NSA historian, suggested otherwise: "Thanks to Japanese communications errors each successive JN25 Baker cipher ... was successfully penetrated by analysts in Washington and Corregidor until [Additive 8] was introduced on 4 December 1941.'[5] Perhaps Japanese code clerks became relaxed in their use of the additive books, frequently using the same additives over and over again, rather than using a wide variety. Also, they may have sometimes used a new additive type concurrently with its predecessor (i.e., Additive version 7 used concurrently with Additive version 6). Regarding message reading, one official source states that no JN-25B messages were read

---

[40] NA II, MMRB, RG457, SRH Series, 190/36/11/2-3, Box 108, SRH-355, *Naval Security Group History to World War II,* Part 1, 398.

[41] Parker, *Pearl Harbor Revisited,* 92.

42 A garble check is a convenient way to determine whether code groups have been received correctly or in a garbled, corrupted state. In JN-25B, the sum of all five digits in a code word had to be divisible by three. For example, the sum of all five digits in the code word 01905 is 15, which is divisible by three. If that code word arrived garbled as 01915, then the sum of its digits would be 16, which is not divisible by three, thereby indicating a problem with reception. The JN-25B garble check limited the number of different code words that could be used because only 33,333 five-digit groups are "divisible by three," in the manner described.

[43] NA II, MMRB, RG38, Crane Naval Support Group, 370/44/16/5, Box 115, 5750/198 – *CNSG, OP-20-GY.*

44 Ibid. See also Budiansky, *Battle of Wits,* 8, 364.

[45] Parker, "The Unsolved Messages," 298. The USN may have "penetrated" JN-25B additives throughout 1941 because it used tabulating machines and difference tables as aids to additive recovery. Holtwick briefly described the utility of these techniques in SRH-355, 399.

in 1941.[46] Alternatively, the *History of GYP-1* explains that the discovery of "a number-date table in Baker code" placed the reading of JN-25B messages "on a current basis," although in a limited way: "The reading of messages in Baker code before Pearl Harbor, however, must be understood to have been a qualified success. Current messages were read on Corregidor but they were few in number and invariably ship movement reports: arrivals and departures, together with some fragmentary schedules."[47] The preceding assessment suggests that Station Cast in Corregidor was limited mainly to reading numbers and dates sent in JN25B. Clearly, these conflicting interpretations must result from conflicting sources.

Yet certain testimony suggests that the USN could more than partially read JN-25B in 1941. Winston Churchill offered a tantalizing assessment in *The Grand Alliance:* "From the end of 1940 the Americans had pierced the vital Japanese ciphers, and were decoding large numbers of their military and diplomatic telegrams."[48] More significantly, Captain Laurance Safford, head of OP-20-G, discussed JN-25B reading ability in a memorandum of 17 May 1945:

> Corn 16 [Station Cast] intercepts were considered most reliable ... not only because of better radio reception, but because Corn 16 was currently reading messages in the Japanese Fleet Cryptographic System (5-number code or JN-25) and was exchanging technical information and translations with the British at Singapore [FECB]. As regards the JN-25 system the current version (JN-25b) had been in effect since 1 December 1 1940 [and] remained in effect until 27-31 May 1942, and was partially readable in November 1941.49

In August, 1970, Safford reaffirmed his views: "By Dec.1/41, we had the code solved to a readable extent."so

Testimony also shows that burglary accounted for access to other Japanese code systems. Farago, in his postscript to the paperback edition of *The Broken Seal,* offered the following testimony:According to Mr. Lee Strobel, an expert locksmith who serviced the formidable safes of the Japanese Consulate General in Los Angeles, he was

[46] NA II, MMRB, RG38, Crane Naval Support Group, 370/44/16/5, Box 115, 5750/197 — *CNSG, Activities and Accomplishments of GY-1 During 1941, 1942 and 1943.* The file is also known as *OP-20-GY History.*

[47] NA II, MMRB, RG38, Crane Naval Support Group, 370/44/16/5, Box 116, 5750/202 — *CNSG, History of GYP-1,* 25-6. The file is also known as *History of OP-20-GYP-1 WWII.* Alternative listing: *History of GYP-1,* Series IV.W.I.5.13, Center for Cryptologic History, National Security Agency.

48 Winston S. Churchill, *The Grand Alliance* (Boston, 1950), 598.

[49] Quoted, Letter dated 17 May 1945, from Cmdr. Laurance F. Safford to Lt. Cmdr. John F. Sonnett, Rusbridger and Nave, *Betrayal at Pearl Harbor,* 169-70. Indeed, Rusbridger and Nave claim that Britain's cryptology unit, the Government Code and Cipher School (GCCS), had "300 people working solely on JN-25," an effort eclipsing that of the USN.

