DOCID: 3928669

Approved for release by NSA on 12-01-2011, Transparency Case# 63852

Now Playing: Churchill as Pearl Harbor Villain

Book Review

Betrayal at Pearl Harbor. How Churchill Lured Roosevelt into World War II. By James Rusbridger and Eric Nave. 303 pp. Summit Books, New York, 1991. $19.95

If you are a devotee of fantasy, this may be your cup of tea. But do not make the mistake of thinking that you are reading history. Many of the 180 pages of text in this volume are, indeed, filled with retold stories of the development of communications intelligence (Comint) in World War I and between the wars and descriptions of how events unfolded preceding and during World War II. Much of this information is factual but neither new nor illuminating, while the remainder is misinterpreted to fit a new conspiracy theory, enunciated in the subtitle. Examination of that theory has led to the *caveat emptor* that follows.

Much in the manner of William Stevenson, who wrote *A Man Called Intrepid,* published in 1976, James Rusbridger gathers his wool from elderly gentlemen recalling heroic events from World War II almost fifty years after the fact and spins it into an imaginative fairy tale. The strands of this fantasy are so interwoven with historical fact that it is difficult to treat the work as a whole. The conspiracy theory yields to analysis, however, if one studies it alone, and then, when its elements are clearly defined, subjects it to the test of established fact and historical evidence. Such a treatment tends to emphasize the basic difference between writing history and concocting conspiracy theories. The former may involve positing a hypothesis based on a limited body of evidence, but then the hypothesis must be tested against all available evidence before it can pass the test of credibility and be accepted as a theory. The procedure for concocting conspiracy theories is less rigorous, one gathers: simply generate a hypothesis to fill a lack of evidence, pull together some

sort of flimsy "body of evidence," and then blame the lack of really convincing evidence on a subsidiary conspiracy to conceal or destroy that evidence.

Basically *Betrayal at Pearl Harbor* argues that British Prime Minister Winston Churchill concealed advance knowledge of the planned Japanese attack on Pearl Harbor from President Franklin D. Roosevelt in order to insure the attack's success and the United States' responsive entry into the war against the Axis powers. The reviewer's interest and competence in this matter is based on his career in Comint, which is portrayed as the source of Churchill's foreknowledge. This reviewer contends that the information purportedly withheld from Roosevelt did not exist, was not available to Churchill or anyone else, and that *Betrayal at Pearl Harbor* makes a feeble case for a conspiracy theory based upon hearsay and misconstrued bits and pieces of information misleadingly presented as "evidence." This review focuses on those parts of the book that pertain to cryptology and does not attempt to deal with every distortion and such general questions as the credibility of attitudes, thoughts, and actions attributed to members of the cast.

The Plot

Even a poor conspiracy, like good fiction, requires a plot. The Rusbridger plot revolves around a villain , Churchill, who seldom appears stage center, but remains in the wings or completely behind the scenes, rubbing his hands in glee as he successfully manipulates a cast of thousands in a scheme to lure President Roosevelt and the United States into World War II to save imperiled Great Britain. The only appearance of Churchill in an active role occurs after the war when he purportedly ordered some duplicate files destroyed, yet somehow he manages to entice Roosevelt into the war by concealing from him knowledge of Japan's plan to attack Pearl Harbor and immobilize the Pacific Fleet. By thus insuring the success of Japan's

plan, Churchill is apparently confident that the American citizenry, in righteous anger and seeking revenge, will eagerly follow Roosevelt's leadership into the war against Japan and that Hitler will cooperate by declaring war against the U.S. There are three sub-plots: how Churchill learned of Japan's plan; how Churchill kept Roosevelt from learning of it; and why Roosevelt did not learn of it from his own sources. There is also a sub-sub plot: how Churchill, even from the grave, kept everyone from knowing of his successful ruse for fifty years until Rusbridger was able to uncover the truth in time for the semicentennial of Pearl Harbor!

How the Plot Unravels

So how did Churchill know of the Japanese plan? According to Rusbridger Churchill knew that Japan would attack Pearl Harbor on 7 December 1941 because British and American cryptanalysts had been reading the Japanese naval general purpose code, designated by the Americans as JN-25. He says messages in this system decrypted by the British Far East Combined Bureau (FECB) in Singapore and the U.S. Navy's station Cast on Corregidor or at OP-20-G, the U.S. naval Comint organization in Washington, indicated both the target and the date of the Japanese attack. Churchill's objective was clear, at least to the author: "From the moment Churchill took office, he had but one aim, and that was to bring America into the war against Germany at any price." (page 90.) "...had Britain shared with the Americans its full knowledge of the work of FECB and GCCS [Government Code and Cipher School, the British Comint organization in England] against Japanese naval codes throughout 1941, the attack on Pearl Harbor would never have occurred, and Yamamoto's Task Force might have been decimated in a well-laid trap. The denial of this information was no accident but the deliberate policy of Churchill himself to achieve his aim of dragging America into the war." (page 154)

The problem with this argument, as is shown below, is that neither the British nor the Americans were actually able to extract significant intelligence from decrypts of JN-25 until after Pearl Harbor; therefore, Churchill simply did not possess the information that he is accused of keeping from Roosevelt.

