REPORT BY THE TECHNICAL COMMITTEE

to the

EXECUTIVE COMMITTEE

of the

U.K.-U.S. CONFERENCE ON SECURITY OF FRENCH COMMUNICATIONS

THE PROBLEM

1. To examine present French cryptographic systems and procedures, and to formulate a U.S.-U.K. plan for improvement of the security thereof.

FACTS BEARING ON THE PROBLEM AND DISCUSSION

2. See Enclosure "B".

CONCLUSIONS

3. It is concluded that:

[redacted]

b. The present French cryptographic organizations do not possess the necessary cryptanalytic appreciation to insure provision of systems affording adequate cryptographic security, or, if they do possess the requisite knowledge, the information is not being applied or properly employed.

c. This situation can be improved only by a relatively complete overhaul of the French cryptographic systems and practices. The present insecure French cryptographic systems and practices should be replaced by secure systems and practices, and a specific plan for such replacement should be established.

d. Positive measures to effect such a plan should be introduced to the extent of providing, at least in part, the cryptographic devices and associated techniques essential to security. A survey is required to establish the number of machines that can be loaned and the dates when they can be made available.

TOP SECRET ACORN

e. This will materially reduce the amount of intelligence now available to Russia from COMINT sources probably exploitable by them;

f. Negotiations with the French should be so conducted and the plan so devised

g. As a preliminary to entering upon any negotiations with the French there should be reasonable assurance that the effects of improving their communication security will not be nullified or diminished by physical and personnel insecurity in the French Government. It is obvious that without such assurance

h. Major advantages will accrue if the technical disclosures to the French are made on a combined basis.

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

RECOMMENDATIONS

4. It is recommended that:

a. Enclosure "A" be approved as the specific plan for improvement of French communications.

b. The U.S. and U.K. determine the number of machines that can be loaned and the dates when they can be made available.

TOP SECRET ACORN

ENCLOSURE "A"

PLAN FOR IMPROVING THE CRYPTOGRAPHIC SECURITY OF FRENCH DIPLOMATIC COMMUNICATIONS

A. DIPLOMATIC

1. The proposal presented herein for ensuring the security of French diplomatic communications considers that the various French diplomatic posts should be subdivided into three categories:

a. Category I: A group of locations which handle the most critical information and in considerable volume, such as Paris, London, and Washington.

b. Category II: All capitals not included in a. plus a selected group of important cities whose communications include information which should have complete protection.

c. Category III: All other diplomatic posts.

Note: ~~The Appendix to~~ A list of 32 of the French posts which should be included in Categories I and II is given in Para. 3

2. The systems recommended, respectively, for the three categories listed above are:

a. For Category I: The Combined Cipher Machine with Simplex settings. The word Simplex is used to mean a procedure whereby each message has its own rotor arrangement and alignment provided by means of a special key list. The lists are prepared for point-to-point use so that each station can decipher only those messages specifically addressed to it. For the transmission of multiple-address messages, a multiple holder Simplex key list is also provided. A one-time pad system should be provided as an emergency stand-by in this category. The number of locations that will be included in Category I will be determined by the number of equipments that can be made available. It is not yet possible to ascertain the number of machines that can be supplied for this purpose because of commitments already made to NATO and the requirement for a survey in this regard by the Services. A small number of machines can be supplied initially to cover the most important locations. As the number of machines available increases, additional locations can be changed from Category II to Category I.

The greater the number of posts which could be included in Category I, the more simple would become the problem of integrated and multiple one-time pad networks for Category II posts.

b. For Category II: A numerical code book super-encrypted with one-time pad. It is recommended that a new code book be issued for this specific purpose.

c. For Category III: Present French systems could continue to be used.

B. ARMED SERVICES:

3. Authorities concerned with NATO communications have already established three categories of such communications:

a. Category I (High-level): This category embraces the top-level military representatives of each nation of NATO. For this level, the British TYPEX machine, with Simplex settings is being used. Consideration is being given to replacing that system by a NATO CCM system.

b. Category II (Intermediate-level): This category embraces military headquarters down to and including Division headquarters or equivalent. For this level the U.S. and the U.K. have already proposed the CCM. It has been accepted by France and the proposal is now to be considered by the other NATO governments. This does not however represent a complete solution to the French Category II problem, because it does not provide for 2nd level military headquarters, both in France and her colonies, which are not included in NATO. No estimate is available of how many additional machines will be required in this regard. It seems clear that the allowance for 2nd level NATO will be insufficient to supply the complete French requirement.

c. Category III: This is the combat level in the Army, Navy and Air Force. Discussions at present taking place in NATO are examining different proposals for combat systems and to that extent may resolve a portion of this general problem. It is recognized that the M-209 may be accepted as an interim solution for this category due to the quantities of equipment available to the French.

