

REPORT OF THE COMMITTEE

APPOINTED TO ADVISE ON THE

ADOPTION OF MECHANICAL CRYPTOGRAPHY IN THE NAVY.

June 1914.

Members of the Committee.

VICE-ADMIRAL SIR DOUGLAS A. GAMBLE, K.C.V.O., *President.*

COMMANDER (Acting) J. A. SLEE, R.N.,

COMMANDER R. H. D. TOWNSEND, R.N.

MR. P. E. MARRACK.

FLEET PAYMASTER WALTER GASK, R.N., *Secretary.*

Terms of Reference.

To examine the devices which have been suggested for mechanical cryptography
And to report whether any existing machine, or any principle on which it
appears that a workable machine might be based, is recommended either for trial or
for definite adoption in substitution for :—

- (a) Flag officers' cypher.
- (b) Ships' cypher.
- (c) Vocabulary code and signal books.
- (d) Transposed alphabet.

The following points should be taken into consideration amongst others :—

- (1) Saving in personnel (especially in war).
 - (2) Rapidity in sending.
 - (3) Accuracy.
 - (4) Secrecy.
-

REPORT.

The Committee have considered the requirements which should be met by a machine for mechanical cryptography. They have examined all existing machines and proposals which have come under their notice, and finding these unsatisfactory, have endeavoured to design a machine which would meet the requirements.

The Committee have visited H.M.S. "Vernon" and consulted with the Captain and Officers of the experimental staff of that establishment. They have heard the evidence of Commodore A. F. Everett, who was mainly instrumental in bringing the proposal for mechanical cryptography to a head. They have consulted with Major Church, R.A., the military expert in these matters.

They have considered the question of the extent to which a satisfactory machine (if produced) could be employed in H.M. service.

REQUIREMENTS.

The requirements which in the opinion of the Committee should be met by any machine employed in H.M. Navy are in order of importance as follows:—

- (1) The principle of the mechanical cypherer employed should either—
 - (a) be of such complexity that it may be expected to baffle an enemy attempting to discover it. The setting of such a machine would require to be changed at outbreak of war and perhaps periodically afterwards, to guard against treachery. We have no hope of finding such a machine; or
 - (b) it should be such that an enemy could only discover it after a considerable period, even if conversant with the principle on which it is based. It should then be changed before the enemy could have time to benefit by it.
- (2) As the machine may be used by untrained men, the working must be quite simple. If possible there should be *no* adjustments or movements necessary other than those in an ordinary typewriter. The machine should encypher or decypher without adjustment, and should not require setting at the beginning of a message.
- (3) For wireless telegraphy purposes the machine should automatically space the messages into groups of not more than six letters; letters and figures should not be mixed.
- (4) The design employed should be such that unavoidable errors, *e.g.*, errors in typing or transmission, should not cause delay or the loss of a message.
- (5) The machine should be capable of working at a rate of at least 20 words per minute, as this is the slowest rate which would enable it to keep up with the wireless.
- (6) The machine should admit of repair on board.
- (7) The machine should be proof against treachery.

REMARKS ON ABOVE REQUIREMENTS.

(1) As regards secrecy the Committee have consulted with Major Church, who has convinced them that the length of time which an expert requires to discover a cryptogram is practically proportional to its complexity, and that no cryptogram can be devised which could not be discovered by an expert who had sufficient material and sufficient time.

They assume that the messages for which the machine would be employed would have only temporary importance and that no harm would result from their being read by the enemy after the lapse of a short time such as 12 hours.

Two methods are then available, viz.:—

- (a) To employ a fairly complicated cryptogram, which might be relied upon to remain inviolate for some period greater than 12 hours, and to arrange beforehand to change it at suitable intervals, *e.g.*, daily, weekly, or monthly. Major Church's report attached shows how difficult it is to find a satisfactory cryptogram, but that mentioned in paragraph (11) (c) appeared to the Committee to be promising.

(b) To employ a simpler cryptogram and change it so frequently that the enemy's expert may not obtain sufficient material to work on. Such a method is open to grave objection. The alterations in the adjustment of the machine must be carried out by the operator himself, and mistakes would cause serious delay or the loss of a message. Also the cryptogram employed must be indicated by the time of the message or else by something of the nature of a key word, so that errors in transmission might cause the loss of a message by altering the time of origin or key word.

