# A Personal Contribution to the Bombe Story

BY JOAN MURRAY

~~*Top Secret Umbra*~~

*Discusses details of the development of the British bombe for deciphering German Naval ENIGMA messages in the Second World War. Includes some background details of the Polish bombe and some references to the American (OP-20-G) version.*

In their review of *The Ultra Secret* by F. W. Winterbotham, Schorreck and Wilson commented on the author's ignorance of wartime cryptographic systems and cryptologic history.[1] I find nothing surprising about this ignorance, because of the strict application of the need-to-know principle in the wartime British Government Code and Cipher School (GC & CS). This applied equally to cryptanalysts like myself working in a specialised area, although Brigadier Tiltman (quoted in the review) obviously had much wider knowledge, because of his research position. In the restricted field of the German steckered ENIGMA, however, I believe that my own recollections may be of some interest in supplementing the official histories. I restrict myself to the bombe story in order to avoid being too long-winded, and because this proved to be the mainstream of ENIGMA work.

Before embarking on these recollections, I should like to present a few facts about the British four-wheel bombes. The authors of the review, who naturally drew attention to the magnificent contribution of OP-20-G bombes—ignored by Winterbotham—unfortunately may have conveyed the impression that the British equivalent was negligible. In fact, in spite of regrettable delays in developing the British four-wheelers, they came into operational use some months before OP-20-G ones. The first was delivered in April 1943, and the first operational success was in GC & CS in June 1943, a month which was also memorable for a successful trial run on American four-wheelers.[2] The final figure of 68 British four-wheel bombes represents a power equivalent to about 90 OP-20-G ones, since each was about two-thirds the speed but double the size—with 36 ENIGMAs and 2 diagonal boards they tested two wheel orders at a time instead of one.[3] This comparison neglects maintenance difficulties attributable to wartime shortages, which explain the GC & CS decision in March 1944 to give priority to the production of three-wheel machines. To quote Alexander, "the raw materials available were now of poorer quality . . .

and it proved very difficult to get mechanics in sufficient quantities."[4] A division of effort seems to have been sensible here, just as work on solving SHARK—the Atlantic U-boat key—was left to OP-20-G from Autumn 1944, when they had developed the cribbing expertise (although I for one was very sorry to drop that task, which had long been our top priority one).

The Polish contribution to Bombe development has been ignored by some writers, whereas Spiegelthal refers to "hundreds of replicas of this Polish brain-child."[5] In fact, the Polish bombe was very primitive; while the wartime bombes were direct descendants of this, they were certainly not replicas, vital improvements in the logic having been made by the British in 1940. The name itself derives from the Poles, with whom the British and French communicated mainly in French. As Alan Turing told the story, the original bombe got this nickname because it made a ticking noise, like an anarchist's time bombe.[6] Turing himself, whose tremendous contribution to breaking the wartime German naval ENIGMA is well known,[7] was one of a small group of academics, recruited in advance for wartime service, who were introduced to the problems in the summer of 1939, and he was present when Dilwyn Knox[8] returned from visiting Warsaw, with A. G. Denniston (Head of GC & CS) and a French colleague[9] (identified by Tiltman as Gustave Bertrand, the author of the book reviewed by Spiegelthal). It was then that the Poles disclosed all their success on the steckered ENIGMA, which included the recovery of the five wheels then in use. To quote Knox's account of this visit, dated 4 August, "Polish methods . . . . tend to the employment of electricity and some of them are neat . . . . Precisely how the machine (Bombe) works I do not know." A circuit diagram was doubtless provided, such as is available among the Knox papers for a second Polish machine, the Cyclometer. The Polish bombe found wheel positions and stecker satisfying "whole bombes" (as they were called in GC & CS), i.e., the same constatation (cipher/plain letter pairing) occurring at three different machine positions, the relative positions being known. Alternatively, it could apparently use similar "throw-on" menus, using "females" provided by the indicators as then used on the Air and Army keys, i.e., cases of Z abc? abc + 3Z, for three different wheel settings abc, and the same Z. In both cases, one of the letters involved had to be self-steckered or testing time would have been prohibitive. This was not too serious a limitation with the 14 self-steckers then used, but there were only 6 self-steckers during the war.

I have not found any records of the early plans for a British bombe, but a small special-purpose machine was already available by 20 October 1939, for producing "sex statistics" in order to exploit the

females in the Air and Army indicators.[10] This indicates that GC & CS had approached British Tabulating Machines company well before this, on the subject of ENIGMA analog equipment.