APPENDIX TO ENCLOSURE "A"

PRINCIPAL LOCATIONS TO BE INCLUDED IN CATEGORIES I AND II

Ankara
Athens
** Baden
* Bangkok
** Beirut
Belgrade
Berlin
Bonn
Brussels
Cairo
** Copenhagen
** Damascus
* Djakarta
The Hague
** Lisbon
London
** Madrid
Morocco
Moscow
New Delhi
New York
** Oslo
Paris
* Rangoon
Rome
Saigon
Singapore
** Stockholm
Taipei
Tokyo
Vienna
Washington

* Proposed by the Foreign Office only

** Proposed by the State Department only

ENCLOSURE "B"

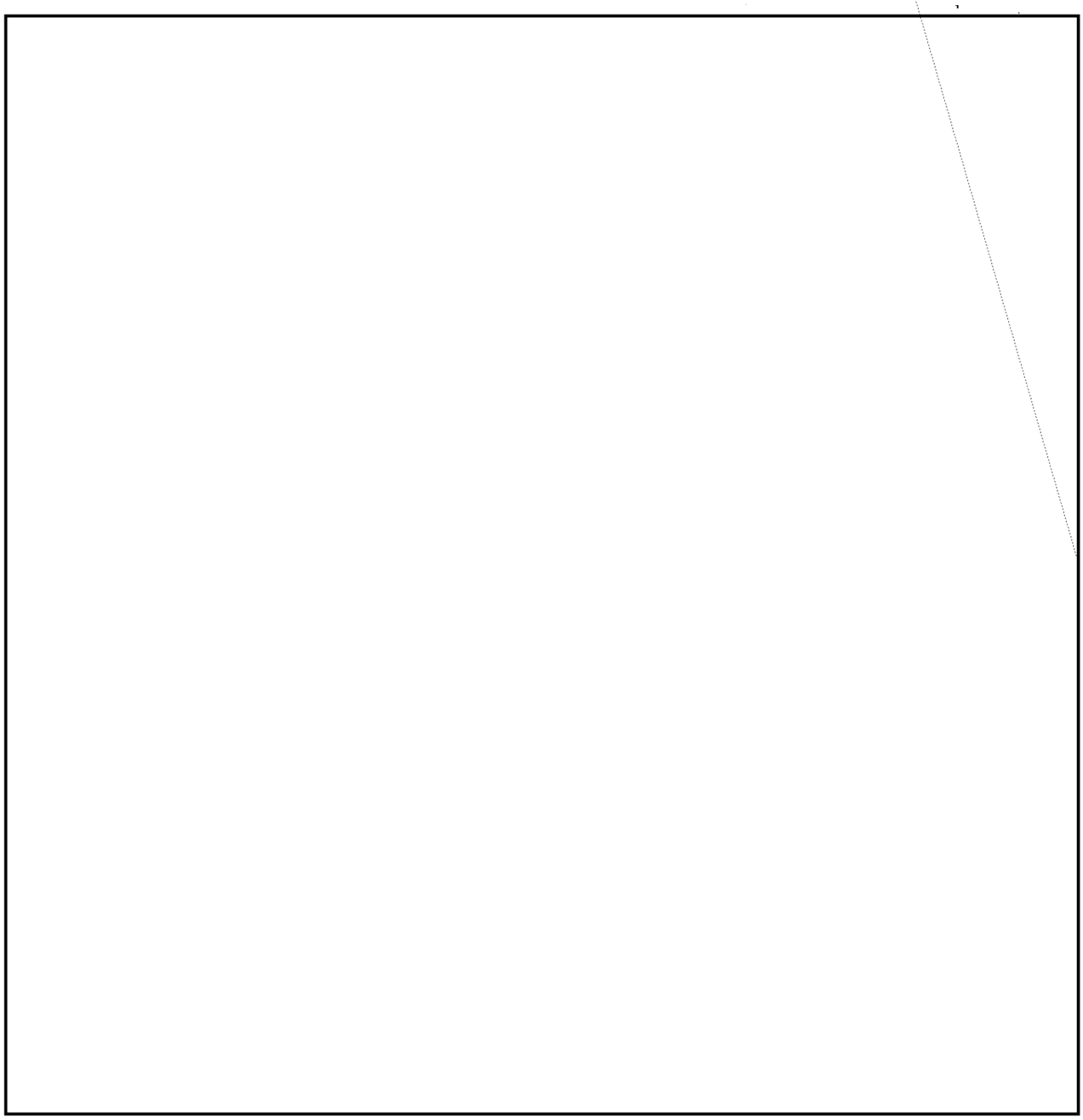
FACTS BEARING ON THE PROBLEM AND DISCUSSION

[redacted]