Churchill's challenge, according to this book, was how to keep information about the impending Japanese attack from Roosevelt "because he believed it to be in Britain's interest that the Japanese attack Pearl Harbor in such a dramatic manner that it would brush aside any further thoughts of isolationism."(page 144) As far as how he concealed the British decrypts, Rusbridger gives us the answer: "One person who saw the raw decrypts of all important Japanese naval signals--particularly JN-25--was Churchill, no matter where he might be, and the decision to pass on this information in either its raw or paraphrased form to the Americans was a matter that he alone decided." (pages 92-93) The author gives no evidence to support Churchill's knowledge and use of JN-25 decrypts. If one accepts the fact that the "raw decrypts" described by Rusbridger did not exist, then, of course, it makes little difference how Churchill might have controlled their dissemination had he possessed them.

But what about the American decrypts? Rusbridger never implies any collusion between Churchill and Americans, but suggests that a high- ranking U.S. naval authority, acting out of distrust of Roosevelt's staff and of army officials who might become privy to the sensitive information, made the decision on his own to deny Roosevelt access to American decrypts of JN-25 messages, .

The decision to keep Roosevelt in the dark over JN-25 could only have been taken by a very senior naval officer, and the most likely candidate is Admiral Richmond K. Turner, director of the Navy's War Plans Division, who, without any apparent authority, assumed total control of the analysis and dissemination of OP-20-G's

output. Turner has been described as the Navy's Patton, and certainly his abrasive manner, distrust of the Army, and his open dislike of Roosevelt's aides all suit this description. (page 179) [i.e., he was not a very likable character and therefore makes a suitable villain.]

Without even considering whether one man could have successfully carried out the alleged concealment that involved so many different individuals, it is necessary again to emphasize that the decrypts never existed before the Pearl Harbor attack.

Now for the question of how this story remained untold until the eve of the semicentennial of Pearl Harbor. On the British side, "In 1945, immediately after the Japanese surrender, Churchill sent personal secret instructions to FECB (then in Ceylon), that all archives were to be destroyed, including those brought out from Singapore in December 1941 before the surrender in February 1942." (page 173) "Despite the destruction of FECB's records, copies of all their work remained with GCCS. These are under the control of GCHQ today and cannot be inspected, nor have they ever been made available for the official histories of British intelligence during World War II, which conspicuously ignore the work of British codebreaking against Japan prior to 1941." (page 174) Rusbridger's assertion that Churchill personally ordered destruction of the duplicate files on Ceylon is based solely on an interview with W. W. Mortimer , a veteran of FECB, in December 1989 (p. 173 and fn 32, p. 279) . It is difficult to believe that Churchill, while in power, would have involved himself personally in so routine a matter as destruction of duplicate files at a remote outpost. By the time of the Japanese surrender Churchill had been removed from office, so it is even more incredible that he would personally, as a private citizen, or as the opposition party leader, have issued secret orders to FECB . As is suggested below, the lack of information on British codebreaking efforts against Japanese

Naval targets before Pearl Harbor is probably due in large part to the disappointing results from those efforts.

As for the American decrypts, the author performs a somewhat more complicated maneuver. He complains that he was unable to find any JN-25 decrypts for the period before Pearl Harbor except for some of the 2,413 translations from the 26,581 Japanese naval messages (largely JN-25) sent during the period 1 September- 4 December 1941 but *only decrypted after the end of World War II* by OP-20-G. These 2,413 post-war translations were deposited in the National Archives in 1979, and a catalog of them was more recently released to the Archives as SRH-406. Rusbridger uses these translations, as does my colleague Frederick Parker in *A New View to Pearl Harbor*, to prove that JN-25 messages did contain intelligence that, *had they been decrypted and translated*, would have alerted commanders to the strong possibility of an attack on Pearl Harbor.[1] Rusbridger goes on , however, to claim, without offering any evidence at all, that these messages were decrypted and translated *before Pearl Harbor*. He argues that "It is also impossible to believe that the few [i.e., 2,413] pre-Pearl Harbor JN-25 decrypts in the National Archives (see Appendix 6) were only decoded in late 1945 and early 1946."(page 171). In view of seven investigations of Pearl Harbor that took place 1941-1945, "...it strains credulity to believe they [the U.S. Navy] would not have been sufficiently curious to know what these few [i.e., 26,581] intercepts contained and to have decoded them

1. David Kahn, respected historian of cryptology and author, among other works, of *The Codebreakers,* expressed some doubt at the Second Annual Cryptologic History Symposium, National Security Agency, Ft. Meade MD, November 1991, that analysts would have been able to sift out the essential warning information from the high volume of JN-25 traffic passed before Pearl Harbor. Prescott H. Currier, veteran U.S. naval Japanese linguist and cryptanalyst who worked on JN-25 at OP-20-G from 1939 until the end of World War II, stated in no uncertain terms that spotting the most significant traffic and working on it first became routine procedure in 1942 when timely exploitation of JN-25 commenced. He has no doubt that analysts would have recognized the significance of the pre-Pearl Harbor messages had they achieved the capability for current decryption of the messages in 1941, which, he states firmly, they had not.

as soon as possible."So he concludes "that these copies in the National Archives have been deliberately falsified in order to create the impression that JN-25 was not being read in 1941."(page 172) "At the bottom right-hand corner [of each translation] is the official date these messages were translated, which the authors of this book believe are false."(Appendix 6, page 1.) The author clearly believes that once the U.S. Navy realized the disaster it had caused, it did everything possible to cover its tracks!