50 SRH-355, 398.

> approached in December 1940 [when JN-25B first appeared] by a man who introduced himself as "Captain Webb of the U.S. Office of Naval Intelligence," and was, with an eloquent appeal to his patriotism, persuaded to `crack' the Consulate's safe, thus aiding `Webb' in the removal of a Naval code the Japanese were supposed to be keeping in it. Mr. Strobel agreed, the safe was opened surreptitiously, the code was found and removed — but it never appeared in any of the later accountings of Japanese crypt-material the Americans had at their disposal'

Farago, explaining this lack of accounting, suggested that Captain Webb was a British agent and that if the British received the code, they failed to inform the Americans. It is more likely, however, that the USN limited the disclosure of its sources for security reasons. Other testimony offered in Farago's postscript discussed the seizure of Japanese merchant navy codes. On 28 May 1941, George Muller, a US Customs Service agent cooperating with Cmdr. R.P. McCullough of the 12th Naval District in San Francisco, boarded the Japanese merchant vessel *Nisshin Maru II* and seized its codebooks.[52] McCullough later brought copies of the codebooks to Washington. Layton, as mentioned, explained that in 1941 Lt. Cmdr. Alwin Kramer, a naval intelligence officer with OP-20-G, stole and made photo-prints of Japanese code books located in New York consulates. There is no evidence that the Navy Department ever stole the JN-25B codebook, although "direct" recovery of Japanese merchant naval codes (i.e., the "S" code) may have provided a better understanding of Japanese terminology and code-vocabulary.

Apart from testimony, other evidence indicates USN code-reading ability. As Stinnett observed, communications intelligence summaries (COMSUM 14s) produced by Station Hypo for Admiral Kimmel demonstrate 5-Numeral Code reading ability on seven different occasions between 4 September and 16 November 1941.[53] Yet inexplicably, no COMSUM14 refers to the 5-Numeral Code again until 19 December, well after the Pearl Harbor attack. The Station Cast Chronology for 16 October 1941 also demonstrates text reading ability: "Itsu Aba Radio (Spratley Isl) was noted originating despatches containing direction finder bearings. Partial breakdown of despatches disclosed that the bearings were taken on two moving targets. These bearings might possibly be on the movement of Cardiv-4 from Sasebo to Takao area."[54] Another example of Station Cast's text reading ability may be found in a COM16 report of 29 November 1941:

---

51 Ladislas Farago, "POSTSCRIPT: New Lights on the Pearl Harbor Attack," *The Broken Seal: "Operation Magic" and the Secret Road to Pearl Harbor* (New York, 1968), 392.

52 Ibid., 393-5.

53 Stinnett, *Day of Deceit,* 133-4. The following COMSUM14s from 1941 show 5-Numeral Code reading ability: 4 and 24 September; 4, 14 and 23 October; and 13 and 16 November. See NA II, MMRB, RG38, Crane – Inactive Stations, 370/27/23/5, Box 3, 5510/4 – *N.4VSECGRU, Fourteenth Naval District Combat Intelligence – Unit Traffic Intelligence Summaries: 16 July to 31 Dec 1941.* Hereafter, communication intelligence summaries produced by Station Hypo (COM14) will be cited as COMSUM14 followed by the date.

54 NA II, MMRB, RG38, Crane – Inactive Stations, 370/27/23/7, Box 16, 3220/3 – *NSRS Philippines, Chronology,* Station C Chronology, 16 October 1941, 86.

> The following encrypted addresses have been noted in the past 2 days' traffic:`Comdr 1ST PATROL FORCE' ... `5`h Air Battalion' ... 3RD FLEET Headquarters'... CinC 3' FLEET shifted flag from the ASHIGARA to the NAGARA; CinC 2ND EXPEDITIONARY FLEET shifted flag from the KASHII to a unit tentatively identified as the CHOKAI ... The CinC 2ND FLEET indicates he will shift communications from the Kure Communication Zone at 0400, 29th; from the Sasebo Communication Zone at 0000, 1st; and enter the Bako Communication Zone at 0000, 2", thus implying a move from Japan proper to the South.55

In late November 1941, Station Cast was reading encrypted addresses and some message text. The preceding report must have been based on JN-25B naval messages: Senior Japanese naval commanders not only initiated the messages, but also discussed naval ship movements.56

Certainly, the ease with which the next additive of JN-25B was solved following the Pearl Harbor attack suggests that good progress had been made on earlier versions. Safford originally made this point in his memorandum of 17 May 1945: "A new system of keys [Additive 8] was introduced on 4 December 1941 and reported by Com 16 [Station Cast] but the carry over of the old code made their solution quite simple and we were reading messages again by Christmas, Corregidor getting the initial break on 8 December 1941."57 Indeed, on 15 December, Station Cast offered to send code recoveries on the "current period" to OP-20-GY if requested.[58] Only three weeks after commencing work on Additive 8 on 17 December, Lt. Cmdr. J.J. Rochefort, chief of the Combat Intelligence Unit at Station Hypo, started getting results with help from Station Cast.[59] As well, Parker explained that USN cryptanalysts had the ability to read JN-25B8 by February 1942, only about twelve weeks into the new additive period.[60] The USN had more resources for cryptanalysis following the outbreak of war, but JN-25B7 reading ability was seemingly well developed in the crucial months before the Pearl Harbor attack.

Contemporary letters, however, offer further insight into the USN's approach to cryptanalysis. In late 1941, OP-20-GY chose to decrypt traffic from earlier additive periods

---

55 NA II, MMRB, RG38, Records of the Chief of Naval Operations, *Translations of Intercepted Enemy Radio Traffic and Miscellaneous World War II Documentation, 1940-1946,* 370/6/26/6, Box 2684, COM16 Report dated 29 November 1941 (COM16-291029-TI).