(2) and (3) These requirements are mainly a matter of mechanical arrangement.

(4) This limits the degree of complexity of cryptogram which can be employed, but the splitting up the message into groups is a safeguard against confusion due to loss of letters. It is very desirable that the machine should reproduce both the cryptogram and the "plain language" form at the same time, so as to enable the accuracy of the copying to be checked.

(7) This condition appears impossible of fulfilment. With most cryptograms the operator would only have to strike a series of A's, then one of B's and so on through the alphabet in order to get a complete record of the cryptogram which he could carry away in his pocket. The machine the Committee prefers—that mentioned in paragraph 11 (c) of Major Church's report—could not be betrayed so simply, but a complete description of the machine could easily be taken. Periodic changes of the parts of the machine which determine the cryptogram would therefore be necessary.

EXISTING AND PROPOSED MACHINES.

A list is attached of the machines and proposals which have been examined by the Committee. (See Appendix I.)

The only ones requiring special mention are Sir P. Scott's No. 3, the Youle Faro machine, the Lefroy-Adams machine, the Committee's own design, the German "Sphinx" and a design proposed by Sir J. Alfred Ewing, Director of Naval Education.

Sir P. Scott's machine consists of two typewriters electrically coupled. The machine employs only a single transposed alphabet at a time, but the alphabet employed can readily be changed for each message or even in the middle of a message. The total number of changes is several hundred. The changes would be determined by a key word or similar method, and, as stated above, the Committee consider that the possibilities of error and confusion involved constitute a grave objection to any such method. The Committee are also doubtful whether a satisfactory machine can be made without prolonged experiment. It is probably partly owing to difficulties of construction that the specimen machine has not yet been completed. Further, it is very doubtful whether any typewriter electrically operated would be satisfactory, especially in small ships.

The Youle Faro machine as constructed was not found mechanically satisfactory. We do not consider it desirable to proceed further with this particular idea, as the cryptogram could probably be read in a few hours.

The Lefroy-Adams machine appears likely to be mechanically effective, though somewhat delicate. It is of a type which must be set to a position known to the recipient. It must also be set to "code" or "decode." In these two respects it is not considered suitable for H.M. Navy. Its construction is briefly described in Appendix I., and a full specification exists in other papers (C.P. Patents 2075/1913).

The Committee's machine appears likely to meet requirements provided that a satisfactory design can be worked out. Commander Slee has been attempting for some months to adapt this design to an ordinary typewriter with the resources at his disposal. He has spent a great deal of time and trouble over the matter, but has made little or no progress. It might be possible that more success would be achieved if a professional designer of typewriter and linotype machines were employed to design the machine *de novo*; but the Committee has hesitated to incur this expense. A brief description of the construction of this machine is included in Appendix I.

The "Sphinx" is a machine manufactured by a firm in Germany, and is for sale. The price is 100*l.*, reduced to 50*l.* if a number are taken. The Committee have been informed that this machine is to be supplied to all ships in the German Navy, and it will rely on the keywords employed to maintain the secrecy of messages.

A specimen is at present at the War Office and has been inspected by two members of the Committee.

The machine is on the typewriter principle, developed like the Youle Faro on the lines of a Blickensderfer typewriter. The cryptogram obtained is a "sliding alphabet" one; that is to say, that if in any particular setting A becomes K, B would become L, C become M, D become N, and so on. The setting for any particular letter of a message is determined by a complicated system of keywords and key-sentences. In the machine as actually constructed the change of setting in the course of the message is partly mechanical, partly manual, but it would be easy to modify the machine so that the process should be entirely mechanical. The setting only repeats after a large number of letters have been typed, so that a single message could not be decyphered unless of enormous length. But experiments have shown that if an enemy could obtain five or six messages sent in the same key, he would be able to discover by trial the shifts which were given to the sliding alphabet in the first few letters of the messages and so finally decypher the batch. The time required varies from half an hour to an hour. It is understood that Major Church is also testing this.

