LETTER TO THE EDITOR

Ralph Erskine

ADDRESS: c/o *Cryptologia*, Department of Mathematical Sciences, United States Military Academy, West Point NY 10996 NY USA.

Dear Editor

I should like to comment on a few details in David Kahn's interesting article, "An Enigma Chronology", which appeared in (*Cryptologia* 1993. 17(3): 237-246).

An entry for May 1940 (page 240) states that the first bombe (used for solving Enigma) was installed in GC&CS then, and that May is more likely than the August date given in F. H. Hinsley *et al.*'s *British Intelligence in the Second World War*, 1 (1979), 184, "because regular solution of RED [a Luftwaffe Enigma cipher] began [in May]."

In fact, the first bombe was installed on 18 March 1940 (Hinsley *et al.* 3(2) (1989), 954. This was the bombe designed by Alan Turing without the diagonal board later invented by Gordon Welchman, although Hinsley does not spell that out. The Turing bombe's "first recorded success" was against naval Enigma - not RED (3(2), 954). RED was solved mainly by hand methods until at least late 1940 (Hinsley 3(2), 953, 954). This explains why surviving Hut 6 veterans do not remember a bombe operating in the spring of 1940, since it was used only by the Hut 8 cryptanalysts (naval Enigma). The first bombe with the diagonal board arrived on 8 August 1940 (Hinsley 3(2), 955).

The entry for March 12, 1941 (page 244), substantially follows Hinsley (1 (1979) 337) in stating that captures from the patrol ship *Krebs* helped GC&CS to read "some March and all April and May naval messages in the Home Waters key net" (but in the Chronology, "March" is a misprint for "February" (see David Kahn, *Seizing the Enigma*, 137 and Hinsley 1, 337)). As to "all April," Hinsley relied on a post-war history, which was compiled from memory. Volume 1 does indeed state that all the April traffic was read before 10 May (when captured material started to arrive at GC&CS), but volume 2 (1981), 163, revises that to "most of the traffic for April." Even that is inaccurate. An analysis of the decrypts on DEFE 3 in the Public Record Office (PRO), London (see Figure 1), shows that only nine days of April traffic were read before 10 May. A further

eight days of that traffic were broken before 26 May. GC&CS did not break 9 signals for 1 and 2 April until about March 1942 (PRO: ZG 151 on ADM 223/2).

On the May traffic, Hinsley merely claims that GC&CS "was able to read *much* of the May traffic with a delay of between three and seven days" (my emphasis). A study of the decrypts confirms this.

The entry for June 1, 1941, "GC&CS reads Home Waters (and U-boat) messages for a month with keys captured from weather ship *München* and U 110" (page 244), is based on Hinsley 1 (1979), 169. Again, Hinsley errs on detail. No general Enigma keys for any month whatsoever were taken from U 110, as distinct from special "Offizier" keylists, which were quite different. Recognition signals (Erkennungssignale) for April and June were captured from U 110, but these were merely flare and "blinker-lamp" signals - not Enigma keys. A detailed account of the cipher captures from U 110, and of their impact, is set out in the present writer's "Naval Enigma - a Missing Link" in *Journal of Intelligence and CounterIntelligence* 3 (1989), 493.

Ralph Erskine

		APRIL									MAY									
		22	23	24	25	26	27	28	29	30	1	2	3	4	5	6	7	8	9	TOTAL
S	27														6		3	2		11
I	26															14	3			17
G	25																			-
N	24																			-
A	23																			-
L	22																			-
S	21										17	2				1				20
	20										6					1				7
A	19											9	3			1				13
P	18									11	10	1	1						1	24
R	17	40																		40
I	16	12	14																	26
L	*TP	2														2				4
	TOTAL	54	14	-	-	-	-	-	-	11	33	12	1	3	6	19	6	2	1	162
	DATE	22	23	24	25	26	27	28	29	30	1	2	3	4	5	6	7	8	9	
				APRIL											MAY					

DECRYPTS

*"TP" refers to one non-Enigma teleprint and one undecipherable Offizier signal.

ZTP 210-271

Figure 1. Naval Enigma Signals Decrypted at GC&CS Before 10 May 1941.

LETTER*

Louis Kruh

ADDRESS: 17 Alfred Road West, Merrick NY 11566 USA.

Dear Editor

On May 16, 1994, Dr. Daniel R. Killoran wrote a letter to *Cryptologia* expressing his disagreement with Robin Denniston's article, "Yardley's Diplomatic Secrets" (*Cryptologia*, [1994] 81-127), particularly where "Denniston suggests that Yardley's sale of secrets to the Japanese is proved."

I wrote to Killoran saying I had also taken strong exception to Denniston's remarks and would reply after some further research.

Denniston attacked Yardley with phrases such as: "[a] reprehensible betrayer of secrets," "his treacherous agreement with the Japanese," "a mercenary and a traitor" and much more. His extravagant tirade includes more than a dozen slanderous comments.

But where is the evidence that justifies Denniston's diatribe?