56 For other interpretations of the COM16 report of 29 November 1941, see Parker, *Pearl Harbor Revisited,* 78; and Stinnett, *Day of Deceit,* 73. Stinnett regarded this particular message as an example of Station Cast's ability to read two Japanese naval codes: the 5-Numeral code and the Ship Movement (SM) code.

57 Cmdr. Laurance F. Safford to Lt. Cmdr. John F. Sonnett, 17 May 1945, cited in Rusbridger and Nave, *Betrayal at Pearl Harbor,* 169-70. See SRN-116741 for evidence that the Japanese navy permitted Additive 7 to be used simultaneously with Additive 8 in the period immediately following the introduction of Additive 8. 5s Cited in *Ibid.,* 168.

59 Layton, et al., *And I Was There,* 339-40.

60 Frederick Parker, *A Priceless Advantage: U.S. Navy Communications Intelligence and the Battles of Coral Sea, Midway, and the Aleutians,* United States Cryptologic History, Series IV, World War II, Vol. 5 (Washington, DC: Center for Cryptologic History, National Security Agency, 1993), 20.

in its attempt to recover JN-25B code values. This approach guaranteed "book-building," but at the expense of current additive recovery. In a letter of 24 October, Lt. L.W. Parke, head of OP-20-GY, offered the following instructions to Lt. John Lietwiler, co-commander of Station Cast: "We are almost ready to begin work on the period recently ended [JN-25B6, 1 February to 31 July]. If you have stopped your efforts on it, please let us know. I expect to have an official directive sent to you soon in that regard, so we won't be duplicating work."[61] In a letter of 19 November, Lt. Robert Densford, also with OP-20-GY, offered further explanation to Lietwiler: "Since you are working on the current AN period [JN-25B7, commencing 1 August], we are shifting to the February-July period. We assume that all recoveries from you and Singapore for that period are now in our hands."[62] Furthermore, OP20-GY continued to have Station Hypo toil away on the infrequently used Japanese Navy Flag Cipher, or AD code. Densford explained to Lietwiler on 19 November that Station Hypo was not able to crack this code: "As for the AD or `successor to the 45 sign code', we ain't got some. Honolulu has been amazingly reticent; they won't even mention the business. Presumably, then, it has not been cracked, and we so notified London long ago. They should inform Singapore."[63] The AD code seemed to be a waste of Station Hypo's resources, given that the station had IBM machines and seven translators at its disposal.64

Meanwhile, Station Cast successfully decrypted JN-25B throughout 1941. Equipped with IBM machines, Station Cast mechanically processed great volumes of intercepted traffic.[65] In May, Lt. Rudolph Fabian, commander of Station Cast, sent OP-20-G 159 negatives of code books, including 44 negatives of the "Five numeral book – subtractors" and 12 negatives of the "Five numeral code book and instructions."66 In a letter of 30 August, Fabian told Safford of the progress made on JN-25B6: "Of course, with the recovery of the new cipher in the AN we will be that much better off - it was wonderful in the last cipher period to recognize a movement, recover the cipher, and have all the R.I. [radio intelligence] deductions confirmed and made more positive ..."67 In the same letter, Fabian told Safford that the current code period, JN-25B7, was beginning to yield results: "The new cipher has

61 3200/1 — *NSRS Philippines, Operations Summaries,* Lt. L.W. Parke, Navy Dept., Washington, to Lt. John Lietwiler, Fort Mills, PI [Philippine Islands], 24 October 1941.

62 NA II, MMRB, RG38, Crane — Inactive Stations, 370/27/23/7, Box 15, 1300/1 — *NSRS Philippines, Assignment & Distribution,* Lt. Robert Densford, Navy Dept., Washington, to Lt. John Lietwiler, Fort Mills, PI, 19 November 1941, 3.

63 *Ibid.*

64 Layton, et al., *And I Was There,* 358.

65 Station Cast's IBM equipment included a Type 405 alphabetical tabulator, Type 075 sorter, type 035 punch and Type 513 reproducing gang punch. For a summary of Station Cast's machine installation, see NA II, MMRB, RG38, Crane — Inactive Stations, 370/27/23/7, Box 18, 5750/4 — *NSRS Philippines, History, General,* 52. For an excellent study of machine cryptanalysis, see Cipher A. Deavours and Louis Kruh, *Machine Cryptography and Modern Cryptanalysis* (Dedham, MA, 1985).

66 3200/1 — *NSRS Philippines, Operation Summaries,* Lt. Rudolph Fabian, Fort Mills, P.I., to The Chief of Naval Operations, Navy Dept., Washington, 5 May 1941.

67 1300/1 — *NSRS Philippines, Assignment & Distribution,* Lt. Rudolph Fabian, Fort Mills, P.I., to Cmdr. Laurance Safford, Navy Dept., Washington, 30 August 1941, 1.

finally started `giving' - now all we lack is sufficient material to prove it ...' Also in his letter to Safford, Fabian urged OP-20-G to work on the current code period: "I sent the letter suggesting that OPNAV work on the current cipher period because it seemed that the info in current intercepts fed back into R.I. would be the best and fastest way of getting the Orange [Japanese] Fleet organization straightened out - it worked so well here that one more source feeding cipher back would have made it work still better."[69] Clearly, successful decryption of JN-25 helped confirm other sources of radio intelligence.