Then, having used the postwar decrypts to prove the contents of the 1941 messages and to build up his cover-up sub-sub-plot, Rusbridger turns around and ignores them, declaring "every scrap of evidence relating to JN-25 between June 1939 through late November 1941 has vanished. Considering the historical importance of this material in the context of Pearl Harbor, it is impossible to believe that this could have happened throughout all the U.S. Navy's codebreaking offices, unless there had been a deliberate policy beginning in the immediate aftermath of the war to conceal or destroy all evidence relating to this code." (page 171) "This is not some casual cover-up but a carefully premeditated policy of deceit of the greatest magnitude that can only have originated from the highest authority to deliberately frustrate the truth being told." (page 173) A photograph of Admiral Turner opposite page 161 has a caption including the statement "After the [Pearl Harbor] attack, *it seemed* [italics mine] Turner ordered the destruction of all JN-25 material so that the role of U.S. Navy codebreakers could not be investigated." What is the evidence to support this accusation of "deceit of the greatest magnitude?" All the author has to offer is the innocuous "it seemed."

If, in fact, JN-25 messages had been routinely decrypted and translated before Pearl Harbor, it would, indeed, be strange that no record of them remained. If, on the other hand, decryption was only occasional and fragmentary, the evidence of this would be in the form of worksheets that might have been saved or destroyed depending on circumstances. The only U.S. work on current JN-25 prior to Pearl

Harbor took place on Corregidor. Certainly one would not expect that the cryptanalysts on Corregidor packed up their worksheets before their last-minute evacuation by submarine! Duane L. Whitlock, a U.S. naval intercept operator and traffic analyst who was conversant with the effort on JN-25 on Corregidor states, "I can attest from first-hand experience that as of 1 December 1941 the recovery of JN-25B [the second codebook in the JN-25 series] had not progressed to the point that it was productive of any appreciable intelligence--not even enough to be pieced together by traffic analysis. ... The reason that not one single JN-25 decrypt made prior to Pearl Harbor has ever been found or declassified is not due to any insidious coverup...--it is due quite simply to the fact that no such decrypt ever existed. It simply was not within the realm of our combined cryptologic capability to produce a useable decrypt at that particular juncture."[2] Rusbridger also fails to explain how the publication and deposit in the Archives of 2,413 translations fits into the cover-up scheme. If all those messages were really decrypted and translated before Pearl Harbor or even before the end of World War II, why were they not also destroyed or concealed ?

That is the basic skeleton of the conspiracy theory presented in *Betrayal at Pearl Harbor.*

The Evidence

The evidence assembled in *Betrayal at Pearl Harbor* begins with a lack of evidence described as "The strange gaps in the American archives, the censored words in what little material has been released by the National Security Agency, and the almost total absence of any reference to Japanese naval codes in postwar histories and the

2. Duane L. Whitlock, *And So Was I, (A Gratuitous Supplement to And I Was There, by Rear Admiral Edwin T. Layton, U.S.N. (Retired))*, (Danville, CA, 1986), 6. Unpublished manuscript in CCH.

eight Pearl Harbor inquiries." These "strange gaps" were supplemented and filled to Rusbridger's satisfaction by the recollections of Eric Nave, "the father of British codebreaking in the Far East," as recounted "with perfect recall" at age eighty-nine in 1988 (page 10) and W.W. Mortimer. Eric Nave is an accomplished Japanese linguist, Australian by nationality, who served with GC&CS and was well grounded in cryptanalysis of Japanese systems. He was at FECB, Singapore, from September 1939 until February 1940, when he was reassigned to Australia and had no further direct involvement with JN-25.[3] W.W. Mortimer also served at FECB even after Pearl Harbor and the evacuation from Singapore, but it is not clear to what extent he was involved with JN-25, if at all. If either he or Nave read the manuscript of this book without recognizing the erroneous statements about JN-25, then they could not have been at all close to the problem. This applies particularly to the misconception that there was a single unchanging JN-25 codebook.

The first and most important contention of Rusbridger's argument is that JN-25 could be readily decrypted and translated by British and American Comint personnel so as to produce meaningful intelligence in time to warn of the Pearl Harbor attack. This subject deserves treatment in some detail even if at the expense of passing over some of the more egregious assaults on logic and historical method launched in this volume.

How Successful Were the British and American Efforts Against JN-25?

At the time that *Betrayal at Pearl Harbor* reached this reviewer's desk, he was drawing up a statement on the subject "JN-25 Before Pearl Harbor" to be used by Mr. Frederick Parker, a colleague at the Center for Cryptologic History, in support of

3. Geoffrey St. Vincent Ballard, *On Ultra Active Service,, The Story of Australia's Signals Intelligence Operations during World War II* (Richmond, Victoria, Australia:Spectrum Publications, 1991), 164.

his paper, *A New View to Pearl Harbor.* The statement attempts to explain the nature of JN-25 and show that reading of messages in that system during the period before Pearl Harbor was very limited, fragmentary in nature, and never quick and easy. The statement follows in its entirety.