2. In regard to the current French diplomatic communications, observed French practices in cryptographic system design and distribution provide direct evidence that the present cryptographic organization in the French Diplomatic Service does not possess the necessary cryptanalytic appreciation to insure provision of systems affording adequate cryptographic security, or, if it does possess the requisite knowledge, the information is not being applied or properly employed, either in the Foreign Ministry or in diplomatic posts. Except as regards certain systems, which may be one-time pad, none

of the French diplomatic cryptographic systems possesses sufficient inherent security to permit its improvement to a point where it might be considered acceptable. It would therefore be necessary to discard the current systems and replace them with other systems based on sounder cryptographic principles. It would also be necessary to provide technically sound associated procedures and training in the proper use of the systems and procedures.

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



4. Although a tradition of sound communication security doctrine did exist in France, the current cryptographic practices observed in French diplomatic traffic indicate that the French have fallen far behind the U.S. and the U.K. in matters pertaining to communication security. The situation may be less serious in the Army and Navy but there, too, there is much room for improvement.

Therefore, technical assistance from outside the French cryptographic services is deemed essential for the success of any communication security program.

5. From an over-all consideration it may be stated that if the security of French diplomatic ~~and military~~ communications is to be improved it would be necessary to:

a. Replace the current ~~French~~ cryptographic systems of the FFO with secure systems for use in all important diplomatic posts, ~~and in the headquarters of all high-echelon military units.~~

b. Establish technically sound communication security procedures.

c. Insure adequate training in the use of the new systems and procedures.

d. Insure careful technical supervision over French diplomatic communications to maintain communication security.

6. In view of the foregoing, it is apparent that in order to achieve total security, a complete overhaul of the French diplomatic and military cryptographic systems and practices would be necessary. This would involve not only informing the French that their present systems are insecure but also establishing a basis on which the French would be provided with appropriate technical assistance to enable them to reorganize their cryptographic systems and practices to insure secure communications.

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

7. It is obvious that in assisting the French in improving the security of their cryptographic communications [redacted] However, (a) the necessity for removing those handicaps to proper diplomatic discussions and negotiations among the U.S., U.K. and French Governments which arise from present insecurity of French diplomatic communications, and (b) the importance of denying to Russia this source of COMINT, [redacted] and also to provide, at least in part, the cryptographic devices and associated techniques essential to security.

8. If the French FFO are informed of the weaknesses of their cryptographic systems, it is highly desirable that ~~they be given~~ as little information as

[redacted]