Yet Station Cast made even greater strides in decrypting JN-25B7 in late 1941. In a letter of 6 October, Lietwiler explained to Densford how Station Cast's "Jeep IV" mechanical tabulator aided in the decryption of Additive 7. "We ... hit the jackpot on the second trial, so the Jeep made a lot of face in a hurry. We are now beginning to break into the additive for this period, and the mathematics solution for indicator subtractors is a great help. It works especially well since there are apparently only 500 keys, and also since quite a few people are `tailing' consistently."[70] Seemingly, machine cryptanalysis offered some assistance in the recovery of code additives.

By November, however, Lietwiler's staff relied on manual solutions to Additive 7 as the novelty of using the "Jeep IV" wore off, considering the time required to set up the machine. Station Cast resorted to "difference tables" as an aid to additive recovery. Difference tables represented the most common differences between code values found in frequently-used message texts associated with pattern naval messages. When such pattern messages were found to be superenciphered with the exact same group of additives, the underlying code values of the text could be estimated using difference tables, thus allowing the remaining value of the additives to be determined. In a letter of 16 November 1941, Lietwiler, responding to Parke's letter of 24 October, explained this process:

> Using the 400 high frequency groups we have compiled a table of 24,000 differences. When we are stuck on a column now we take any likely looking group and subtract it from every other group in the column from the master group. By reference to the table, the groups which produce these differences are found and tried in the proper spots, i.e., on the master group in the case of the original column, and on the columnar group in the case of the reciprocals. Two days ago I saw MYERS walk right across the first 20 columns of a sheet using this method almost exclusively. In view of this I do not believe we want a new Jeep IV.'

Lietwiler also furnished definitive evidence of Station Cast's ability to read JN-

---

69 Ibid., 2.

Ibid., 3.

[70] 1300/1 — *NSRS Philippines, Assignment & Distribution,,* Lt. John Lietwiler, Fort Mills, P.I., to Lt. Robert Densford, Navy Dept., Washington, 6 October 1941, 1.

[71] 3200/1 — *NSRS Philippines, Operations Summaries,* Lt. John Lietwiler, Fort Mills, P.I., to Lt. L.W. Parke, Navy Dept., Washington, 16 November 1941, 1.

25B7. In the same letter of 16 November, Lietwiler explained to Parke how Station Cast successfully read JN-25B7, requesting that OP-20-GY assist with current traffic decryption:

> We have stopped work on the period 1 February to 31 July as we have all we can do to keep up with the current period. We are reading enough current traffic to keep two translators very busy, i.e., with their code recovery efforts, etc. included. In this connection, I certainly wish you could see your way clear to drop the ancient history side of this cipher and work with us on each current system as it comes up. With Singapore, we have adopted a system of exchanging block numbers to prevent duplication. We have more or less given them a free hand in selecting the cipher blocks they tackle on account of their more limited traffic.72

The translators at Station Cast not only read current traffic, but also assisted in the recovery of code values. Lietwiler's remarks clearly show that JN-25B7 was readable in 1941, although the security classification of relevant contemporary records obscures the results of decryption.73

Nonetheless, USN intercepts of Japanese traffic may be evaluated for their possible intelligence value in 1941. To begin with, later publications of pre-Pearl Harbor messages show that the bulk of intercepted Japanese naval traffic was indeed sent in JN-25B. SRH406, entitled *Pre-Pearl Harbor Japanese Naval Despatches,* includes 188 Japanese despatches from 1941 that were decrypted and translated by the USN in 1945-46. These 188 despatches were selected from a group of 2,413 translated despatches that, in turn, were selected from a collection of 26, 581 decrypted despatches. An original copy of SRH-406 shows that about 90% of all intercepted Japanese messages were encrypted in JN-25B, a code that the USN could partially read in 1941.[74] Of course, the SRH-406 collection, in its

---

[72] *Ibid.* Leitwiler's letter to Parke is also discussed in a USN military history of the Philippines found in 5750/4 — *NSRS Philippines, History, General,* 54. Historians continue to debate USN code reading ability. Budiansky's assessment of OP-20-GY status reports led him to conclude that only 3800 JN-25B code groups, along with 2500 additives (Additive 7), had been recovered by November 1941: "It was far less than 10 percent of the total, nowhere near enough to read current traffic." See Budiansky, *Battle of Wits,* 8. Yet Lietwiler's letter of 16 November to Parke clearly states that Station Cast was reading current traffic. Perhaps the OP-20-GY status reports do not reflect the *entire* range of code groups and additives that were recovered by the USN and its Allies. Moreover, it is possible that the USN had solved the particular additives that Japanese code clerks used repetitively, and had solved the code values most frequently used in pattern naval messages.