The first British bombe, delivered in May 1940, was like the Polish one in only testing closures, which had to have a letter in common, and in testing one stecker assumption at a time for one letter, but it already represented some advance, since with 30 ENIGMAs (the later standard was 36) it could use more complicated closures and test three wheel orders at a time. I joined Hut 8 on 17 June 1940, and was put on to testing bombe answers on my first day, after the sketchiest of introductions to the ENIGMA. As there was only one bombe but a generous quantity of perfect crib (from a German vessel captured near Narvik in April), a "column" menu was being used, i.e., taking constatations for only one position of the fast wheel. This meant that the effect of the fast wheel and stecker together could be considered as a non-reciprocal stecker, so that the identity of the fast wheel was irrelevant, and the wheel orders to be tried were reduced from 210 to 42 with the basket of 7 wheels then used by the German Navy. Moreover, by using one of the wheels with only two pairs of parallel wires in the fast position, one run could test 24 stecker assumptions for the input letter, instead of a single one. In view of all this, I think I can be excused for misunderstanding the secondary testing required on other columns—a mistake which must have particularly fixed this in my mind!

Appropriately enough, since use of the bombes was shared between Hut 6 and Hut 8, the first one was maintained and operated by "the Army and the Navy and the Air Force"—one NCO from each, the senior being Sgt Jones, who later reached the rank of Squadron Leader and was in overall charge of the bombe operations at Bletchley Park and the outstations. The heads of both Hut 6 and Hut 8 were involved in the vital developments in the logical design of bombes, which took place near the time of my arrival. The first was Welchman's idea of the diagonal board, which made use of the reciprocal property of the stecker. I understood later from Turing that Welchman's objective in specifying this was simply to provide entry to a secondary chain of constatations—with the original form of test on the bombe, this secondary chain would need to include a closure in order to be of any value in reducing the number of bombe answers. Meanwhile, both Welchman and Turing were looking for a general method of achieving simultaneous scanning, i.e., testing all stecker assumptions for the input letter at the same time. I remember Turing jumping up with the remark that "the diagonal board will give us simultaneous scanning," and rushing across to Hut 6 to tell Welchman. Turing's contribution was the realisation that a wrong stecker assumption for the input letter

would imply all wrong steckers, if one allowed an unlimited number of re-entries into the chain. In the electrical implementation which provided simultaneous scanning, 25 relays represented the other steckers for the input letter, and the new test was whether any of these relays was *not* activated. When I mentioned the subject to Turing after the war, when he was visiting GCHQ at Eastcote as a consultant, he minimised his own contribution compared with Welchman's idea of the diagonal board, saying that Welchman or someone else was bound to have realised it before long—but I doubt whether anyone else would rate Turing's contribution to bombe theory so lightly. The new test in fact gave simultaneous scanning even without a diagonal board, but in that case one needed 4 closures in a single chain to provide a strong enough menu for the three-wheel problem.[11] The combination of diagonal board and the new test proposed by Turing made a dramatic improvement in the type of menu which could be run, as well as giving simultaneous scanning, and one can understand the statement that the first two bombes arrived in *August* 1940, which must refer to the new type of bombe.[12] The name Spider, used to distinguish this type from the primitive bombe, was soon dropped. Keen, of British Tabulating Machines, was responsible for the engineering design of all British bombes, except that Dr. Wynn Williams produced the Cobra attachment, to convert three-wheel bombes for the four-wheel problem, an expedient used for 12 of them (which provided the earliest four-wheel bombes).

The first disclosure to the Americans of GC & CS successes against the German ENIGMA was before Pearl Harbour and was hedged about with conditions. It took place early in March 1941 (or in 1940?),[13] when a US delegation of two Army and two Navy cryptanalysts visited GC & CS and communicated the solution of the Japanese Purple machine. My recollection starts with Turing preparing to explain the methods for German naval ENIGMA, and expressing his disgust that he would not be allowed to mention the bombes. He could explain Banburismus, the statistical attack which was then considered the most important aspect of Hut 8 work—it had been developed in 1940, and provided the only solutions that year—but even Banburismus solutions were completed on the bombes. Turing had to prepare a story that we completed the solutions with box-shape catalogs, after recovering the grund alphabets for the fast wheel and middle wheel indicator positions. Such catalogs, by cycle lengths of the permutation transforming the substitution produced at one position on the ENIGMA cycle into that at another position, had been used by the Poles to exploit the earliest "boxing" indicator system, when there were only 6 wheel orders, but of course they did not exist for the 336 Naval wheel orders. Fortunately the high-level decision about mention of the

bombes was rescinded in time, although full details of them were naturally not provided until much later. The visit of Lts Ely and Eachus to GC & CS, in July 1942, was to me the landmark for the beginning of full cooperation between Hut 8 and OP-20-G.