JN-25 Before Pearl Harbor

JN-25 is a U.S. designator for a series of enciphered codes used for general purposes by the Japanese navy during the period 1939-1945. The following summary based upon all sources available to the Center for Cryptologic History pertains only to the JN-25 enciphered code used by the Japanese navy during the period immediately before the attack on Pearl Harbor.

The second Japanese codebook in the series, JN-25B, was introduced on 1 December 1940. It consisted of 33,333 potential code groups of which approximately 27,500 were assigned two distinct meanings for a total of 55,000 code values. As of January 1941, approximately 2,000 (4%) of these code values were probably recovered, consisting overwhelmingly of numbers 000 through 999 and values used in stereotype messages, e.g., the endless ship movement reports and the medical reports that were judged to be of little value. Until August 1941, efforts to recover JN-25B code values were restricted to the British force at the Far East Combined Bureau (FECB), Singapore, and four U.S. officer-linguists at Corregidor, working in close collaboration with the British. In August 1941, OP-20-G, Washington, began to help with JN-25B code recovery, but was hampered by lack of linguists familiar with Japanese naval terminology and usage and by the slow communications available at the time.

On 1 August 1941, the seventh JN-25 additive book, JN-25B7, was introduced. It consisted of 500 pages, each containing 100 random five-digit groups to be used in enciphering the JN-25B coded messages.

In order to read messages encrypted in JN-25, cryptanalysts and linguists working closely together had to recover several vital elements of information including: an enciphered indicator showing whence in the additive book the additives were extracted; the additive itself; and the meaning of the code groups used. This slow and time-consuming process was applied by the analysts at Corregidor to JN-25B7 from 1 August until 4 December 1941, when JN-25B8 replaced it. The only current JN-25 messages read by U.S. analysts on Corregidor during this period were few in number and were invariably ship movement reports: arrivals and departures, together with some fragmentary schedules. In view of the full collaboration and exchange with FECB, Singapore, there is no reason to believe that the British exceeded the U.S. accomplishments. [end of statement]

What is the author's evidence to support his contention that both British and American Comint authorities were reading JN-25 with ease before Pearl Harbor? Rusbridger's first statement on the subject of British efforts against JN-25 after its introduction on 1 June 1939 occurs on page 88. After an explanation of the structure of JN-25 that is too long and inaccurate to treat in detail, he said of the British effort at the GC&CS in England:

By the autumn of 1939, GCCS... had reconstructed the JN-25 codebook, and Commander Burnett flew out to FECB to give Nave the reconstructed dictionary and current keys. Thereafter, JN-25 offered no problems, and FECB/GCCS were able to reconstruct the monthly key table changes without difficulty. 'For the first three or four weeks into the new table change,' recalls Nave, 'there was a slight delay, but we soon overcame this. As with all Japanese codes, JN-25 started

off very simply and only later did the Japanese try and make it more complicated, by which time GCCS had completely mastered it.'

So by the end of 1939, GCCS and FECB could read JN-25, ...;the naval attache traffic...; and several other low-grade codes, such as the Appointments Code, which contained little of importance.(page 88)

By page 133 the author has jumped from the end of 1939 to the end of 1941, leaping from one codebook to another and over three successive additive books to further emphasize the extent and facility of British success against JN-25. He describes Yamamoto's deployment of his task force to Tankan Bay in November 1941 making a big point of discounting the "mythology... that after sailing to Tankan Bay, the Task Force maintained total radio silence."(Rusbridger considers the transmission of messages from naval headquarters in Tokyo to the silent task force as a violation of the task force's radio silence!) But there was little difficulty in following the task force even after a callsign change. "FECB found this much easier because *they were reading the JN-25 messages.*"(page 133) "It was these operational messages sent in the JN-25 naval code... that contained the vital information about the attack. Therefore, *anyone who could intercept and read these JN-25 messages* [all italics mine] would automatically know about Yamamoto's plans to send a Task Force to sea." (page 134)

Just in case any doubt remains about the ease of reading JN-25 messages and who could do so, we have on page 137:

But Nave is adamant that every message intercepted by the Americans would also have been intercepted by the British, and because JN-25 *had been broken by him* since the autumn of 1939, all these intercepted messages would have been read *without difficulty or delay* by FECB and GCCS.[all italics mine] (page 137)

Up to this point the author has repeatedly asserted that the British were able to decrypt and understand the meaning of JN-25 messages, but he has offered no evidence to substantiate this claim other than the statements of Nave, who left FECB a year and a half before the messages relating to the Pearl Harbor task force were transmitted, and ten months before the second and greatly enlarged JN-25 codebook was introduced. But the author attempts to suggest the existence of other evidence.

As mentioned above, Rusbridger describes the contents of several JN-25 messages intercepted in 1941 but only decrypted after the war by OP-20-G. (pages 137-140) He chooses to believe that these messages were <u>really</u> decrypted and translated in <u>1941</u>. Using the rationale described in the above quotation, i.e., that if the Americans could intercept the messages, then FECB could not only intercept them but break them and read them without difficulty or delay, he introduces some of these messages with phrases such as "decoded by FECB," or "FECB decrypted, " or "FECB could read,"when, in fact, there is no evidence that FECB ever intercepted, decoded, decrypted, or could read any of them.[4]

But FECB was not alone in reading these messages, we are told. "Thus anyone able to read JN-25--*as could Churchill*--[italics mine] knew by 25 November that a large Japanese task force was at sea, with the intention of commencing hostilities, and that one of the most likely targets was Pearl Harbor."(page 139)[5] This quotation illustrates the author's tendency to imply a great deal without saying

4. Slipped among the 1945-1946 OP-20-G decrypts is a message from another source, introduced with the phrase "On 25 November FECB decrypted..." A footnote on page 273 indicates that the message, now reposing in the U.S. National Archives, was originally recovered from a sunken Japanese cruiser. There is no evidence that the message was encrypted in JN-25 nor, as with the OP-20-G post-war decrypts, that FECB ever intercepted or decrypted it.