[73] Past censorship has taken its toll. An index to the USN's depository at Crane, Indiana, the contents of which were moved to the National Archives II in 1994, shows that several files end well before December 1941. For example, Station Cast's *Miscellaneous Japanese Translations* file ends at 30 March 1941. Station Cast's *Communication Intelligence Reports* file ends on 30 April 1941. Moreover, files entitled *Japanese Navy Addresses, Japanese Navy Callsign Data, Japanese Navy Communications Data,* and *Japanese Navy Movement Reports* all end on 31 October 1941.

[74] Brian Villa located an original copy of SRH-406 and noted that the majority of intercepted Japanese messages had been encrypted in JN-25B. Indeed, the document lists the number of messages encrypted in each of five Japanese code systems. Out of 26,581 decrypts of messages intercepted between September and December, 1941, 23,778 used JN-25B, 819 used JN-20-C, 631 used JN-39, 426 used JN-161, and 927 used JNA-20. These figures

final form, dates from 1945-46; it proves which messages the USN intercepted in 1941, but it does not prove which messages or message-fragments were decrypted and translated in 1941. Other intercept collections, if they exist and are eventually released, may prove the latter point.[75] The task at present, however, is to emphasize that the USN could partially read JN-25B in 1941, that the USN intercepted over 26,000 Japanese naval messages between September and December 1941, and that about 90% of these messages were in JN-25B. But what important intelligence did these messages contain?

Apparently, message headings alone revealed the existence of a Strike Force. In October and November of 1941, the USN intercepted several messages addressed to the Strike Force.[76] The first mention of the Strike Force occurred as early as 13 October, when a Combined Fleet despatch gave instructions for communication drills to the "STRIKING FORCE" and the "ADVANCED EXPEDITIONARY FORCE."[77] The address of the preceding message had not even been encrypted within the main text. Although the Japanese began burying their address headings in encrypted text by early November, Station Cast could very likely read these addresses in JN-25B7.[78] Japanese despatches of 9 and 11 November provided the composition of the Strike Force in their address headings.79 Furthermore, Parker explained that two messages of 16 November, SRN-115430 and SRN-116430, "revealed details of designator list and scope of forthcoming fleet operations."80 Japanese messages were even sent to the Strike Force after it departed Hitokappu Bay on 26 November. For example, despatches of 28 and 30 November were both addressed to the Strike Force.[81] Message headings confirmed the existence of the Strike Force until the very

---

show that 89.5% of all decrypts had been originally encrypted in JN-25B. See NA II, MMRB, RG38, Crane Naval Support Group, 370/44/18/1, Box 183, 5830/115 – CNSG, *Pre-Pearl Harbor Japanese Naval Despatches.*

75 Alternatively, a textual analysis of the SRH-406 and SRN collections may show that some of the messages were read in 1941, but reassessed in 1945-46 for the purpose of being included in a more comprehensive collection of recently translated messages. Textual analysis might include the study of call sign lists, message addresses and translators' remarks. The author is grateful to Prof. Brian Villa for originally making these observations.

76 SRNs 116430, 116431, 116432, 116433 and 116434.

77 SRH-406, Chapter 1, 9.

78 As previously mentioned, the COM16 report of 29 November 1941 (COM16-291029-TI) demonstrates that Station Cast could read encrypted addresses. Furthermore, an original, uncensored copy of SRH-406 shows that the external address of a message could be compared with its internal encrypted address to compromise the identity of the address list. For example, regarding Message No. 951 dated 27 November 1941, the editor of SRH-406 offers the following explanation: "Note how the internal heading compromises the external heading. Now we are positive SI WI 1 is the Striking Force." The SRH-406 collection, in its final form, dates from 194546, but nevertheless offers some indication of how message headings might have been compromised in late 1941. Seemingly, even after the Japanese navy began burying messages addresses within encrypted text in early November 1941, the external address offered some indication of identity. A full explanation of how Japanese naval messages were structured and encrypted after early November 1941 will have to await the release of 1941 USN decrypts and worksheets, if they still exist.

79 SRNs 115709 and 115787. The message of 9 November concerns secret training exercises for fuelling at sea, whereas that of 11 November concerns anchorages assigned in Saeki Bay.

80 Parker, *Pearl Harbor Revisited,* 59.

81 SRNs 115690 and 115460. The message of 28 November is a weather report, whereas that of 30 November is a list of geographic designators such as "AI" (Oahu) and "AF" (Midway).

end of November 1941. As well, given that British Intelligence had become aware, by November 1941, that the Japanese navy had formed a "special task force," it is not unreasonable to assume that the USN came to the same conclusion.[82]

Other messages intercepted by the USN alluded to Japan's intentions in the Pacific. Not surprisingly, many messages correctly showed that Japan had military intentions in the south. An enormous amount of intelligence pointed to targets in Southeast Asia. Yet many naval messages encrypted in JN-25B suggested that Japan intended to launch a trans-Pacific raid on capital ships anchored in shallow waters. Parker's study of 1991, entitled "The Unsolved Messages of Pearl Harbor," demonstrates that several Japanese messages intercepted by the USN pointed to an attack on Pearl Harbor. Disregarding Parker's contention that these messages were not readable when originally intercepted, the messages may be assessed in terms of their possible intelligence value in 1941. Expressed in Wohlstetter's terms, certain "signals" could have soared well above the background "noise" of information.

