COPY 1

~~U. S. EYES ONLY~~

AFSA-OOT/ef

26 April 1951

MEMORANDUM FOR DIRAFSA

SUBJECT: U.S.-U.K. Conference on French insecurity

References: (a) U.K. Paper DGC/1640
(b) U.K. Paper DGC/1643
(c) AFSA Draft Staff Study on the improvement of French communications

Enclosure: Comparison of U.K. and U.S. proposals

1. a. The subject conference was initially proposed and intended by the U.K. to deal with insecurity of French diplomatic communications. Upon informing the U.K. of our desire to expand the agenda to include insecurity of French Armed Services communications, since in our view there was room for improvement in both categories, the U.K. accepted the expansion of the agenda, and prepared two papers:

(1) Reference (a): DGC/1640, "The insecurity of French non-diplomatic cyphers"

(2) Reference (b): DGC/1643, "The insecurity of French diplomatic cyphers"

b. The two U.K. papers are of about the same length, and each of them is, in fact, considerably longer and more detailed than our own single paper. Moreover, reference (a) deals with the cryptosystems not only of the French Armed Services, but also those of other Departments, such as Colonial and Interior. Under the Armed Services it deals separately with "Service Cyphers" and "Service Attache Cyphers". The British, having accepted our proposed expansion of the agenda, have decided to cover practically the whole field in some detail.

c. A first reading of the U.K. papers leaves one with a vague feeling that something is missing; upon consideration it dawns on one that they seem to have been written almost in a vacuum with respect to what has been or is being done along these lines by the same or other authorities: not one mention is made of the use of TYPEX and CCM for Western Union or NATO communications. In fact, there is but one reference to NATO and that is in the statement in reference (b), Par. 5: "It is known officially through N.A.T.O. channels that some French authorities are using the T.52...", a point which leads only to

~~U. S. EYES ONLY~~

a rather vague inference that NATO authorities have said something about French communications; it certainly gives no idea that specific action has been taken by NATO authorities to improve the security of one very important segment of French communications.

2. a. For the sake of brevity, I have, in the Enclosure, considered both U.K. papers more or less simultaneously, although, where necessary, reference to specific paragraph(s) in each paper is made.

b. In general I believe our paper and the plans proposed by us for improving the security of French communications of the two main categories much more succinct, clear, and practical than the U.K. papers and plans. Our paper would certainly be much more acceptable, from the point of view of draftsmanship at least, than the U.K. papers, if something has to go forward to the USCIB or to the U.S. Joint Chiefs of Staff. I do not mean to criticize the U.K. papers as to format; they just do things in a different manner. Their papers were perhaps purposely prepared for the consideration of technicians, rather than high-level executive or command authorities.

c. The Enclosure sets forth details of comparison, similarities, and differences between our single paper and the two U.K. papers.

William F. Friedman

WILLIAM F. FRIEDMAN
AFSA-OOT

Copies to:
AFSA-OOA
AFSA-OOB
AFSA-OOC
AFSA-12
AFSA-123
AFSA-14
AFSA-02
AFSA-03
AFSA-04

~~U. S. EYES ONLY~~

COMPARISON OF THE U.K. PROPOSALS, AS OUTLINED IN REFERENCE (a) (DGC/1640) AND REFERENCE (b) (DGC/1643), AND THE U.S. PROPOSALS, AS OUTLINED IN REFERENCE (c) (STAFF STUDY ON THE IMPROVEMENT OF FRENCH COMMUNICATIONS).

1. Physical and Personnel Security:

a. Conclusion 3g of Reference (c) states that "as a preliminary to entering upon any negotiations with the French there should be reasonable assurance that the effects of improving their communication insecurity will not be nullified or diminished by physical and personnel insecurity in the French Government."