5. The author was careless in selecting messages, using, for the most part, those that concerned units that were involved in southern operations and were not part of the northern strike force which attacked Pearl Harbor.

much of anything precisely. Is the author simply stating that someone routinely passed translations and intelligence reports to Churchill, or does the author want us to imagine decryption of JN-25 as so simple a matter that almost anyone could do it? Are we to picture that Churchill, too industrious to sit around at Chequers playing checkers, was easily and without delay, deciphering indicators and applying five-digit groups of additive to JN-25 messages, reading off the deciphered code groups' meanings in Japanese out of the reconstructed codebook, translating into English, and piecing together intelligence to pass the time of day?! With such spectral stuff the author attempts to flesh out the skeleton of his conspiracy theory. It is a little scary, but completely unconvincing.

What is the truth about British capabilities against JN-25?

All sources available to the reviewer indicate that there was no successful meaningful decipherment of current operational traffic encrypted in JN-25 until early 1942, approximately one year after the commencement of full-scale collaboration between the U. S. and Great Britain, and two years after Nave's departure from FECB..[6] Whitlock, who continued to work with JN-25 in Australia after evacuation from Corregidor , states that by May 1942 "...JN-25 was only about 20% readable. (That does not mean we were reading 20% of all Japanese Navy messages - simply that we were reading an average of about 20% of the content of any message we could manage to decipher.)"[7]

6. OP-20-G and station Hypo (Honolulu) were ordered to begin decryption of current JN-25 traffic on 18 March 1942 according to an unpublished document, *The History of GYP-1, 29* CCH (Classified)

7. Whitlock, *And So Was I,* 3.

Documentation

In the first 139 pages of 180 pages of text, Rusbridger has yet to offer any documentary evidence in support of his claim that the British read JN-25 before Pearl Harbor. His whole case rests on the recollections of Nave and Mortimer and his own statements repeated again and again to the effect that JN-25 could be easily and quickly decrypted and read. It is not surprising if Nave and Mortimer might , at this late date, have some difficulty in distinguishing between what they learned from JN-25, what they learned from other more easily read systems, what they deduced from traffic analysis and direction finding, and what they learned from collateral sources. It might even be questioned whether they remember exactly what they learned and when. The only documents introduced are the messages OP-20-G decrypted and translated in 1945-46. Arguing that FECB must have been able to intercept and decrypt these messages in 1941, Rusbridger proceeds to use them as if such decryption and translation actually took place at the imagined time and place. This lack of anything even remotely resembling valid documentation continues through page 173 .

Then two of the last seven pages of text are reproductions of what the author describes as "pre-Pearl Harbor JN-25 decrypts." Neither of the two documents presented are JN-25 decrypts. Both are intelligence reports and there is no indication that either is based upon JN-25 decrypts. The first is an intelligence summary dated 30 December 1940 from FECB to the Australian Commonwealth Naval Board and the New Zealand Board titled "Conversion of Trawlers: Mandated Islands." The author states that "The text shows that it must have come from reading messages in JN-25, since it deals with future intentions." He does not explain why

future intentions concerning use of trawlers and fishing boats necessarily requires encryption in JN-25, nor does he offer any justification for calling the report a "JN-25 decrypt." The second message dated 24 January 1941 refers to "special intelligence" from September 1940 indicating landing of naval stores on Marcus Island and construction work under way on Saipan. This is identified as "another JN-25 decrypt" apparently on no basis other than the reference to special intelligence. (page 174) The subject matter of both reports suggests that if either was based in part on decrypts, those decrypts were probably from a lower level system than JN-25.

On the same page we are referred to Appendix 2, which contains six "copies of JN-25 decrypts from FECB in Colombo in early 1942." Again, five of the six are not simply message decrypts and translations, but intelligence reports that may include information derived from JN-25. (The third example appears to be based solely on traffic analysis, mentioning only an address.) Since all six reports postdate Pearl Harbor, they are completely irrelevant to the author's thesis except that he goes out of the way to claim:

> What is particularly important about these messages is that the additive table in use for this period came into operation on 4 December 1941. Since the messages contain no corrupt groups, it confirms that despite the upheaval of moving from Singapore to Colombo in late December, FECB had no difficulty in overcoming this table change within four or five weeks.
>
> It follows, therefore, that as the previous table change occurred on 1 June 1941, FECB would have been reading all JN-25 traffic without difficulty long before November 1941.[page 186]

First, since the documents shown date from no earlier than 12 February 1942, they do not demonstrate any capability before 7 December 1941. Since they are, for the most part, intelligence reports and not message decrypts, the absence of

corrupt groups would prove nothing. (The term "corrupt groups," which normally is applied to code groups garbled in transmission or incorrectly copied by a cryptographer or intercept operator, is understood here to mean code groups that could not be decrypted). If no messages could be decrypted so as to produce meaningful intelligence, and the report was based entirely on other sources, then there would be no evidence of "corrupt groups." If, on the other hand, there is some useful information in an incomplete or uncertain decrypt, such incompleteness or uncertainty might be indicated in the report. The second example in Appendix 2, the only one appearing to be a direct translation of a decrypt, is exactly such a report containing corrupt (i.e., unrecovered) groups and recoveries of low validity. It follows in its entirety with "corrupt" or low validity portions underlined:

Naval Special Intelligence from Colombo dated March 1st.

