

~~TOP SECRET FROTH~~
~~TOP SECRET FROTH~~

8 January 1954

MEMORANDUM FOR THE SPECIAL ASSISTANT, INTELLIGENCE

SUBJECT: Meeting of the Ad Hoc Committee for the Improvement of Allied (NATO) Communications Security.

1. The Ad Hoc Committee for the Improvement of Allied Communications Security met on 8 January 1954 from 1030 to 1330 to consider means of improving French COMSEC during the Berlin Conference of Foreign Ministers. This meeting was held at the request of the State representative because of the suggestion at the USCIB meeting of 7 January that the Department of State consider action on this matter. The meeting was called to order by its Chairman, who explained the problem and who then asked the Executive Secretary of USCIB to assume the chair. Those present were Captain Taylor and Major Culmer of USCIB Secretariat; Messrs. Friedman, Raven, Corey, Shinn and Kerby of NSA; Messrs. Polyzoides, Packard and Walker of State; and Mr. Ellis of FBI. Mrs. Farrell of State acted as recording secretary.

2. The meeting was conducted in accordance with terms of reference offered by Mr. Polyzoides, accepted by the Committee and attached to this memorandum. The meeting also considered the recent de Vosjoli request but concluded finally that it did not affect the Committee's recommendations.

3. Initially, the Committee attempted to determine what alternative methods could significantly improve the security of French communications between Berlin and Paris, without regard to the possibility of timely implementation of these methods. The following methods were suggested:

(a) To instruct the French in the secure use of the STURGEON machine.

(b) To have the US, UK and France agree to use only authorized first-level NATO crypto systems.

~~TOP SECRET FROTH~~
~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~

-2-

(c) To provide the French with SIGTOT machines modified with tape slitters.

(d) To provide the French with US off-line literal systems such as the AFSAM-7 and the ECM.

(e) To have the US, UK and France agree that all conference communications, after encipherment in national systems, be super-enciphered and transmitted in an approved UKUSA system through a common message center.

4. The Committee then proceeded to discuss the technical implications of each method as well as the time and administrative difficulties each would involve. For technical reasons alternatives (a), (c) and (d) were eliminated. Alternative (e) was eliminated as being a more complicated method of reaching the result achieved by alternative (b). It was agreed that alternative (b) is technically feasible. [Under this method the US and UK may use any of their national systems which have received NATO approval as first level crypto systems. Since the French have no NATO-approved national first level system, they will have to use TYPEX MK II. Extra machines are available in the UK if needed.] Additional technical reasons for settling on this alternative are (a) French use of and familiarity with the TYPEX MK II; and (b) the relatively higher protection afforded by TYPEX MK II against operator abuse.

5. The Committee then considered the effect of such a proposal to the French with reference to the terms of the US-UK Conference of June 1953 and the US proposed long-range program for the improvement of French COMSEC. It was agreed that if the US, UK and France are included in the proposal, and if no extension of TYPEX use is proposed except to Berlin, it is within the terms of the June Conference. The Committee is unable at this time to determine the effect of this proposal on the long-range program but believes that it may not be harmful and might even be helpful.

6. The Committee also considered the effect of this proposal on French lateral communications. It was concluded that in addition to the strong possibility of improving

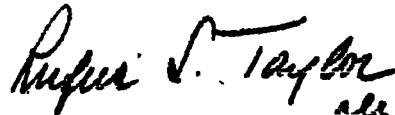
~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~

-3-

COMSEC between Paris and Berlin, the proposal also offered the possibility of improvement on the links between Paris and London and Washington. The proposal would not offer the possibility of improvement on the links between other points such as Paris-Moscow, Paris-Rome and Paris-Saigon. The Committee noted that all extra available TYPEX machines are held by the UK and that, consequently, the UK will have to determine both the necessity to provide additional equipment for this purpose and the time required to do so.

7. The Committee did not consider the political feasibility of the proposal in detail. It was noted, however, that the proposal might be made attractive to the French by virtue of the location of the conference.



RUFUS L. TAYLOR
Captain, U. S. Navy
Chairman Pro Tem

Enclosure:

Terms of Reference.

~~TOP SECRET FROTH~~
~~TOP SECRET FROTH~~

8 January 1954

SECURITY OF FRENCH COMMUNICATIONS CONCERNING THE
BERLIN CONFERENCE OF FOREIGN MINISTERS

1. Are there any feasible means by which these French communications can be made secure (Plan A, Plan B, etc.)?
2. If so, are these plans within, or beyond, the terms of reference established by the US-UK Conference on the COMSEC of NATO Countries in June 1953?
 - a. Those within --
 - b. Those beyond --
3. What would be the effect of applying any of these plans now to the long-range program for the improvement of French COMSEC?
4. What changes to the terms of reference of the US-UK Conference would be required to implement those plans which exceed the terms of reference established by the Conference?
5. In the light of (a) paragraphs 2-4 above and (b) the risks to the success of the Conference and to the security of the US which may be expected to arise from the insecurity of these French communications, should any of these plans be recommended to USCIB and LSIB?