The machine inspected broke down several times. It is also very slow (probably not more than 12 words a minute) and requires considerable practice in its use. It is therefore not thought necessary to consider the machine further.

In view of the imperfections detailed above, the Committee think it doubtful whether the statement as to the supply to German ships is correct, unless it be for trial purposes.

Sir Alfred Ewing's proposed machine was of a similar nature to the "Sphinx," but based on the Hammond typewriter. It was open to similar objections and the Committee do not consider it suitable.

EXTENT TO WHICH A MECHANICAL CYPHERER COULD BE EMPLOYED.

The Committee have found it very difficult to deal with this portion of their task. Even assuming that a machine can be produced such as they describe, they consider that its scope could only properly be determined by actual use, and that it would be most dangerous to state didactically that the machine could replace signal or code books for any specific purpose.

They do not consider it possible to employ such a machine in place of any of the special cyphers (A, B, or C). Messages are sent in these cyphers which are of strategical or diplomatic importance, so that it would be most undesirable that they should be read by an enemy even after a considerable time had elapsed. As has already been remarked, no letter cypher can be relied upon for more than a limited period, so that a mechanical cypher would be most unsuitable for this type of message. Further, it is not probable that Flag Officers would view with favour the abolition of any of these cyphers. Their use enables a message to be kept practically secret between the sender and the recipient, whereas one sent through a mechanical cypherer would become known to several persons.

As regards its use in place of the signal books for wireless telegraphy, the following facts require consideration:—

- (1) A message sent by a mechanical cypherer must have the *same* number of letters as the "plain language," whereas a message put into code has *fewer* letters than the "plain language."
- (2) In sending by a mechanical cypherer, the total period may be less, from the time the message is evolved in the mind of the sender till it is understood by the addressee, yet the time the message occupies the ether must always be greater than in a coded message and the difference is often very appreciable.
- (3) This longer occupation of the ether reduces the probability of the message getting through without interruption and delays the next message.
- (4) In using a mechanical cypherer, the accidental omission of one group by either the sender or receiver must render the whole of the remainder of the message absolutely unintelligible.

There are certain portions of the signal books, in particular the emergency and position tables, which are specially designed to convey a quantity of vitally important matter in a very few signs. In such messages brevity is of especial importance

because it is expected that the enemy will attempt to prevent their transmission by "jamming." If the machine were employed the message would be so much longer that there would be no saving in time of coding and decoding to balance the greater length of time in the ether, while the increased probability that the message would be "jammed" by the enemy would be a fatal objection.

The Committee consider, therefore, that in any case the code form must be retained for messages of this description.

Further, the ordinary messages sent by private ships and detached squadrons are usually, and should be almost invariably, short reports which can readily be coded by the signal books in a small number of groups. The time taken to code and decode such messages at present depends on the amount of training that can be given to the coding staff in peace, but the Committee are by no means confident that the machine would have an advantage over the signal books in dealing with such messages, seeing that it would be much more difficult to check undue loquacity in sending if the rigid forms of the signal book were abolished. Captain Nicholson, of H.M.S. "Vernon," was strongly of opinion that no advantage would be gained by the use of a machine, and that progress could best be made by insisting on brevity and the elimination of unnecessary messages.

It is certain, however, that there must always be a number of long messages which cannot be conveniently coded by the signal books. For such messages Commodore Everett has shown that a mechanical cypherer is superior so far as the time of getting through a single message is concerned.

To sum up, the Committee consider that it would be undesirable that the machine should replace the signal books entirely and that much experience would be required before deciding how far it could replace them, if at all. Until such experience has been gained the two systems, if adopted, would have to run side by side.

It is understood that one of the chief advantages expected from a mechanical cypherer was a reduction in the coding staff. It does not, however, appear that any such reduction could be achieved. The Committee have already stated that they do not think that it would prove possible to dispense with code books altogether, so that, if the machine were introduced, a staff would have to be provided for two distinct purposes, i.e., for coding and for the cypher machines. It does not appear that the difficulty of providing this doubly trained staff would be less than that experienced at present.

The transposed alphabet is at present only used :—

- (1) for such words as are not included in the Vocabulary Code ;
- (2) for communication with destroyers.

