GOVERNMENT COMMUNICATIONS HEADQUARTERS
U. S. Liaison Office

GC/133/51

25 May 1951

~~TOP SECRET~~

MEMORANDUM FOR DIRECTOR, AFSA

Subject: French Modification of the M-209 Converter

Ref: (a) AFSA 041811Z May 1951 (409)

EO 3.3(h)(2)
PL 86-36/50 USC 3605

1. As instructed in the reference and in company with [redacted] I examined the modified M-209 converter in Paris on 21 and 22 May. We agree in the conclusion that the modification is well engineered and that its use is operationally feasible.

2. [redacted] and I met in Paris and on the afternoon of 21 May called upon Colonel Veyron LaCroix, Etat-Major Combine des Forces Armees, 51 Boulevard de la Tour-Maubourg. The colonel welcomed us and provided means of conducting us to the office of Commandant Arnaud, at Ministere de la Guerre, 231 Boulevard Saint-Germain. Here we examined the machine and discussed it with Commandant Arnaud, who conceived the modification. At his request, we returned to his office on the morning of 22 May for a further discussion with Colonel LaCroix and him. As [redacted] has fluent French, the conversations were conducted in that language and I put my questions through him. His report, therefore, is the "first-hand" account of what was said and embodies all the information elicited by both of us; copies of it will be available for forwarding to AFSA possibly today. This letter is being mailed at the earliest possible moment in order to provide detailed information of the mechanical features of the modification. Commandant Arnaud classified as SECRET my rough sketches of the device.

3. The modification consists of replacing the original fixed-slide normal alphabet print and index wheels with demountable print and index wheels of approximately the same physical dimensions as the originals, and that have radial slots in which metal type can be set so as to provide any desired sequence on the wheels. For convenient reference, Figure 1 describes the original M-209 print wheel assembly.

a. First stage of the modification is to remove the original print and index wheels by cutting off the assembly, flush with the left face of the space function cam (as indicated by vertical line in Figure 1).

b. A slot about 1/8" wide is cut through the edge of the space function cam diametrically opposite the space pin and paralleling the horizontal axis of the assembly. This is shown in red in Figure 2.

c. Figure 2 shows general details of the new print and index wheels. The unit slips on to the shaft against the space function cam and is held in the correct relation to the space pin by the spline or projection (11) which engages the slot in the cam. A wing screw in the end of the shaft prevents the assembly from slipping to the left.

d. The index wheel (4) and the print wheel (6) each have 26 radial slots. A side view of a type for the print wheel is shown at (9); it will be clear that the left end hooks under the coil spring (7) lying in a groove in the circumference of the print wheel while the right end is secured by screwing down the retaining ring (8).

e. A letter for the index wheel is shown at (10). The "number disc" (2) is detached from the index wheel (4) by lifting aleaf spring (not shown) and rotating it about 15° with reference to the index wheel (4) so as to release the lock provided by the heads of three pins (3), which are so spaced that the disc can be put on in only the correct position. The index wheel letters (10) then are slid into the slots from left to right, engaging the coil spring (5). Replacing the number-disc locks the letters in place by preventing their movement to the left.

f. The number-disc has single digits in normal order (2.4 decades) around its circumference; these may be used to encipher digits as letters. A red mark is provided on the rim opposite the letter Z, which is fixed permanently on the index wheel (and print wheel) and is always used for space. The pins holding the number-disc on the index wheel are so arranged that the disc cannot be installed in any but the correct position.

4. No tools are needed to change the alphabets. When the wing screw, which is inside the operating knob (1), is removed, the print wheel unit can then be slid to the left completely free of the machine. The number disc is taken

off, after which the index wheel letters (except Z) are removed by sliding them to the left. The letters are then put on in the new sequence relative to the "Z" left on the wheel. The number disc is replaced as described above. Unscrewing the retaining ring (8) frees the type on the print wheel (6) (except Z) after which the new sequence is put on the print wheel, advancing in the opposite direction to the index wheel sequence. By wiping the print wheel with a piece of paper most of the ink can be removed, so that making the change of type is hardly a dirtier job than changing a typewriter ribbon. I tried it myself and was able to take off the old and set up the new alphabet on both wheels in thirteen minutes. Commandant Arnaud said that his tests had shown that after a message or two with a new alphabet, the operator learns it and has little difficulty using the new sequence on the index wheel. I believe this, especially since the highest frequency character (Z for space) never changes. Putting on a new alphabet presents no difficulty in conditions of good light and working space; a 26-letter check, which Arnaud expects to issue with the key lists, should prevent mistakes if faithfully executed. Changing the alphabets with hands stiff from cold, or without a clear space to lay out the bits and pieces, would be less easy, but in any case no more trouble than changing the peg and cage settings.