Indications that the Japanese navy was preparing for war came early *in* this coded traffic. On 5 September, the 2nd Fleet chief of staff transmitted the following directive to his fleet: "A STATE OF COMPLETE READINESS FOR BATTLE OPERATIONS MUST BE ACHIEVED BY THE FIRST OF NOVEMBER ..."[83] On 9 September, the Combined Fleet chief of staff explained to all fleet chiefs of staff and all fleet commanders that "AS CONDITIONS BECOME MORE AND MORE CRITICAL EACH AND EVERY SHIP UNIT WILL AIM AT BEING FULLY PREPARED FOR COMMENCING WAR OPERATIONS BY THE FIRST PART OF NOVEMBER ..."[84] Evidently, war was coming in late 1941.

USN intercepts also indicated that a particular battle plan had emerged. On 6 October, the 1st Air Fleet staff offered the following drill instructions to various commanders: "IN FIRST AIR FLEET AERIAL TORPEDO ATTACK DRILL #13 WHICH IS SCHEDULED TO BE CONDUCTED ON 21 OCTOBER AGAINST BATTLESHIP DIVISION 1, AKAGI AND KAGA ARE EACH ALLOTED 9 TORPEDOES AND SOORYUU AND HIRYUU ARE EACH ALLOTED 6 TORPEDOES."[85] Drills simulating aerial torpedo attacks on battleships placed the 1st Air Fleet in a special category of training: these drills echoed the tactics that had insured a British victory at Taranto on 12 November 1940. Moreover, special shallow-water torpedoes were being developed as outlined in this 28 October message from the 1st Air Fleet chief of staff:

> ON 30 OCTOBER, THIS FLEET WILL PICK UP FROM 5 TO 10 NEAR SURFACE(?) TORPEDOES AT SASEBO MILITARY STORES DEPARTMENT(.) CLASSES ON THIS TORPEDO WILL BE HELD AT

---

[82] Public Records Office (PRO), ADM 223/494, Far East and Pacific: 1, History (1926-1946), *Pearl Harbor & the loss of Prince of Wales & Repulse,* 1.

Cited in Parker, "The Unsolved Messages," 301.

[84] SRN-115533, cited in Parker, "The Unsolved Messages," 302.

85 SRN-117453, cited in *ibid.*

> KANOYA FOR ABOUT FIVE DAYS FROM THE 31ST AND THEN WILL BE SHIFTED TO FIRING PRACTICE.... BY WORKING NIGHT AND DAY, IT SHOULD BE POSSIBLE TO COMPLETE 10 (A SPECIAL ATTACHMENT FOR TORPEDOES, PROBABLY BOW OR STERN PLANES) BY 5 NOVEMBER.86

Parker also produced evidence showing that "three carrier divisions totaling six carriers were to be equipped with the new torpedoes" and that "practice torpedo drills were to be conducted against anchored capital ships."[87] There were many capital ships anchored in the shallow waters of Pearl Harbor.

Furthermore, a message of 3 November from the 1st Air Fleet staff to the Saeki Air Base commander spelled out plans for a surprise air attack conducted in two waves:

> IN THE 3' SPECIAL DRILL IN AMBUSHING, 54 SHIPBOARD BOMBERS WILL CARRY OUT A BOMBING AND STRAFING ATTACK IN SIGHT OF SAEKI BASE FROM 0815 ON THE 4TH, 0715 ON THE 5TH AND 0815 ON THE 6TH, AND ABOUT AN HOUR OR AN HOUR AND A HALF AFTERWARDS 54 SHIPBOARD ATTACK PLANES WILL CARRY OUT A SIMILAR BOMBING ATTACK.88

Such messages made clear the battle tactics being perfected by the 1st Air Fleet, even if they did not allude to the location of the intended target. It is interesting to note that on 5 November, Admiral Kimmel issued a report to the Pacific Fleet entitled *Aircraft Depth Bomb Alert Watch.*[89] Whether or not Kimmel received intelligence reports based upon decrypts of recent Japanese messages or simply exercised caution on his own initiative remains unknown.

Apart from battle tactics, clues relating to long-distance carrier refuelling appeared in other Japanese messages. Japanese oil tankers, or *Marus,* were engaging in carrier refuelling exercises, as this 30 October message from the 1st Air Fleet chief of staff demonstrates:

> WHEN INSTALLATION OF GEAR FOR REFUELING UNDER TOW AND PREPARATIONS FOR ACTION HAVE BEEN COMPLETED, KUROSHIO (KOKU/CHOO) MARU AND SHINKOKU (KAMI/KUNI) MARU WILL DEPART SASEBO AND KURE RESPECTIVELY ON

---

86 SRN-117301, cited in *ibid,* 302-3. All parentheses were added by the translator.

87 *Ibid.,* 303. See SRNs 116323 and 117665.

88 SRN-117665, cited in *ibid.,* 303.

89 National Archives – Pacific Alaska Region (NAPAR), RG181, 13th Naval District Commandant's Office, Classified Central Subject Files, 1934-41 (514955-61), 8/29/11, Box 8, File FF1/A2-11, Route Slip 4 December 1941, CINCPAC to Staff HQ, Thirteenth Naval District, Subject: *Aircraft Depth Bomb Alert Watch,* Serial no. 01765, 5 November 1941.