As regards (1), no case can be made out for the supply of an expensive machine, as the occasions on which it would be used are rare. As regards (2), a machine would be suitable for use with destroyers, but it is not considered that a machine is required for this work, which is at present satisfactorily done by the extremely simple means provided.

As regards the cost of a mechanical cypherer the Committee are unable to speak. They consulted the manager of Messrs. Salter, typewriter manufacturers, who said that he could give no estimate in the absence of a finished design for the machine. It is stated that the "Sphinx" if supplied in large numbers will cost 50/. As a machine to meet the requirements of the Committee must be more complicated and better finished, the cost would be correspondingly greater. It would be necessary to supply at least two to each ship, to guard against the chance of one breaking down ; a large reserve stock would also be necessary. It is probable therefore that at least 500 would be required.

As their investigations have progressed the Committee have been impressed more and more with the drawbacks attaching to any form of mechanical cypherer, which drawbacks may be summarised as follows :—

- (1) The limited nature of the secrecy which can be ensured, and the confusion which would arise if frequent changes are made in the setting in order to counteract this.
- (2) The liability to mechanical breakdown and the fatal delay which might occur before such breakdown was discovered and remedied.
- (3) The increased length of messages, which may well result in the fleet wireless organisation breaking down entirely at critical periods through failure to deal with the flood of matter.

APPENDIX I.

LIST OF MACHINES EITHER IN A COMPLETED STATE OR IN DESIGN STAGE.

Scott's Machine No. 1.—Plain transposed alphabet. Tried in Fleet and reported on adversely. Reasons, slow in working and ease with which it can be decyphered. Definitely rejected by Admiralty.

Scott's Machine No. 2.—Progressive transformation, but machine is of similar workmanship to No. 1 and equally slow.

Seen by Members of the Board and Flagship of Home Fleets.

Dropped by Admiralty and also by inventor.

Scott's Machine No. 3.—Only rough drawings seen by Admiralty.

Inventor is having a machine made which was to be examined by Committee when ready. Stated to be completed by 14th January 1914, but no news has been received of it up to the date of this report.

Youle-Faro machine.—Invented by Assistant-Paymaster Youle. Mechanical progressive transformation. Tried in Home Fleet and adversely reported on by Captain of the Fleet on account of mechanical imperfections.

Damm's Machine.—Description only given with cardboard model.

Electrically worked progressive alphabet which can be used in irregular order, on a principle similar to those investigated by Major Church, and condemned by him. Seen by Mr. Marrack. Inventor offered to make a model, but it was not gathered that a practicable design has been made out.

Declined by Admiralty with thanks.

Nicholson's Machine.—A suggestion for transposing messages with six alphabets used in rotation.

"Vernon" reported adversely, both from point of view of secrecy and difficulty of mechanical construction, and no further action has been taken.

Groves' Machine.—Electrically worked transposition. Two standard typewriters used.

Description in Annual Report of Torpedo Schools, 1912. Partially working model inspected by Committee, and not considered suitable.

Lefroy-Adams Machine.—The machine is of the nature of a continually progressing transposed alphabet, the repetitions recurring after about 900 letters. It is therefore necessary to arrange some means whereby the recipient shall know at what point in the progression the message commenced so that he can set his machine to the same spot in order to commence decoding. The machine must therefore be separately "set" for each message, and it must also be set to "code" or "decode." It has no arrangement for taking a check copy of the message as handed in.

Its mechanism is extremely ingenious and somewhat complicated and may be briefly described as follows:—

- (a) The machine is a Hammond and has been arranged so as to break up the message into groups of five letters.
- (b) The type on the drum have been extended so as to completely surround it, three complete alphabets being used for this purpose.
- (c) The type drum has been mounted on a differential gear, in all respects similar to the live axle of a car on a very small scale. When one of the keys is pressed the type-drum is rotated until one of the letters is in line with the hammer, which strikes it. As the carriage moves on when the key is released, the type drum is again rotated by means of the differential through an arbitrary number of degrees. Thus if the same key was again pressed a different letter would be printed.

There are thus 26 connected sliding alphabets in use, but they are used in an arbitrary order so that the repetition of pairs of letters does not commence for about 900 letters. In other words it might be described as a progressive substitution cypher having a keyword of about 900 letters.