5. No specific installations were contemplated (for NATO), however the French expect to convert 1800 of the M-209's for army use by the end of the year. Arnaud said most holders would be issued two machines, each with three sets of print and index wheel letters to provide spares in case of loss or breakage. He expects to change alphabets as often as every other day, depending upon the traffic load, in which case security would appear to be quite high. We asked him to describe what he considered a suitable indicator usage and were told that this was a mere technical matter he had not reached the point of formulating. Cost of the modification is 8,000 francs (about $24.) per machine; the movable-type print wheel is covered by a French patent concerning which he indicated there would be no difficulty if other nations wanted to modify their own machines.

6. The modification makes no provision for variable slide, and this subject was not mentioned in the discussions.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

7. [redacted] report will develop fully our other observations during the visit. It is almost certain we were in the immediate vicinity of whatever French cryptanalytic effort there is. Colonel LaCroix did not give the impression of being a technical cryptographer or -analyst. Arnaud, on the other hand, had the look and manner of an extremely capable

and alert person who knew very well what he was doing. On the wall of his office, in two frames, hung a French military code of 1760. In his bookcase was a collection of dictionaries - including Swedish and Spanish, among others - also the ABC and Bentley codes, a copy of "The American Black Chamber", the French version of Fletcher Pratt's "Secret and Urgent", etc. - but no books on mathematics. He produced cross-section paper for sketches, including some which appeared to be a 30 x 40 transposition cage. Protruding from a folder on his desk marked "LOWDRES" was a sheet with a hand-written hatted alphabet running down the side. Neither he nor LaCroix, however, asked any prying question, except that at the start of our conference Arnaud inquired blandly, "In what fields are you gentlemen experts". [redacted] describes his reply in his report, which was to the general effect that we were there only to report what we saw, for expert evaluation. Your instructions that the discussions were to be cryptographic in nature were strictly obeyed. They did not ask where I was stationed, and appeared to believe I had come from Washington for the meeting.

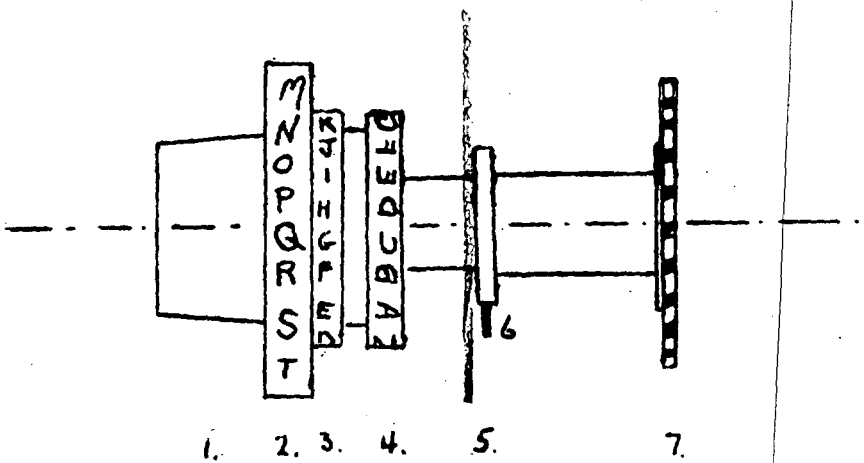
[redacted]

8. [redacted] is seriously studying the security offered by the [redacted] When it first became known that the proposed modification was based on a random-alphabet print wheel, [redacted] This first conclusion is not borne out by examination of the device and the impression gained of Commandant Arnaud's technical competence, and I believe it possible [redacted] may consider the machine acceptable for NATO use at third level, at least as an interim measure, subject to establishment of satisfactory rules for use, such as bisection, frequent change of alphabet and settings, good indicator system, etc. Use of the machine by the French should increase the security of their internal communications considerably.

9. In addition to sending [redacted] report, which as stated represents our combined experience, I will forward any other information obtainable on this subject. The visit to the French was a most interesting and worthwhile experience. I am very grateful for the opportunity.

GRIFFIN CHILES
Commander, U.S. Navy
U.S.L.O.

ORIGINAL M-209 CONVERTER "PRINT WHEEL ASSEMBLY"



(Not to Scale)

Approximately actual size.

1. Operating knob.

2. Index Wheel, set against mark on cover of machine.

3. Index showing letter which is in printing position (reciprocal of letter to which index wheel is set); read against edge of machine case.