An unknown force possibly which is hostile from DAVAO is to arrive ? at 5 degrees 15 minutes South? 108 degrees East at 0700? 3rd March. Speed 9 knots.

Similarly, the fifth and sixth examples both contain evidence of "corrupt groups" as well as indications that they are not simply decrypts but Comint reports based on plain language and traffic analysis as well as possibly decrypts. The fifth example is headed "Plain language and special intelligence,"and refers to an "unknown reconnaissance unit." The sixth example refers to leaving "an unknown place" and refers to possible identification of call signs.

So the evidence presented is not exactly what it purports to be (i.e. JN-25 decrypts), is not necessarily based on JN-25 at all, is not free of "corrupt groups" as the author claims, in no way demonstrates that FECB had no difficulty in recovering from the additive table change of 4 December 1941, and has no bearing upon anyone's capability to decrypt JN-25 *before Pearl Harbor*. The author also errs in stating that "the previous table change occurred on 1 June 1941." There was no

change of JN-25 on 1 June 1941. The last previous change was on 1 August 1941 and the one before that on 1 February 1941.

In summary, Rusbridger's argument that British analysts could read JN-25 easily and without delay during the period when they might have received warning of the Pearl Harbor attack is based solely on Nave's and Mortimer's recollections, spurious "evidence," and imaginative speculation. It contradicts the accounts given in other detailed and convincing sources.

Rusbridger's Account of the American Effort Against JN-25

The first mention of American capabilities in respect to JN-25 is a casual reference on page 82 to "the JN-25 naval code that OP-20-G were also decrypting." We next learn that by October 1940, OP-20-G "had made sufficient progress to turn over the work of reconstruction" on the code, first introduced on 1 June 1939, to less experienced analysts.(page 83) It is only at page 166, however, that the author begins a systematic investigation of American progress. This appears to be the first instance of conclusions based on documentation! Unfortunately, Rusbridger is inclined to cite sources and then draw conclusions not supported in those sources. He deduces that "JN-25 was broken by OP-20-G soon after its introduction, matching the progress made by Nave and Burnett."(page 168) Actually, the initial roles of Nave and Burnett were only those of receiving the recoveries carried to Singapore and that of courier, respectively. The author is correct, however, in suggesting that OP-20-G accomplished a basic diagnosis of the structure and functioning of the enciphered code system much on the order of GC&CS's, and well before the attack on Pearl Harbor. On the same page, however, he cites a statement that on 1 [sic] December 1941, JN-25, which had been in use for two and a half years, became unreadable but that the change was only in the additive table. From

this he deduced that JN-25 "was read throughout the two-and-a-half-year period to late 1941" and "the basic code remained unchanged and only the additive tables (or keys) altered." Admittedly the source cited by Rusbridger is not clear on the two points made, but as is shown below, the term "readable" is ambiguous. It is also not fair to deduce from the statement that at a point JN-25 became unreadable, that it had been readable for the previous two and a half years of its existence. Also it is a fact that the basic code changed completely on 1 December 1940, almost doubling the number of code groups available for use, and did not remain unchanged for two and a half years as implied.

One of the basic problems Rusbridger faced in developing his conspiracy theory was lack of access to those official records concerning JN-25 that remain classified and probably will remain so indefinitely because of their scope and technical depth. Another problem was the lack of precision in the use of certain terms concerning cryptology, a problem one encounters even in reading technical reports on cryptanalysis. The importance of these distinctions in terminology justifies departing from the specific at this point to make some general observations that apply not only to what follows in this review, but to what has preceded as well.

Problems of Terminology

Such terms as "break," "read," "solve," "reconstruct," and "recover" and derivatives thereof have different connotations depending on context and the frame of mind of the user. When a cryptanalyst says he has "broken" or "solved" a code, he usually means that he has diagnosed the structure of the cryptosystem and how it works. Thus, when analysts first "broke" JN-25 they probably had established that the Japanese naval general purpose code was a five-digit code enciphered by the application of random five-digit additive groups extracted from a book of additives in accordance with an indicator enciphered by a single daily

changing additive. They apparently recovered the indicator system, some additive, and perhaps some code groups, but could not necessarily read anything more than fragments of some stereotyped or "pattern" messages., such as routine ship movement reports and medical reports.