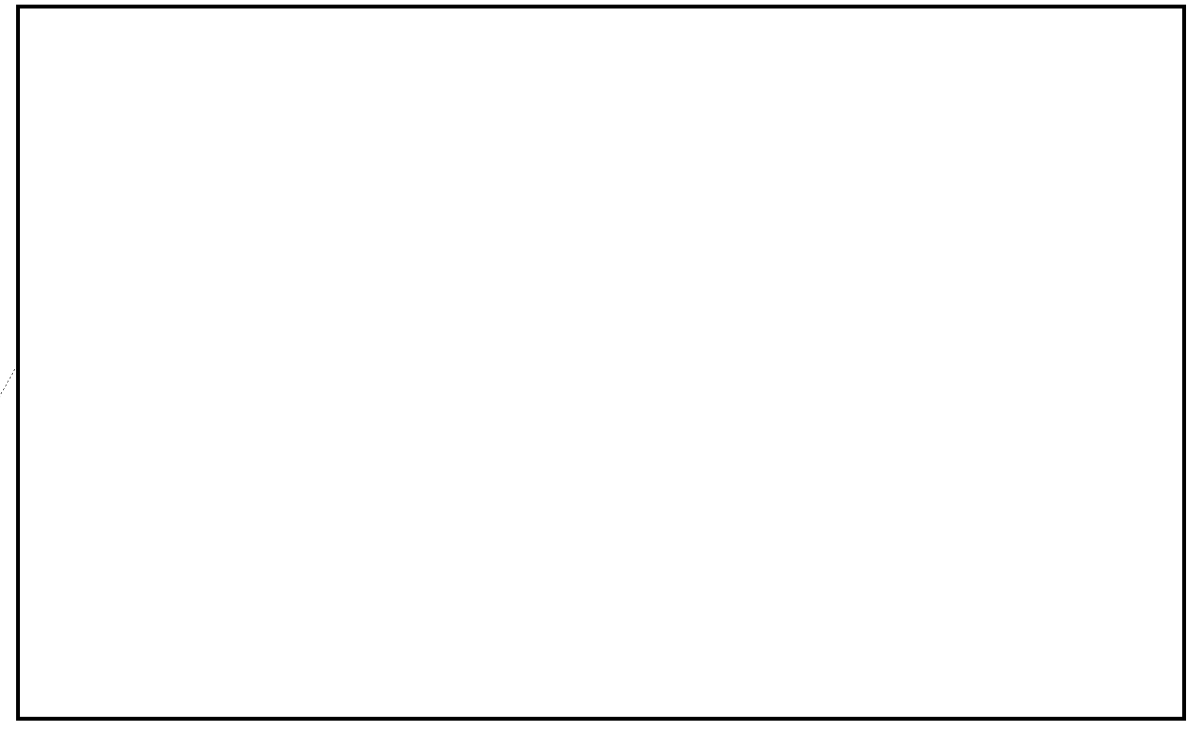
b. The British, however, have chosen to disassociate the problem of French physical and personnel insecurity from the problem of French communication insecurity, and simply do not mention the former at all in either Reference (a) or (b).

COMMENT: This is a fundamental difference in position between the U.K. and the U.S. and must be resolved before any progress is made by the Conference. This matter was considered by the U.S. Subcommittee on Security and its report should be studied in this connection. It is true that Par. 2 of Reference (b) proposes no assistance to the French and [redacted] until they have agreed (1) to overhaul completely their cipher arrangements and (2) to accept the appointment of British and/or U.S. experts to assist them; but these provisos by no means address themselves to the fundamental point at issue and do not answer the point raised in the last sentence of Par. 3g of Reference (c).

2. First Approach to the French:

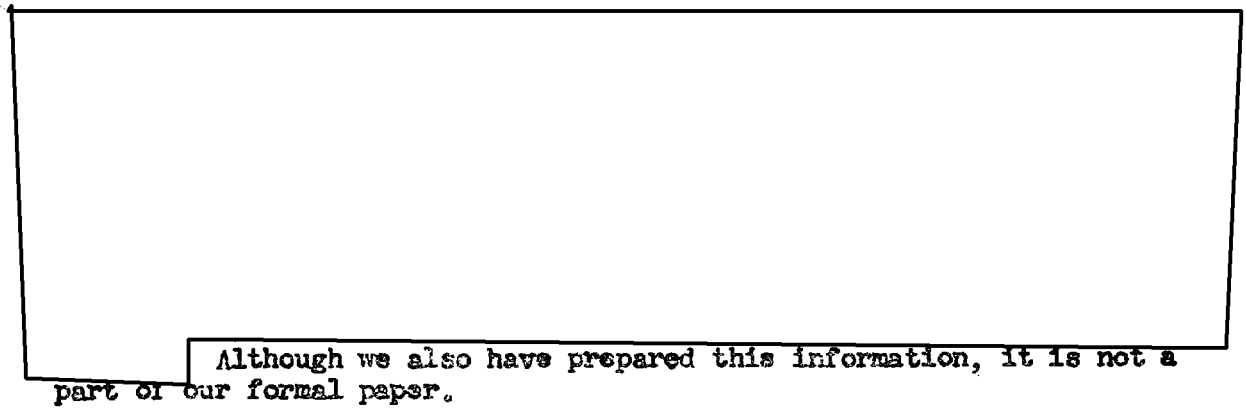
a. The U.S. paper (Par. 3h of Reference (c)) states that the "bases for a successful approach to the French Government cannot yet be indicated and should be established in the discussions at the U.S.-U.K. Conference in Washington." However, Par. 6 of Enclosure B to the U.S. paper outlines in general such approach as might be feasible and would be necessary, if the plan to discuss the COMINT security is carried out:"...it is apparent that a complete overhaul of the French Diplomatic and Military cryptographic systems and practices would be necessary. This would involve not only [redacted] but also establishing a basis on which the French would be provided with technical assistance to enable them to reorganize their cryptographic systems and practices to insure secure communications."

b. The British propose a first approach to the French at the highest level and outline quite specifically, in Par. 2 of Reference (b), the steps to be taken:



COMMENT: While not differing in basic ideas as to necessity for a complete overhaul of French diplomatic systems, it will be noted that the British plan is already well-defined and possibly too concrete, indicating some rigidity in British thinking on this point; the U.S. plan still fluid.