THE 13TH AND PROCEED TO KAGOSHIMA BAY, CONDUCTING EXERCISES WITH CARRIERS ENROUTE. REQUEST THEY LOAD FUEL OIL FOR REFUELING PURPOSES BEFORE THEY DEPART.[90]

In November, messages showed that large quantities of fuel were being stockpiled and that plans were being made to carry extra fuel aboard carriers of the 1' Air Fleet.[91] Moreover, an oil tanker sent a message on 20 November stating that after loading fuel and aviation gasoline, it would join the Strike Force by 27 November.[92] The Strike Force evidently required a lot of fuel for a long voyage.

In late November, USN intercepts placed the 1st Air Fleet in the Kurile Islands, a likely point of departure for the North Pacific. A JN-25B message of 18 November sent from Tokyo to the chief of staff, Ominato Guard District, revealed the location of the 1st Air Fleet: "PLEASE ARRANGE TO HAVE SUZUKI (1776) WHO WAS SENT TO 1ST AIR FLEET ON BUSINESS PICKED UP AT ABOUT 23 OR 24 NOVEMBER AT HITTOKAPPU WAN ..."[93] In the preceding message, "HITTOKAPPU WAN," had been encrypted letter by letter rather than by a single code group – an easy decrypt for USN cryptanalysts. Furthermore, a message of 20 November concerning the movements of submarine I-19 confirmed that the 1" Air Fleet laid beyond Ominato: "I-19 WILL LEAVE YOKOSUKA COMM ZONE ON NOVEMBER 21 AND ENTER OMINATO COMM ZONE. AT 1600 NOVEMBER 22 WILL ENTER 1ST AIR FLEET FLAGSHIP COMM ZONE."[94] These changes in communication zones indicated a northern voyage from Yokosuka to Ominato and beyond. Certainly, the Kuriles lay beyond Ominato.

On the eve of the Pearl Harbor attack several USN intercepts pointed to a North Pacific operation. A message of 27 November addressed to the Strike Force discussed shipping conditions in the North Pacific: "ALTHOUGH THERE ARE INDICATIONS OF SEVERAL SHIPS OPERATING IN THE ALEUTIANS AREA, THE SHIPS IN THE NORTHERN PACIFIC APPEAR CHIEFLY TO BE RUSSIAN SHIPS ..."[95] This message explained that there were only two Russian ships westbound from San Francisco. Moreover, weather reports sent to the Strike Force from 28 to 30 November likely reflected weather conditions in the North Pacific.[96] In terms of direction-finding coverage, a JN-25B message of 29 November revealed that the Japanese were covering "U.S. ships and planes in the Northern Pacific" using the "#1 D.F. net".[97] As well, on 1 December, the oil tanker *Shiriya* sent a message conveying its position in the North Pacific to Destroyer Division 7 of the

---

[90] SRN-116588 cited in Parker, "The Unsolved Messages," 304. All parentheses were added by the translator.

[91] *Ibid.,* 304-5. See SRNs 117180 and 116566.

[92] SRN-115375; Layton, et al., *And I Was There,* 232, 548 n34.

[93] SRN-116643, Parker, "The Unsolved Messages," 307.

[94] SRNs 116329 and 116990 cited in *ibid.,* 309.

[95] SRN-116667, cited in *ibid.,* 310.

96 Ibid., 309. See SRNs 116668, 115460 and 115690.

[97] NA 11, MMRB, RG38, Records of the Chief of Naval Operations, *Translations of Intercepted Enemy Radio Traffic and Miscellaneous World War II Documentation, 1940-1946,* 370/6/26/6, Box 2684, Message No. 289 29 November 1941, Chief– Tokyo D/F Control, to various Communication Units, GZ # 1420-Z-DI.

Strike Force: "THE SHIP IS PROCEEDING DIRECT TO POSITION 30.00N, 154.20E. EXPECT TO ARRIVE AT THAT POINT ON 3 DECEMBER. THEREAFTER WILL PROCEED EASTWARD ALONG 30 DEGREE NORTH LATITUDE LINE AT SPEED 7 KNOTS."[98] This course, Parker calculated, placed the *Shiriya* in the North Pacific at 30° N, 170° E, on 7 December, Honolulu time. Clearly, the *Shiriya* supported a Strike Force operation in the North Pacific rather than in the south. Only the date of battle operations remained undisclosed. Yet on 2 December, the USN intercepted the famous "Climb Mount Niitaka" message, which told the Combined Fleet that hostilities would begin on "1208," or 8 December, Tokyo time: "THIS DISPATCH IS TOP SECRET. THIS ORDER IS EFFECTIVE AT 1730 ON 2 DECEMBER. CLIMB NIITAKAYAMA 1208, REPEAT 1208."[99]

USN intercepts of Japanese naval messages could have provided forewarning of the Pearl Harbor attack, provided that USN cryptanalysts read enough of the message texts in JN-25B. Parker succinctly summarized the intelligence value of these intercepts: "An objective extraordinarily far from Japan, the ambush of anchored capital ships, shallow-running torpedoes, six major carriers in a strike force, carrier fuel stored on deck, and a demonstrated interest in the waters of the northern Pacific – all these pointed inexorably to Pearl Harbor."[100] The Japanese offered important clues concerning their intentions in the North Pacific on the eve of the Pacific War.

