

~~TOP SECRET CANOE - SECURITY INFORMATION~~

MINUTES OF SECOND MEETING
US CONFEREES
FRENCH COMMUNICATIONS SECURITY CONFERENCE

1000 MONDAY, 25 MAY 1953
Room 19-232B, U. S. NAVAL SECURITY STATION
WASHINGTON, D. C.

Those present were:

Mr. W. F. Friedman, NSA, Chairman
Mr. R. F. Packard (State)
Mr. W. H. Godel (OSD)
Mr. V. P. Keay (FBI)
Mr. F. B. Rowlett (CIA)
Capt. R. L. Taylor, USN (Navy)
Capt. G. Grange, USN (Navy)
Col. M. L. Sherburn, USA (Army)
Lt. Col. J. M. Anderson, USAF (Air Force)
Lt. K. B. Monypeny, Jr., Secretary (NSA)

NSA Observers

Dr. L. E. Shinn
Dr. L. W. Tordella
Dr. H. J. Stukey
Mr. Frank Austin

1. The minutes of the first meeting were considered and the last clause of paragraph 6 corrected to read as follows: "... and until that report was available it would be impossible for the US conferees to recommend to USCIB a US position." Other nonsubstantive changes were directed and the minutes approved as corrected.

2. With reference to paragraph 8 of the minutes of the first meeting, the Chairman stated that, in an interview with Mr. Elliot, he had requested his personal and latest views as to the state of internal (physical and personnel) security in the French government. In substance, Mr. Elliot's views, as reported by the Chairman, were as follows: that certain improvements have been made in the armed services and perhaps in certain of the civil

This document is to be read only by those personnel officially indoctrinated in accordance with communication intelligence security regulations and authorized to receive the information reported herein.

~~TOP SECRET CANOE - SECURITY INFORMATION~~

administrations; however, in the Ministry of Foreign Affairs (MFA) little if any improvement had been accomplished thus far; and that an approach to the MFA would be inadvisable at this time because it is not known who is secure. The Chairman added that a cable has been sent by Mr. Elliot to the CIA representative in Paris, to ascertain the immediate situation and an interim reply is expected by 27 May, 1953.

3. In elaboration of the foregoing statement, Mr. Keay stated that security in France is not government wide, and that the French could not be considered security conscious. He said that they have handicaps to overcome in approaching anything like what we have. Examples of handicaps were as follows: 26 per cent of electorate is communistic, the constitution prohibits firing any government employee for political beliefs, and communism is considered as just another political belief. In conclusion he noted that French security was improved but thus far was well below acceptable standards.

EO 3.3(h) (2)

PL 86-36/50 USC 3605

4. The Chairman pointed out the difficult problem to be faced.

However, the same information would most probably not be denied to the Soviet, because it is presumed that it has the means of obtaining the information from agents, or could steal the cryptomaterial. Yet in time of war we are to be allied with these NATO governments and the security of our troops will to a greater or lesser degree depend on their communication security. In any case the net result of whatever action we take remains the same, namely: If we tell and show them how to improve their cryptosystems and associated procedures,

The Chairman added that there were some who felt that the Polyzoides report does not present a clear-cut solution to the problem. Dr. Shinn then explained that this was due to the committee being given two separate charges--the first, to make a study of the facts of leakage of vital information, and the second, to make the paper a basis for the official position to be taken by the US conferees in the forthcoming conference, with specific recommendations. He added that the result was not strictly one thing or the other.

This document is to be read only by those personnel officially indoctrinated in accordance with communication intelligence security regulations and authorized to receive the information reported herein.

~~TOP SECRET CANOE - SECURITY INFORMATION~~

5. In a discussion concerning the noted improvement of French Communications security, Mr. Rowlett stated that it could be concluded that such improvement was due to one, or ^{both} more of the following:

- a. General world-wide tendency towards better cryptographic security.
- b. NATO program of improvement in cryptographic usage.