I knew of one feature in which the logical design of OP-20-G bombes differed from the British ones, which Turing passed on to me as soon as he learnt of it, so that I too might enjoy its elegance. The British bombes used small contacts, and it was necessary to switch off the sensing mechanism when the continuously moving wheels (fast and very fast) were in intermediate positions. To provide enough time for the sensing relays to react, Keen arranged that the motion was slower during that part of the cycle when the contacts were made, a process which was given the very descriptive name "drunken drive." The American solution, which must have made it easier to attain a greater speed, was to have large contacts: this would provide the longer time wanted for testing, while in the intermediate positions each moving contact bridged two stationary ones, eliminating any danger of spurious answers, by providing extra re-entries of the current.

I assume that OP-20-G bombes were more convenient to operate than British ones. In particular, the contacts in the ENIGMA wheels of British bombes were bundles of stiff wires set at an angle, and any attempt to turn a wheel in the wrong direction was liable to displace some wires. Even with experienced WRNS operators, much time during runs was spent in checking those wheels which had just been dismounted, and stroking any displaced wires back into position. During a slack period later in the war I spent about a week as a supernumerary bombe operator, for interest's sake, and I could probably still plug up a menu—but I assume that all these bombes were scrapped long ago! My experience was on an old three-wheel bombe; and the input stecker for a "stop" (i.e., a possible solution) was discovered by eye or by running your fingers over the relays to find one which wasn't jumping as the sensing was switched on and off. The four-wheel bombes, and some later three-wheel ones, had typewriter output. "My" bombe was called Ming, after the popular giant panda in the London zoo, but I am uncertain whether the practice of an individual name for each bombe was continued for all 198 or 212 of them.[14]

I have obviously presented only a very patchy picture. In the later years I was less aware of bombe developments, many of which were mainly for Hut 6 jobs. What mattered to me was simply that there was adequate bombe time for the Naval work, whether British or American.

REFERENCES

[1] H. F. Schorreck and V. J. Wilson, Jr., "A Review: *The Ultra Secret*," *Cryptologic Spectrum*, Fall 1974.

[2] *Naval Sigint*, Vol. I (*GC & CS History*), p. 163 and Vol. VIII, p. 171.

[3] In *Naval Sigint*, Vol. I, p. 167, the comparison of four-wheel bombes ignored the speed difference, concluding that "the English . . . . did end numerically ahead of the Americans."

[4] *Naval Sigint*, Vol. I, p. 161 and Vol. VIII, p. 278.

[5] E. S. Spiegelthal, "The Cryptologists Who (Briefly) Went Back into the Cold," (Book Reviews), *NSA Technical Journal*, Vol. XIX, No. 3 (Summer 1974).

[6] I believe this, rather than what Milner-Barry quotes as "possibly apocryphal," that "the signal of a potential solution would be the dropping of a heavy weight (the bomb) to the floor." *The History of Hut 6*, Vol. I, p. 51.

[7] See, for example, I. J. Good, "Turing's Contributions to Cryptology," *NSA Technical Journal*, Vol. VIII, No. 3 (Summer 1963).

[8] "Dilly" Knox, who was then the senior cryptanalyst on ENIGMA problems, had been recruited in World War I. His early involvement with the *steckered* ENIGMA was unknown to me during the war, except that when I pioneered the use of a self-stecker decode for the Offizier problem (of known settings but unknown stecker), I was afterwards told that I had used "pure Dillyismus." This was after Yoxall had proved the possibility of Offizier solution by the E-rack, a more valuable rediscovery.

[9] Knox reported that his French colleague took little interest after learning that the wiring of the end-plate was in the order ABC . . . instead of QWERTZU . . . , evidently the explanation of earlier difficulties. There had certainly been previous contact between the French and Polish cryptanalysts, and French and British, and liaison continued afterwards as long as it was possible. The Knox papers available to me may not have been known to the authors of the ENIGMA cryptanalytic histories.

[10] Draft note from Knox to a French contact, Captain Brac. This part was in fact omitted from the note as sent.

[11] This was occasionally done, to allow testing of four wheel orders per bombe, with only three diagonal boards.

[12] *The German Steckered Enigma I* (*GC & CS Naval Cryptanalytic Studies*, Vol. II), p. 121.

[13] The 1941 date comes from archive material held in GCHQ, but *Naval Sigint*, Vol. I, p. 163 gives 1940, with reference to *OP-20-G History*, GYA425, p. 9.

[14] 198 in *Naval Sigint*, Vol. I, p. 163; 212 in *The German Steckered Enigma-I*, p. 119.