The charge of Yardley's betrayal first appeared publicly in Ladislas Farago's 1967 book, *The Broken Seal: The Story of "Operation Magic" and the Pearl Harbor Disaster*. He cites a Japanese foreign ministry memorandum as his source for accusing Yardley with selling his cryptologic secrets for $7,000.

To put that memorandum into its proper perspective, it is necessary to review its background.

Yardley's revelations in *The American Black Chamber* that the United States had intercepted and decrypted Japan's secret communications to its negotiators during the 1921-1922 Washington Disarmament Conference caused a huge uproar in Japan. The country's leading newspapers leveled intense criticism at the foreign ministry and blamed it for its lack of security.

Anticipating questions about Yardley's disclosures that might arise at a coming session of the Diet, the foreign ministry prepared a list of potential questions and possible answers. It is in this internal Japanese foreign ministry memorandum – designed to deflect criticism – that the charge against Yardley was raised for the purpose of discrediting him.

*Any responses received to this letter will be published in our January 1995 issue.

Consequently, some historians and writers have suggested that to save face and to reduce the damaging effects of Yardley's book, the foreign ministry sought to brand him a traitor. They also point to the absence of corroborating evidence and note that all pertinent documents are dated after publication of Yardley's memoirs although the alleged sale had occurred previously. In *The Codebreakers*, David Kahn calls the charge "unquestionably false." Even Denniston acknowledges this view in a footnote, "Despite the evidence it is possible to interpret the matter differently – as a Japanese attempt to cover up their embarrassment at the ABC disclosures."

Like Killoran, others suggest that even if someone had sold United States' secrets to the Japanese, it doesn't necessarily mean the seller and Yardley were the same person. Killoran points out that in *The American Black Chamber*, Yardley mentions that his office was broken into after an incompetent attempt to seduce him.

Some support for this view comes in a June 6, 1931, letter from Yardley to Frederick Sullens, editor, *Jackson [Mississippi] Daily News*. In his letter, Yardley tells how the American Black Chamber was forced to move to another location "when our files were rifled by the secret agent of a foreign government" (National Archives, SRH-038, p. 154).

In that same letter, Yardley's penultimate paragraph could rebut Farago's original charge.

> When the American Black Chamber was closed, should I have desired to continue in my profession my only employer could have been a foreign government. One of the great powers, learning through their secret agents of the abandonment of cryptography in the United States, approached me with a view to my creating such a bureau and training their subjects in the science of cryptography. Although I have felt no hesitancy in revealing the secrets of the American Black Chamber, I did not feel that I could accept such a position for my knowledge would have been turned against my native country in the reading of her diplomatic secrets. The United States Government paid me $7,500 per annum. This foreign power offered twice this amount and expenses for myself and family.

Now, however, Denniston makes the startling claim that Yardley's treachery was corroborated in 1992. But he makes a major error by relying on a secondary source without checking the primary document it allegedly quoted, to insure its accuracy. And, as it turns out, his source is absolutely wrong.

Denniston cites an anonymous article, "Yardley Sold Papers to Japanese" in

The Surveillant, [1992] 99, a useful publication. After noting that Yardley had sold "his papers and his research to a foreign government" the unnamed writer says:

> Word of Yardley's lack of good judgment appeared first in an 11-page pamphlet released by the National Security Agency in 1988 titled *Pioneers in U. S. Cryptology* ... It first mentions that Ladislas Farago, in his 1967 book *The Broken Seal: The Story of "Operation Magic" and the Pearl Harbor Disaster* alleges that Yardley had sold cryptographic secrets to the Japanese government for $7,000. ... The key document, an internal Japanese foreign ministry memorandum, indicated that Herbert O. Yardley was paid the $7,000 in 1930 (after the closing of the Black Chamber). *And Japanese documents were later found which make reference to, or used techniques devised by, Yardley.*[Emphasis added]

But the NSA brochure, *Pioneers in U. S. Cryptology*, does not contain that sentence and there is no evidence that any such documents exist.

In conducting further research in 1994, I learned that thousands of documents related to Yardley were being declassified and would be released in the near future. Therefore, I delayed writing this letter until those documents became available.

In the meantime, I informed *Surveillant* of my concerns and it subsequently published a clarification that changed "documents" to "document." But there is no publicly available evidence of even one Japanese document that makes "reference to, or used techniques devised by, Yardley."

In February 1995, the National Archives released thousands of Yardley's MI-8 and Cipher Bureau papers. David Kahn, who has examined the papers, says they do not include any evidence or corroboration of Yardley's purported treachery.

(Although not directly related to this issue, my review of the Archives of the Japanese Ministry of Foreign Affairs found a memorandum dated June 10, 1931, which refers to a cablegram allegedly sent by the foreign minister to the Japanese ambassador in the United States in June 1930, about terms for purchasing papers about their codes. But the seller is not identified and the cablegram has not been located.)

In other words, a "smoking gun," if one exists, has not been found.

But the search for further Yardley papers will undoubtedly continue, as it should, given the controversies that marked his career. In the meantime, I thought it important to set the record straight based on the information available today.