4. Print wheel. The alphabet on this wheel must be the same sequence, but in reversed order, as the alphabet on index wheel.

5. Space function cam.

6. Space function pin. The position of this pin relative to the print wheel determines which letter is used for "Space" (Letter "Z" in M-209).

7. Driving gear through which kick of running key is applied.

(Fig. 1)

MOVABLE TYPE PRINT WHEEL ASSEMBLY (Modified M-209 Converter)

Not to scale. Approximately twice actual size.

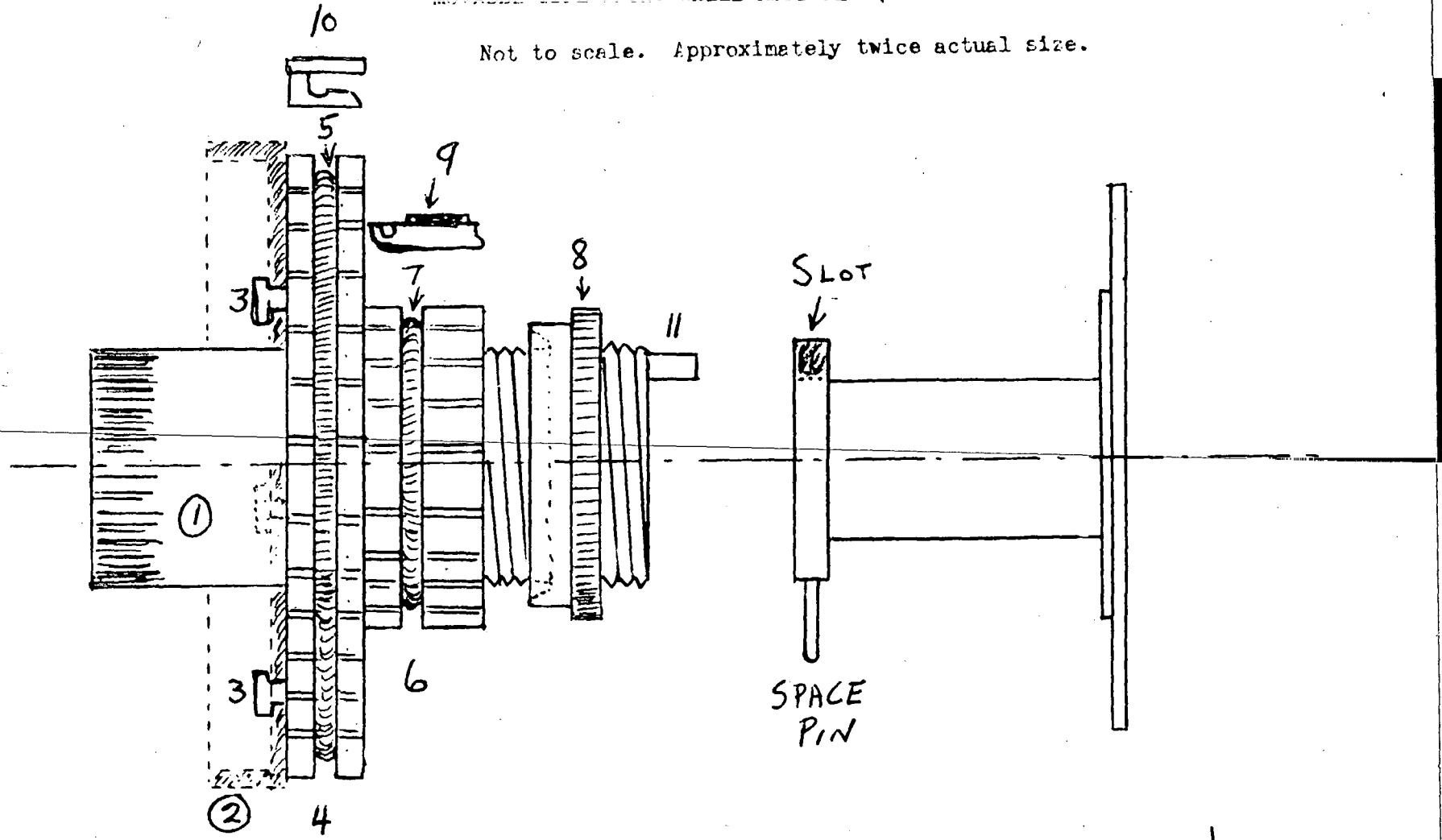


FIGURE 2.
For explanation see text.