- (d) The necessary locking gear to hold the type drum steady whilst the type are being struck and the "code" or "decode" fittings make up an extremely ingenious but somewhat delicate mechanism.

Committee's Machine.—It appeared to be practicable to convert a Hammond typewriter to perform the following movements:—

- (1) To break up the message into groups of five.
- (2) To replace the "plain language" letters by others selected from eight alphabets.
- (3) To disturb the letters and to rearrange them in an arbitrary order, the letters in each group of five being interchanged differently in each group.
- (4) To reset itself at the beginning of each line.

By using suitable alphabets in (2) and by making the rearrangements in (3) under a definite scheme, such a machine will code or decode without adjustment, that is to say if "plain language" is copied out the machine will write cypher and if cypher is copied out the machine will write "plain language."

It was also proposed to directly couple an Empire typewriter above the Hammond and to carry a roll of paper sufficient for four hours working in the paper carrier of the Hammond. The end of the paper was to be rove through both machines and the Empire would copy out the message as handed in at the top of a length of paper whilst the Hammond wrote out the message in its other form on the lower end of the paper. After comparing the top message with that handed in, the sheet should be torn in half and the lower portion would be ready to be passed out of the coding office.

The movement (2) was to be effected by increasing the travel of the type drum from three tiers of letters to eight, and working them up and down by a mechanism similar to the "shift" key from a serrated racer carried on the moving part of the machine.

The movement (3) was to be effected by dividing the moving part of the machine into two, the lower part being moved forward as usual, but jumping every sixth position so as to divide the message into groups of five letters. The upper part was to be caused to move backwards and forwards over the lower by the upper end of a bell crank whose pivot was on the lower part of the moving part of the machine and whose lower end travelled along a standing serrated racer.

In the actual conversion of the machine the first difficulty was the arrangement for cutting the message into groups of five. This necessitated the rebuilding of the escapement. The next difficulty was to make the short arm of the bell crank climb the serrations of the racer without causing such strains on the pivots due to the great magnification of the movement as would distort the frame. This was never satisfactorily got over, and this motion is now obtained by a large disc having an irregular spiral groove on its surface. The weight of the large disc necessitates the use of an auxiliary spring, and the resulting strains are too great for the pivots of the machine generally. The printing is very erratic and the movement must be considered as a failure.

As a result of these experiments it is considered that it would be quite feasible for an expert in typewriter design to produce a machine which would meet all the requirements laid down by the Committee, but that such a machine would have to be designed entirely for the purpose and not as an adaptation of any existing machine, though the Hammond system lends itself to the matter and is particularly suitable, due to the easy, rapid, and cleanly method by which the whole of the alphabets in use can be changed in one operation, thus reducing the difficulties attending the changing of the cypher in use to the minimum.

"Sphinx" Machine.—Made by a German firm. A specimen was inspected at the War Office and notes thereon are contained in Report.

Sir Alfred Ewing's suggestion.—Sir Alfred Ewing proposed to replace the three tiers of letters in a Hammond typewriter by four or five revolvable rings each having the ordinary alphabet continued completely round it in the natural order. Each ring would be rotated to a given position relative to the spindle and locked before the message began, the position being determined by a keyword. The type would be moved up and down as the message proceeded by some mechanism similar to that proposed in the Committee's machine. The effect would be to employ four or five sliding alphabets in an irregular order as in the "Sphinx." Experiment proved that when the principle of the machine had once been found out, the discovery of the keyword of the day would take not more than two hours, and probably much less. This suggestion is therefore not recommended.

APPENDIX II.

REPORT BY MAJOR G. R. CHURCH, R.A., ON CRYPTOGRAMS SUGGESTED FOR USE IN H.M. NAVY.

(1) The system of the cypher now under discussion was examined with a view to testing its suitability for use with some form of an encyphering machine, by the use of which it is hoped to automatically encypher and decypher any message by the simple process of typing it out.

(2) The system is somewhat complicated. Eight arbitrary alphabets are used, but not in any regular sequence, until they have been changed some 60 times. By this means no true repetitions of two or more letters can occur except at intervals of 60 letters, whatever the number of letters may be, before the system repeats itself.

