TOPSECRET
OP-20-GE/mb

TOP SECRET

File CCM liaison
+ Sub. Comm.
on research
o/n

24 July 1944

MEMORANDUM

From: OP-20-GE
To: OP-20-G50

Subject: C.C.M., termination of researches on at Arlington Hall.

1. The technical Sub-committee of the Committee to investigate the security of the C.C.M. met for the last time at Arlington Hall on 22 July. The first meeting was on 1 May. The projects completed during this period are outlined below. Lt. Levit (OP-20-K) is continuing with a project of his own, and I shall maintain contact with him and Lt. Cmdr. Linn. The Army contingent is, however, securing. A report will be made shortly to the Committee.

2. The Sub-committee will make the following suggestions to the Committee:

(a) Rigid enforcement of the "legal limit" of 200 groups to a message.

(b) Change the indicator system to one not exhibiting monoalphabetic characteristics. Thus, under the present system, two messages in the same day with indicators LJCAQ and XTCRQ have the same initial setting of the 3- and 5-wheels.

(c) When the 3-wheel has a stepping contour on both sides, all wheels will turn ("lobster") one time in four. This may be remedied by avoiding oppositely placed contours in making up the wheels. Actually, OP-20-N has already made a set of "anti-lobster" wheels.

(d) It is unwise to simply rewire a compromised set of wheels, without changing the cam contours. In destroying wheels to prevent capture the cam contours must be obliterated as well as the wiring.

3. The projects leading to the above suggestions follow. Except in (c), it is assumed the enemy is in possession of a C.C.M. and the appropriate set of wheels.

(a) The wheel-order and setting of a 1000-group message (actually sent), with matched plain and cipher text, were found by means of lobsters. The same was accomplished with a

TOP SECRET

TOP SECRET

day's file of 250 messages all within the legal limit of 200 groups; to do this the indicators were used to line up messages to be in depth on the 3-wheel.

(b) From the one set message in (a), the daily indicator setting was found by an IBM sort. Thus, with known wheel order, a five-letter crib is easily set.

(c) Using the long message in (a), and assuming the stepping pattern, which can be found from the lobsters, the wiring was recovered.

(d) Two 200-group messages were enciphered with all but the 5-wheel in depth, and having a 7-letter plain text coincidence between them. Using the cipher text only, the wheel order and settings were found, and the messages read. The technique used was statistical, and a machine similar to Hypo could handle it. Without the 7-letter coincidence, however, the number of trials would be about 2½ billinn, and there is some doubt whether the right answer would stand out.

4. Lt. Levit's project is to find the wheel-order and setting of a single message of 300 groups, using the period of 338 on the center three wheels and the constant precession of the end wheels. (These were also used in project 3 (c) above). His method becomes unworkable at the legal limit of 200 groups, and consequently no recommendation is contemplated at the present time to avoid the center cycle of 338.

5. Needless to say, consideration of "bad" wheels, which produce a short cycle, was excluded.

6. I believe that the results of paragraph 3 show that, unless the suggestions of paragraph 2 are adopted, there is a small but non-negligible chance that the enemy (having captured a C.C.M. and wheels) might read an occasional day. The use of the C.C.M. for Ultra dispatches of the bean-spilling variety would then plainly be unwise. On the other hand, it is noteworthy that none of us thought of an operationally feasible method, whereby the enemy could read more than a scattered day here and there. The difficulties are:

(a) close to a million wheel-orders;

(b) erratic stepping of the end wheels, the one regularly stepping wheel being well buried;

(c) no discoverable test on whether a stretch of plain and cipher text is properly aligned (such as by crashing on enigma).

Because of (a), bombing is out of the question, and because of (b) it is hard to see how to strip off wheels one by one. I feel that the designers of the CCM did a very good piece of work,

Respectfully submitted

A H Clifford

Lt USNR

TOP SECRET