3. Details as to disclosures to be made, technical approach, and general considerations regarding existing systems:



Although we also have prepared this information, it is not a part of our formal paper.

Enclosure to AFSA-00T
MEMO TO DIRAFSA, 26 Apr 51 4 Enclosure

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

~~U. S. EYES ONLY~~

[redacted] whereas Reference (a) goes into this matter quite in detail, British anxiety about the matter being quite apparent. It is possible that the U.S. paper fails to give sufficient consideration to the matter.

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

c. Both the U.S. and the U.K. agree in the desirability of disclosing a minimum amount of information [redacted]

d. Reference (b) goes into considerable detail as to specific weak practices in the [redacted] The U.S. paper is couched in more general terms and appears to me to give a much better overall picture of the situation.

e. The U.K. paper dealing with non-diplomatic systems (Reference (a)) is so long and involved that a detailed analysis and comparison as to technical content is not possible in the time available. It is apparent that the British regard the problems of improvement in this sphere as being more difficult of solution, and the schemes they propose appear to me to be too complicated, impractical, and not likely to be accepted by the French. Before suggesting solutions, the U.K. paper (Reference (a)) sums up arguments and conclusions by stating (Par. 42):

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

[redacted] The remainder of this paper is therefore based on the assumption that the French are to be given this information."

4. Conclusions:

a. The conclusions in the U.K. papers (both References (a) and (b)) concern themselves mostly with technical details; those in the U.S. paper are much more general in character and, I believe, more to the point.

b. One conclusion in Reference (b), that in Par. 16(i), is of interest: "Unless they /the French diplomatic posts/ are issued with British or American machines, ... only hand systems will be available". Evidently, the British have given no serious consideration to U.S.-U.K. providing the French with the CCM or equivalent, for

diplomatic use. Hence, the British proposals for the solution to the problem of what the French should use for diplomatic communications become quite complicated, involving considerations as to types of code books, subtractor systems, and their probable abuse, one-time pad systems, weaknesses of French methods for generating the pads, lack of personnel, etc.

c. The foregoing differences in the U.S. and the U.K. papers point up the principal difference in the solutions proposed. This is taken up in the next paragraph.

5. Recommendations as to systems to be offered or recommended to the French:

a. Diplomatic:

(1) The U.S. plan divides French diplomatic posts into three categories:

Category I: a small group of locations which handle the most important information;

" II: all capitals not included in a plus a selected group of important cities;

" III: all other diplomatic posts.

For Category I, the CCM with Simplex settings is recommended; for II the M-209 with special settings to be used with a special literal code; for III, the present French systems. In the U.S. Plan, one-time pad systems would be used only as an emergency stand-by for Category I, and their cumbersomeness is noted, with consequent comment as to its probable unacceptability to the French for rapid communications.

(2) The British plan (Par. 17 of Reference (b)) is "to put the major part of their /French/ important traffic on to one-time systems." Main centers and outstations which would use the one-time systems are outlined -- the set-up appears complicated, and, moreover, it does not "cater for" certain important traffic. In order to do so further complications are added.

COMMENT: The U.S. plan is believed to be much more simple, specific, and practical than the U.K. plan, which is not likely to be accepted by the French. The U.K. is willing to offer only advice and technical assistance of experts; the U.S. is willing to offer all that and much more, viz., machines.

~~U. S. EYES ONLY~~

b. Military:

(1) The U.S. plan divides the Armed Service communications into three similar categories: Category I (high-level) for top-level military representatives of each nation of NATO; II (intermediate level) for French communications down to division level; and III for national military communications below division. For I, the U.S. plan states that British TYPEX with Simplex systems is now being used and an adapted NATO CCM system is proposed; for II the CCM is proposed; for III, the M-209 to encipher plain language (not code groups as in the case of Category II of the plan for the Diplomatic communications).

(2) Neither Reference (a) nor Reference (b) mentions plans for NATO communications and thus the British have not coordinated their proposed solution with plans for security of NATO communications.

(3) The British propose a wider use of one-time pads, the placing of fixed naval communications onto multi-way pads; and, by way of modification of existing machine procedures, the use of present machines but with double encipherment, using two machines with different lug and pin settings; machine systems with underlying basic book instead of plain language. Simplex settings with the B-211 are also considered, and improved procedures are mentioned.

CONTENT: The British propose the use of one-time pads and the continued employment of present machines used by the French, with double encipherment or Simplex settings. The U.S. proposes the replacement of the French machines by CCM or adapted CCM. One-time pads are believed by the U.S. to be too cumbersome for diplomatic and particularly for general military use.

~~U. S. EYES ONLY~~