(3) It was proposed to alter the system periodically by introducing new alphabets and transpositions at stated intervals, which would probably be 24 hours, and by this means it was hoped that the solution of a message received one day would be of little or no assistance in the solution of messages received the next. That this was not the case we shall see later.

(4) It may be mentioned that it was never anticipated that the system would prove absolutely insoluble. The most that was hoped for was that it would prevent hostile experts from working out a solution for sufficient time to render that solution worthless when obtained, in other words, that our messages should be safe for three to four hours.

(5) The discovery of the system itself—as distinct from the translation of particular messages—would be a matter of no great difficulty to a hostile expert. Provided he had obtained sufficient material to start on the solution of individual messages, he would quickly discover that the main recurrences occurred at intervals of 55, 60, 65, or as the case may be. Later he would soon detect that only a limited number of alphabets was used. There would, therefore, be no advantage in trying to keep the system itself a secret at the expense of not giving officers practice in peace time.

(6) With a view to practically testing the system, certain messages were sent to me. These were all known to be in unabbreviated English prose and were as follows:—

Message A. 4,190 letters. Subject unknown.

Message B. Really two messages in exactly the same cypher. The first, 710 letters, was known to be a description of scenery. The second, 1,790 letters, was on some unknown subject. For all practical purposes these two may be treated as one message of 2,500 letters. Though the general arrangement of the cypher differed from that of message A, it was known that some of the same alphabets were used.

Message C. 730 letters. Known to be about angling. Some of the alphabets used in B were known to be used again here.

(7) All three messages were read, the times taken being:—

A = 20 hours.

B = 9 hours (estimated).

C = 5½ hours.

The difference in the times taken will be noted. These are partly accounted for by the extra clerical work that the longer messages involve, but in a greater measure by the fact that the knowledge that some alphabets were employed in successive messages gave great assistance to the solver.

The times given for solution are in my opinion rather misleading, since I was working practically single-handed all the time. The solution of messages in this system involves a vast amount of clerical work, at which four or five clerks could all work at the same time without requiring any expert cypher knowledge. Moreover it was not at first realised the letters "reciprocated" e.g. if E en clair is represented by X in cypher, then X en clair must be represented by E in cypher. The knowledge that this is the case is of great assistance to the solver. The times could certainly be reduced by 25 per cent. in all cases, and in the case of the longest message (A) by 40 to 50 per cent.

(8) It would be tedious to enter into details of the method of solution here, but it may be noted that the solution would be effected by continental experts by methods already well known to them. The only open question is how long they would take and we must give them credit for a skill at least equal to that of our own experts.

(9) Let us now suppose that an enemy employs a vessel installed with wireless for the sole purpose of tapping our messages and that experts capable of dealing with them are on board; that hostilities have commenced; that the key of the cypher is changed every 24 hours at noon; that message A. represents material collected during the first 24 hours, message B. (in another key) that collected during the second 24 hours, message C. that collected during the third; and also that the hostile intercepting installation is able to collect material at the rate of 50 groups (250 letters) per hour. This is what might happen:—

Commencing at noon on the first day 3,000 letters would be collected by midnight, more than sufficient to commence work on. By 5 a.m. second day 4,250 letters (message A.) would be to hand and the key for the 24 hours might be expected by 4 p.m. on the second day—too late to be of practical use.

By 10 p.m. second day 2,500 letters (message B.) would be collected in the new key introduced at noon second day. The solution of these messages might be expected by 7 a.m. third day. Messages which arrived between that hour and noon third day could be read off directly received.

By 3 p.m. third day 750 letters (message C.) would have been collected in the new key introduced at noon third day. By 8.30 p.m. the key would have been obtained and all messages arriving within the next 15½ hours could be read off as received.

It will, I think, be agreed that this system will not suit unless we can improve it.

(10) We have therefore to consider whether a cypher of this type can be made more difficult to solve by introducing new features.