A report from OP-20-G notes that although JN-25 had been "completely solved" and "completely broken" in the fall of 1940, during the winter of 1940-41 progress was slow towards actually reading even a few of the messages sent a year earlier. By that time the original JN-25 codebook designated JN-25A was replaced (1 December 1940) by the greatly expanded JN-25B and the Japanese had progressed through two additive books and had started on a third (JN-25B5) beyond those used for the 1939 encryptions (JN-25A1 and JN-25A2). Analysts at OP-20-G intentionally restricted their work on additive and code recovery to the 1939 traffic, now more than a year old, hoping to maximize their knowledge of the types of underlying plain text. [8](This bet paid off by providing a backlog of plaintext cribs which could be used effectively by the time of the Battle of Midway. Once a gigantic increase of resources was applied to work on current traffic in the spring of 1942, JN-25 quickly began to yield valuable intelligence.) So the statement that a system is broken, solved, reconstructed, or readable does not mean that all messages, all of any one message, or any current messages in the system are necessarily readable. Unless it is said that all messages are completely readable within a given period from their time of intercept, it is best to assume that "readable" means that the general drift of some messages can be determined.

Likewise, "recovered," lacking the adverb "completely," usually means partially recovered, and "reconstructed" usually means that we have a blueprint of the superstructure or "shell" of the cryptosystem. A codebook is reconstructed when we know its size and shape, the size and nature of its code groups, and perhaps

8 *The History of GYP-1*, 14 (Classified).

something about the location in the book of code groups within a certain category of meanings (e.g., numbers, unit designators). With the book reconstructed, the "bookbuilder" (the British form of the less descriptive American "bookbreaker") can go about gradually recovering the meanings (or values) of specific code groups and entering them into the book. It often takes considerable time after a codebook is "reconstructed" before it can be used to read any significant messages.

The American Effort (continued)

Scraping the bottom of the shallow barrel of unclassified U.S. sources, Rusbridger cites an excerpt, "The first completely decrypted message/translation in JN-25 followed the first decrypted Purple message by about a week."(page 169) He observes that the first Purple message was decrypted in September 1940 and concludes that "from early October 1940... JN-25 was being broken by OP-20-G." The conclusion is correct, but the single message that was read was at least ten months old, was from a "broken" codebook that by October 1940 was being enciphered by the third successive replacement additive book and would in another two months be replaced by a new and greatly expanded codebook. The JN-25A1 or JN-25A2 message read in October 1940 was enciphered, essentially, in a different cryptosystem than the JN-25B7 messages that might have given warning of an attack on Pearl Harbor. The reading of a single message from an outdated encipherment system hardly justifies Rusbridger's statement on page 177 that "...American codebreakers were able to read the Japanese operational orders sent in JN-25 throughout the months leading up to Pearl Harbor."

While in one place having maintained that the American decrypts and translations of 1945-1946 were actually the work of pre-Pearl Harbor times, Rusbridger in another context used the argument that with all the investigations

going on 1941-1945 surely OP-20-G would not have let all those 1941 messages just sit there undecrypted. This argument illustrates the author's complete lack of understanding not only of the limited American pre-Pearl Harbor capabilities against JN-25 but also of the intensive effort expended to wrest intelligence from a huge volume of JN-25 traffic during the years 1942-1945. After Pearl Harbor there was a war going on, and the immense resources that were made available to deal with JN-25 were all focused on maximizing the production of current intelligence.

Other Problems With *Betrayal at Pearl Harbor*

Although this review does not attempt to deal with many of the non-cryptologic aspects of the book, there must be mention in passing of the extremely jaundiced view of Winston Churchill taken by Mr. Rusbridger. Without quoting or summarizing at length, one can merely glance at the entry "Churchill" in the index, find the sub-category "duplicity and dirty tricks," and read the listing: 111, 122-123, 135, 151-154, 177-178, 180.

Rusbridger charges that U.S. Army-Navy rivalry and lack of cooperation in Comint "was to prove one of the primary causes of the Pearl Harbor disaster"(page 60) and "helped lead to the ultimate disaster at Pearl Harbor."(page 63) While the rivalry and mutual distrust certainly existed, Rusbridger's charge of cause and effect is overdrawn and unsubstantiated.

The book is filled with errors of fact of which the following is only a small representative portion. "Newly arrived codebreaker Larry Clark" is credited with suggesting to others in the Army's Signal Intelligence Service in 1940 that telephone selector switches were the key component of the Purple machine.(page 80) It was not Clark but Leo Rosen. [9]At the time Rosen was relatively new on the job while Clark had been there ten years. Henry Stimson is identified as being Secretary of

State, rather than War, in 1940. (page 81) On page 83 it is stated that in October 1940 Currier was transferred to the German naval Enigma problem while the source cited says Currier "will continue to handle Orange [Japanese] Naval Attache and other Orange Navy systems." which, in fact, he did for the duration of the war.

The description of and examples of JN-25 given on pages 86 and 87 contain several errors the most important of which is the indication that the JN-25 codebook remained unchanged during the war when in fact replacements were provided with increasing frequency as the war progressed. The designators for successive codebooks, e.g., JN-25A (used 1 June 1939-30 November 1940) and JN-25B (used 1 December 1940-27 May 1942) are mistakenly identified as successive additive books which, of course, changed much more frequently and were designated by a one-up numbering following the designator of the codebook in use. (e.g., JN-25A5 and JN-25B6.)