~~c. Recognition of general danger of penetration by USSR agents or sympathizers.~~
Whether Col. Black and his organization have been involved in

6. Mr. Rowlett suggested that in order to proceed with the work assigned to this committee it might be advisable first to examine the Polyzoides report, next to consider the question of French internal security, and finally to enter into discussion with the British to ascertain their views. The Chairman pointed out that the British were coming, as stated in the LSIB memo to USCIB, "to review the proposed tactics of the approach to the French", and not to review the whole question. Capt. Taylor commented that in view of Mr. Dulles' statement that the National Security Council should be asked to reaffirm the US 1951 position, we were not committed to making an approach to the French. Mr. Friedman then recalled that in a recent telegram to Brig. Tiltman, the contents of which were conveyed to Rear Admiral Wenger, it was hinted that Mr. [redacted] was included in the UK team in order to be in a position to deal with the whole question of whether or not it is advisable to make an approach. Therefore, it seems clear that the forthcoming conference will go beyond a mere review of the proposed tactics of an approach.

improving French Security is essential.

7. Before considering the conclusions and recommendations of the Polyzoides report, the Chairman asked Mr. Austin to present such general comments as he cared to make. Mr. Austin stated that he felt the report is a good basis for discussion with the British, except that it does not specifically answer the question. [redacted]

[redacted]
The recommendation of the report seems to say

PL 86-36/50 USC 3605

This document is to be read only by those personnel officially indoctrinated in accordance with communication intelligence security regulations and authorized to receive the information reported herein.

~~TOP SECRET CANOE - SECURITY INFORMATION~~

that the cryptosystems of these allies are good but their procedures are bad. It is known that we can improve the procedures; however the result of this would be a review of other systems

3. Dr. Shinn commented that it was just a matter of time. He pointed out that already steps had been taken to help to NATO governments in the form of cipher machines and other cryptomaterial. The recommendations of this report would accelerate such a decrease, and any direct approach involving would accelerate it even more. He suggested the question to consider is: How fast does the US want this process to be speeded up?

9. The conferees then proceeded to examine the conclusions and recommendations of the Polyzoides report and agreed to present the following comments thereon to USCIB:

- a. A paragraph 3 should be included under Section B on page 6, to read as follows: "Nonetheless, it can be assumed that the security of military traffic could bear improvement."
- b. With reference to paragraph 6 of Section C on page 7, it should be noted that while the total number of messages containing information whose "leakage" to the USSR made them potentially damaging to US interests (see paragraph 3 of

- c. Paragraph 7 of Section D (page 9) should be reworded to read as follows: "An effort

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

This document is to be read only by those personnel officially indoctrinated in accordance with communication intelligence security regulations and authorized to receive the information reported herein.

~~TOP SECRET CANOE - SECURITY INFORMATION~~

to improve national cryptographic and communications practices could reduce appreciably the total communications security problem under consideration and should be made prior to any effort to alter the crypto-systems basically or to encourage the use of more complicated cryptographic equipment."

- d. Paragraph 1 of the Recommendations (page 10) should be reworded to read "No nation-to-nation approach involving disclosures" etc.

10. The conferees then agreed that:

- a. If paragraphs 2 and 4 of the Recommendations are implemented, [redacted]

[redacted] and that this will depend on how long a time we wish to take to implement those recommendations.

- b. The foregoing consequence should be made clear to USCIB and those in higher authority.
- c. The Ad Hoc Committee Report could well serve as a basis for discussion with the UK delegation to the forthcoming US/UK Conference.
- d. The UK delegates may have information not possessed by the US delegates, or they may be able to present the matters involved in a different light, or as a consequence of frank interchange of opinions the US delegates might better be able to arrive at recommendations for a USCIB and thus, in turn, a US position with respect to the question of the advisability of making an approach to the French and other NATO countries.
- e. USCIB be informed of the opinions expressed in subparagraphs c and d above.

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

This document is to be read only by those personnel officially indoctrinated in accordance with communication intelligence security regulations and authorized to receive the information reported herein.

~~TOP SECRET CANOE - SECURITY INFORMATION~~

f. With reference to paragraph 7 of the Recommendations (page 11), for the present NSC should merely be briefed and informed of an impending conference with the British, and the reasons therefor; the NSC should not, at this time, be asked to affirm any previous decision on the question or to make a new decision in the premises.

11. There was some discussion of the advisability of recommending to USCIB at its forthcoming meeting on 28 May 1953 that a message be sent to the UK suggesting that, because of the complexity of the problems involved and the shortness of time in which to consider them and arrive at a firm position, the conference be postponed for a short time. However, the Conferees finally agreed not to make such a recommendation; on the contrary, they felt that there was perhaps something to be gained by not asking for a postponement since discussion with the UK delegates might help us jointly to find a logical position in the whole question.

12. There was no further business to come before the meeting. The meeting adjourned at 1230.


K. B. Konypeny, Jr.
Secretary