In conclusion, USN cryptanalysis made important intelligence much more accessible in late 1941. Cryptanalysis most likely revealed the existence of a Strike Force and allowed numerical data such as ship schedules and positions to be read with relative ease. Evidently, Japanese messages transmitted primarily in JN-25B, a code that the USN could partially read, foretold of a long-range air attack on ships anchored in shallow waters. The sole fact that Station Cast was "reading enough current traffic to keep two translators very busy" in November 1941 suggests that at least a portion of Japanese message-texts were accessible to the USN prior to the Pearl Harbor attack. Again, the determination of which messages or message-fragments were read in 1941 will have to await the release of other intercept collections, if they exist. It must be noted that the selection, decryption and translation of the most relevant messages amongst many thousands of intercepts would have been an arduous task in 1941. The resources dedicated to the solution of JN-25B, rather than other code systems, remained limited. Nonetheless, our present understanding of USN cryptanalytic abilities in 1941 suggests that foreknowledge of Japanese intentions in the North Pacific was a possibility. The range of possible historical interpretations must now be redefined.

The new evidence lends more support to revisionist interpretations than to traditionalist interpretations. Wohlstetter, Kahn, Farago, Prange and Prados offered assessments of USN cryptanalysis that are no longer tenable. These authors, who were necessarily dependent upon limited sources, incorrectly asserted that USN cryptanalysts could not effectively read the principal Japanese naval code, JN-25B, and failed to appreciate

[98] SRN-115398, cited in Parker, "The Unsolved Messages," 306.
[99] SRN-115376, cited in *ibid.,* 312.
100 *Ibid.*

the intelligence value of messages encrypted in this code. Layton, Rusbridger and Nave, and Parker correctly appreciated the potential value of JN-25B messages, but incorrectly believed that such intelligence was inaccessible to USN cryptanalysts. Yet Rusbridger and Nave belong in a special revisionist category. The new evidence does not support their principal contention that the British read JN-25B while the Americans did not. Indeed, JN-25B was a joint project between the USN and its Allied counterparts. Station Cast in Corregidor exchanged code values with the FECB in Singapore. The new evidence, however, buttresses the revisionist positions advanced by Toland and Stinnett, although neither author proved that the USN could read JN-25B in late 1941. Toland did not address the issue, whereas Stinnett suggested only the probability of current decryption. Nonetheless, the new evidence supports any interpretation suggesting that USN code breaking may have provided foreknowledge of Japan's intentions.

Future interpretations of USN cryptanalysis must assess *how much* message text was currently read through JN-25B decryption, rather than questioning the very possibility of such decryption. Although past security classification, as well as missing or destroyed documents, make historical reconstruction more challenging, the historical discipline can at least establish the probability of either the traditionalist or the revisionist thesis within Pearl Harbor historiography. More importantly, completely different kinds of evidence may buttress the arguments made thus far. Historians may consider direction finding or traffic analysis in their assessments of pre-Pearl Harbor intelligence. It is likely that other signals intelligence techniques supported cryptanalysis. Historians must now turn to signals intelligence in their attempts to understand the events of 7 December 1941 because such methods had the potential to reveal Japan's intentions and actions in the North Pacific prior to Pearl Harbor attack. Wireless signals that once spanned the vast expanses of the Pacific now offer a new understanding of Pearl Harbor.

Decoding Pearl Harbor: USN Cryptanalysis and the Challenge of JN-25B in 1941, by Timothy Wilford [Article]. Family Grows Impatient Waiting for Exoneration of Adm. Kimmel, by James R. Carroll [Article]. The Final Secret of Pearl Harbor, by John T. Flynn [Article]. Freedom of Information Act Files Prove FDR Had Foreknowledge of Pearl Harbor?Â Revisionism and the Historical Blackout, by Harry Elmer Barnes [Article]. Robert Stinnett Responds to NSAâ€™s Pearl Harbor Claims, by Anthony Gregory [Article]. Seventy-two Years of Infamy, by Anthony Gregory [Article]. Things You Canâ€™t Say in America FDR Knew About the Attack on Pearl Harbor, by Alexander Cockburn [Article]. The Truth About Pearl Harbor: A Debate, with Robert B. Stinnett vs. Stephen Budiansky. The 1941 edition (JN-25b) was sufficiently broken by late May 1942 to provide the critical forewarning of the Japanese attack on Midway. British, Australian, Dutch and American workers were cooperating in attacks on JN-25 well before the Pearl Harbor attack, but because the Japanese Navy was not engaged in significant battle operations before then, there was little traffic available to use as raw material. Before then, IJN discussions and orders could generally travel by routes more secure than broadcast, such as courier or direct delivery by an IJN vessel.Â "Decoding Pearl Harbor: USN Cryptanalysis and the Challenge of JN-25B in 1941", in The Northern Mariner XII, No.1 (January 2002), p.18. Wilford, p.18. Wilford, p.20: citing Kahn, The Codebreakers.