It is certain that if a code could be used in conjunction with the cypher it would be possible by an intelligent arrangement of equivalents to make messages much more difficult to solve and thereby to attain our ends as far as the time limit is concerned. Such a code need not necessarily be secret, though it would of course be an advantage if it were so, but it would certainly have to run the risk of being used in peace time. Officers could then get thoroughly acquainted with it and most of them would be able to a greater or less extent to "think in code." It would, moreover, be unnecessary to put messages entirely into code, plain language might be mixed with it. Its use would shorten messages a great deal and thus "conserve the ether," and further it would enable a less complicated cypher system to be used, thus decreasing greatly the original cost of providing machines. Of course, it would take longer to encypher messages if a code were used, but experiment alone will prove whether this labour would not be compensated by the decreased time necessary for transmission.

(The Committee do not consider this proposal practicable.)

(11) Should this suggestion not be considered feasible, it will be obligatory to further complicate the system in some way. Several courses may be considered:—

(a) To arrange for a complete change of alphabets daily. The use of caps on the keys of a typewriter might help to this end. The process, however, would involve delay not only for the daily setting up, but also since those using the cypher would have to work with an unfamiliar keyboard.

(b) To change the key at more frequent intervals. This is undesirable as experience proves that such procedure leads to confusion and mistakes among those using the cypher. Moreover, it is doubtful whether it would be efficacious.

- (c) To arrange by some mechanical means to transpose the letters of a message so that the normal order of the letters is destroyed. This would give greater but not necessarily complete security. Much, however, depends on the amount of complication which can be introduced, and this depends entirely on what is mechanically possible.

(12) Finally, I should like to place on record my opinion that no mechanical contrivance which relies on a repetition of the key is absolutely safe, no matter how complicated it may be. Though 99 messages out of a hundred might be safe, an unlucky message might give the system away. At present the use of a code as suggested in paragraph 10 above seems essential to security.

2.5.14.

(Signed) G. R. CHURCH.

APPENDIX III.

SUMMARY OF EVIDENCE GIVEN BY COMMODORE A. F. EVERETT, C.B.

This officer stated that in urging the adoption of a typewriter capable of automatically cyphering messages written en clair the question of saving of personnel had not been considered. Indeed, he admitted that the use of such a machine presupposed that the coding staff were capable of using an ordinary typewriter with precision although comparatively slowly.

The only reason he was in favour of the introduction of a practicable cryptographic typewriter was the time capable of being saved from the moment the message had been written en clair by the originating ship until it was handed (en clair) to the addressee.

The result of some exhaustive trials he had conducted in the Home Fleet in 1911 had shown, under the most favourable conditions (i.e., expert coders and a clear line), that, supposing a message of 100 words was handed in to be transmitted by Vocabulary Code, it would take about—

35	minutes to code,
10	„ „ send,
25	„ „ decode.

Total - - 70 minutes in all.

Assuming a typist who, although comparatively slow, was precise, it would, supposing the provision of a cryptographing machine, take about—

5	minutes to type,
15	„ „ send,
8	„ „ re-type.*

Total - - 28 minutes in all.

or a saving of 60 per cent. in time.

It was to be observed from the above that the time to send the message (i.e., the time the aether is blocked by a message) is 10 minutes in the case of using Vocabulary Code and 15 minutes in case of the desired typewriter. In both cases it is assumed that the message (not being sent en clair) will be repeated (i.e., made twice). It is therefore admitted that should such a cryptographic typewriter be a practicable machine to produce, the aether for messages now made by Vocabulary Code would be blocked 50 per cent. more than it is at present. On the other hand the message would be delivered from start to finish in 60 per cent. less time.

The net result is dependent on the answers to these questions:—

- Is it possible to construct a typewriter which will automatically shift the transposition of the letters so frequently in a single message as to render its secrecy reasonably inviolate?
- Can the coding staff be sufficiently trained to use a typewriter with sufficient precision (not necessarily at a fast speed)?
- Is it a matter of fact that the delay in getting messages through is more due to the line being occupied than to the time taken to code and decode by Vocabulary Signal Book?

My W.T. Lieutenant states that his answer to Question (c) would be, if the experience of the late manoeuvres can be taken as approximately the state of war, that the aether is very rarely unoccupied.

* A longer time has been allowed for the re-tying as it would be more difficult to manipulate the keys for groups which are neither phonetic nor spell sense.