On page 92 the author describes what appears to be the system for processing German Enigma traffic at GC&CS, Bletchley Park, and seems to suggest that JN-25 was included in the process although, in fact, after the initial diagnosis of JN-25 it was assigned to FECB for all further development and exploitation in September 1939. The statement "So the raw JN-25 material was seen by very few people working in Huts 8 and 4" is undoubtedly accurate. They were all working on German machine ciphers and had nothing to do with JN-25, which was FECB's responsibility. The impression of a vast effort on JN-25 at GC&CS (page 169 refers to GC&CS having "300 people working solely on JN-25") crops up at various places in the book although the author cites no basis for claiming more than minimal monitoring of FECB's work.

9. William F. friedman, National Security Agency documents in Record Group 457, National Archives, SRH-159, *Preliminary Historical Report on the solution of the "B" Machine*, 9.

Rusbridger asserts (page 109) that if, in the fall of 1940, the British had given the U.S. "an Enigma cryptograph," it "would allow the U.S. Navy to break the signals from German U-boats operating off America's eastern seaboard." Although the British were reading *Luftwaffe* Enigma in the fall of 1940, they possessed no "Enigma cryptograph" capable of decrypting naval Enigma.[10] The author's whole treatment of early Anglo-American cryptanalytic collaboration emphasizes American distrust of the British and British reluctance to be altogether forthright. Although there was some suspicion and dissatisfaction among American command figures, those Americans directly involved with cryptanalytic exchange (e.g., Currier and Sinkov)[11] did not share these feelings.

On pages 112-113 there are several references to FECB producing Purple decrypts with a "Purple machine" provided by the U.S. through GC&CS. The author gives no source for this assertion, but If he had more carefully read one of his sources cited elsewhere he would have known that FECB never had a Purple analog and never deciphered any Purple messages.[12] The examples reproduced in Appendix 3 give no indication that the reviewer can detect of an origin at FECB.

10. David Kahn, *Seizing the Enigma* (Boston:Houghton Mifflin, 1991), 126.

11. Currier and Abraham Sinkov were the senior American naval and army representatives, respectively, who initiated Comint collaboration with the British, carrying two Purple machine analogs and an "almost empty" (Currier's description) JN-25B codebook, among other things, to GC&CS, Bletchley Park, in January 1941.

12. Dundas P. Tucker, "Rhapsody in Purple, A New History of Pearl Harbor - I," *Cryptologia*, (July 1982) VI, 3:204-205. This article is based on notes written by Captain Laurance F. Safford, U.S. naval cryptologic pioneer, typed up by Commander Charles C. Hiles who also wrote an introduction and added some notes, annotated by Harry E. Barnes, and finally written up by Tucker with further notes. Rusbridger makes use of this source in *Betrayal at Pearl Harbor* (page 260, fn 17; page 262, fn 15; and page 267, fn 4), but apparently overlooked the statement on pages 204-205 of the source that there was no " Purple Machine" at Singapore, the machine cipher messages decrypted at FECB being from the Red Machine.

DOCID: 3928669

Major Problems of Methodology

The author's basic problem of trying to build a case on a lack of evidence, is compounded by difficulties with proper use of sources when he finds sources to use. We have noted in passing so many cases of misreading or misusing sources that one has to conclude it is a basic fault of methodology. On page 170 we find reference to a source that says "A new system of keys was introduced on 4 December 1941...but the carry over of the old code made their solution quite simple...". The conclusion follows that this "confirms that after the additive table change on 4 December 1941 messages were still being sent in both the old and new keys." The cited source neither confirms nor hints at anything of the sort! It simply says that the additive book (key) changed, but the code did not.

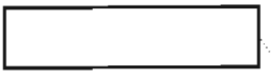
On page 93 the author cites a message from the British Secretary of State for Dominion Affairs to the Australian Prime Minister dated 2 September 1941: "information from most secret sources should not be passed to the United States observers [at Singapore] but... to FECB." From this he concludes that "As a result the Americans in Singapore were certainly unaware until after Pearl Harbor that the British had broken JN-25." The purpose of the instruction was obviously to tell the Australian Prime Minister to pass on Comint information only through established British Comint channels. It was not intended, as implied, to shut off Americans from information that, in fact, was being freely exchanged between American Comint practitioners on Corregidor and their British counterparts at FECB.

Conclusion

As a historian the reviewer understands the author's frustration in trying unsuccessfully to get at old but still classified sources, some of which certainly could be made public. This review is no apologia for the overall record on declassification

of U.S. World War II cryptologic history. On the other hand, as a cryptanalyst emeritus, the reviewer appreciates both the profound difficulties faced in declassifying cryptologic materials and why some information can not be declassified even after fifty years. The reviewer also appreciates the difficulty of locating, perusing, understanding, and then interpreting cryptanalytic records for the general reader. It is a job that requires specialized knowledge, stubborn determination, and a cautious, questioning, and skeptical frame of mind. These difficulties, however, do not justify misrepresenting sources and jumping to unjustified conclusions to make an argument which is based on the faith of a true believer rather than historical evidence. The fact is that we have no evidence that any JN-25 messages decrypted before the Pearl Harbor attack gave warning of that attack. The whole thesis of the book under review collapses lacking the support of such evidence.

Despite the frustrations and difficulties of the job, researchers at the Center for Cryptologic History along with other responsible historians will continue their efforts to describe the role of cryptology in history. It is necessarily slow and painstaking work that places a premium on accuracy and logical thought. Such sensational and carelessly constructed publications as *Betrayal at Pearl Harbor* only make the job more difficult.



STATUTORILY EXEMPT