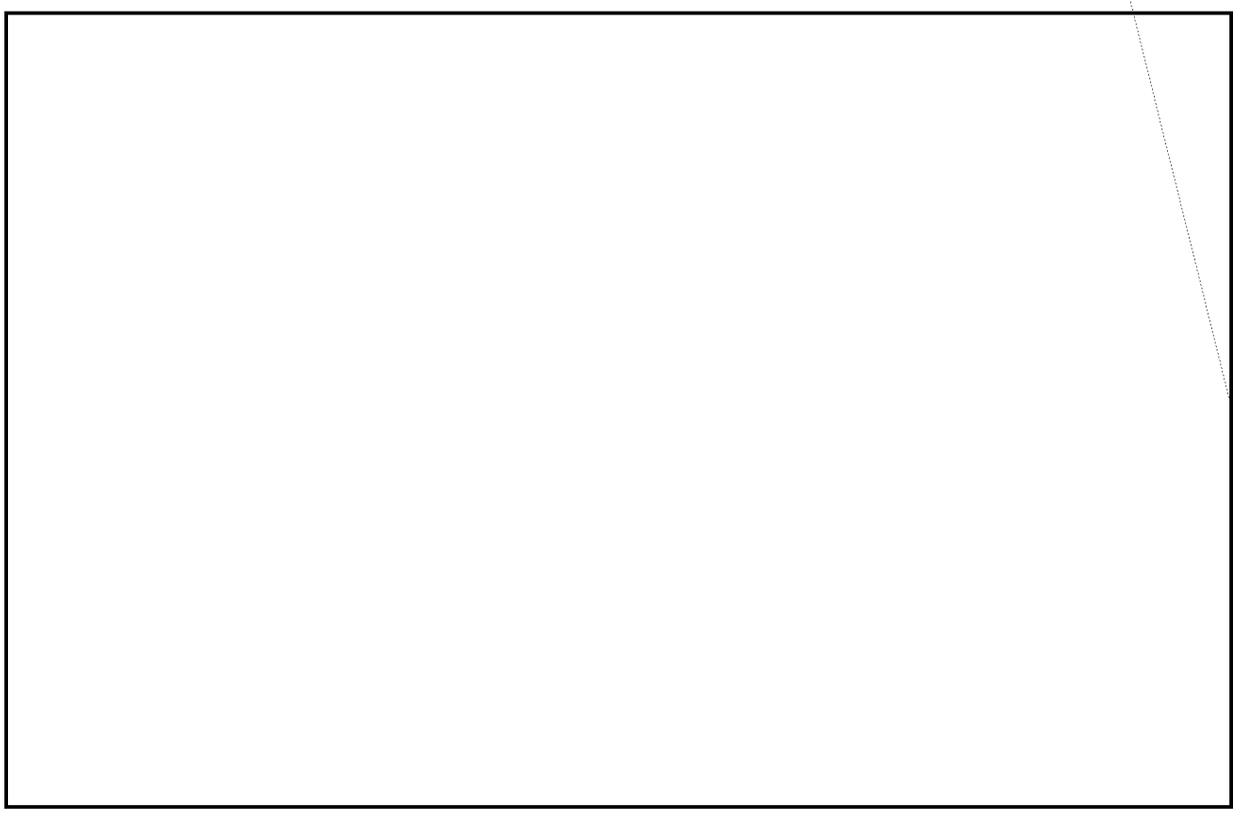
9. The possibility of Russian penetration of some or all of the French services, both diplomatic and military, cannot be ignored. Penetration may be either complete or partial, and may extend into either the sources of information or into the cryptographic services. Complete penetration of either type would make totally ineffective any plan for improving cryptographic security. [redacted] Therefore, before any steps are taken, there should be reasonable assurance of adequate physical and personnel security in the French Foreign Office, the French Armed Services, and the offices which control the cryptologic services. In addition to this, it is important that any plan proposed should provide the maximum possible protection against the effects of partial penetration of either type.

10. The localization introduced by Simplex procedures has a double advantage. First, it increases the cryptosecurity generally. An operating error will involve at most the compromise of one message as opposed to that of all the traffic sent in one day in a general cryptosystem. Secondly, if there should be an instance of penetration by the Russians at any installation, other than the Central Paris offices, which grants access to cryptographic information, the dangers resulting from such penetration are confined to those cryptonets in which that installation is involved. This results in reducing the consequent loss of information. This second advantage applies equally to the one-time pad cryptonets.

11. Considerable experience on the part of the British (and particularly of the Foreign Office) in the field of one-time pads has shown that the implementation of complex one-time pad networks is entirely practicable.

12. As regards production, by virtue of the fact that the British utilize [redacted] to a much greater extent than the U.S., the former have carried out a series of successful major investigations in the field of one-time pad manufacture, and have evolved improved processes, both on the duplicating and printing side and on the security aspects of the use of IBM/Hollerith equipment, including such matters as the preparation, size, and control of the random card file. ~~The results have proved to be very satisfactory.~~ There will however be an important and major requirement to instruct the French in such matters; it is not improbable that ~~the French Foreign Office~~ they are very little versed in these uses of tabulating machinery and have at present very little, if any, of the equipment available. Adequate detailed technical instruction can nevertheless be given to the French technicians [redacted]

13. The merit of the proposals in the Cryptographic Plan is the provision of a high degree of security for upper level French diplomatic and NATO communications, together with a minimum disclosure to the French of systems and ideas with which they are not already familiar. There is the further operational advantage of an electrical machine to replace slower and more laborious hand systems. For the transmission of international diplomatic or highest-level military traffic dealing with Western Union and NATO affairs, the French have been provided with TYPEX machines and they are presently using a Simplex procedure with these machines in the highest echelons of NATO; the Combined Cipher Machine is also being offered to them, as well as to other NATO signatories, for NATO communications and this has already been accepted by the French. Adequate training in the new systems will therefore be greatly simplified as a result of the already-existing familiarity with them.



15. With the exceptions mentioned in paragraph 14, the plan proposed in Enclosure "A" is a reasonable and economical program for providing adequate cryptographic security for the various levels of French diplomatic and military communications. The plan will, if properly executed, effectively prevent the production of a significant amount of communication intelligence. The plan is divided into two parts: A- For diplomatic communications, and B- For the communications of the Armed Services. Part B has been coordinated with the plan now under study by authorities concerned with NATO communications.