MINUTES OF THIRD MEETING
US CONFEREES
FRENCH COMMUNICATIONS SECURITY CONFERENCE

1000 THURSDAY, 28 MAY 1953
Room 19-252E, 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. S. E. Ellis (FBI)
Mr. F. B. Rowlett (CIA)
Capt. R. L. Taylor, USN (Navy)
Capt. J. Grange, USN (Navy)
Col. M. L. Sherburn, USA (Army)
Lt. Col. J. M. Anderson, USAF (Air Force)
Lt. M. E. Monypeny, Jr., Secretary (NSA)

NSA Observers

Dr. L. M. Shinn
Dr. L. W. Tordella
Dr. H. J. Stukey
Mr. Frank Austin
Mr. T. A. Polyzoides
Mr. F. A. Raven

1. The minutes of the second meeting were considered and paragraph 5 corrected as follows: 5(c) was deleted from the minutes; the word "more" in the paragraph heading was changed to read "both"; an additional sentence was added as a comment on the whole paragraph "Whether Col. Black and his organization have been involved in improving French Security is conjectural." The minutes were then approved as corrected.

2. The Chairman then requested the view of the conferees on the British position paper. It was the consensus that there had not been sufficient time to study the report, but that it appeared to form a firm basis for discussion.

3. The Chairman said that he had called the meeting for the purpose of obtaining a US viewpoint on the

British paper. He stated that in his opinion there was not too much divergence between the British position paper and the Polyzoides report, pointing out the ultimate consequence of the action recommended by each paper would be the same, viz, [redacted] from these sources, and that the major question, therefore, merely was how fast we should proceed with the steps to be taken to improve the communication security of France and other NATO members. He noted that the UK position was that steps should be taken immediately, [redacted] On the other hand, he stated that US position seemed to be to take steps by a gradual "educative" process, meaning that the same end-result would be accomplished but the process would extend over a longer period of time during which we could perhaps continue [redacted] from those sources.

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

4. The Chairman continued by saying that although the UK paper had been carefully drafted he considered that the report contained one glaring weakness. He stated this weakness as being the statement, unsupported by facts, "that were this source of leakage [redacted] removed, the Russians could not obtain the same information by physical means." (See Par. 3, Introduction, DGC/3441) Mr. Polyzoides commented that the assumption that penetration never occurs was fantastic, and particularly with regard to France. He added that penetration by the British had been excellent in the past.

5. In response to a request by the Chairman, Mr. Polyzoides presented his personal views on the British paper, noting that he had not had sufficient time to study it carefully. He stated that he found it difficult to relate the facts to the conclusions, and as a result could not agree with the recommendations. He said that he had the feeling that the UK was trying to prove a point with material which could not be used for that purpose, and as a result the report contained dangerous generalities. ~~He noted that in reaching a decision as to what steps to take to improve French security, there was no battle to be fought between the [redacted] Yet, he said, the British paper seemed to lead one to such conclusions.~~ He stated that there was no proposal in

the paper to correct simple misuse of communications procedures. In concluding, he added that the critical problem concerned was the danger to our COMSEC by the intrusion into [redacted]

6. Mr. Austin stated that he considered the main difference between the UK position and the Polyzoides report to be a difference in timing and a difference in how to make an approach. He added that he did not consider the British had the facts to support their conclusions. He requested that Mr. Polyzoides elaborate on his last statement concerning COMSEC. Mr. Polyzoides replied that he was concerned with the progress rate of this type of education for other nations. He said that he did not consider it necessary to [redacted] show other nations how to use the Hagelin properly. Mr. Austin then agreed that the approach should be to do what was necessary through COMSEC.

7. The Chairman then distributed to the conferees a paper (TAB 1) prepared by Dr. Shinn setting forth his views of the UK paper. After a brief perusal it was discussed in detail by the conferees.

8. The Chairman then inquired if any of the conferees had suggestions for recommendations to be made to USCIB. Mr. Packard proposed the following recommendations:

a. That the conference be held as planned.

b. That neither USCIB nor NSC adopt, prior to the conference, a fixed position as to the steps to be taken to improve French and other NATO members' COMSEC.

c. That the British be informed forthwith that the US desires to extend the agenda to include a review of all conclusions reached at 1951 conference, and that their paper (DGC/3441) together with our paper (Polyzoides report) be used as a basis for discussion.

d. That USCIB should accept the ad hoc Committee report as a partial basis for discussion with the UK delegation; sanitise the report and hand it forthwith to the Senior British Liaison Officer (Brig. Tiltman).

The conferees agreed that these recommendations should be presented to USCIB. It was further agreed that a memorandum should be prepared for the signature of the Chairman, USCIB, to be sent to SBLO, notifying him of the above.

9. The next meeting of the conferees was scheduled for 0930, Tuesday, June 2, 1953, at the same location. There was no further business to come before the meeting. The meeting adjourned at 1225.

K. B. Mohyphny, Jr.
Secretary

COMMENTS ON UK POSITION PAPER ~~TOP SECRET SECURITY INFORMATION~~

1. The subject paper is noteworthy not so much for its convincing nature, as for its evidence of a completely crystalized and rigid British position.

2. The portions dealing with mechanism can be ignored at this time, since they are secondary to the main question which is whether or not this step should be taken.

3. It appears from the paper as a whole that the U.K. is convinced:

A. That the insecurity of NATO national ciphers is of more value to Russia [redacted]

B. That Russia could obtain the information [redacted] by no other means.

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

C. That this requires that we unequivocally sacrifice all [redacted] without further delay.

4. Point 3A above is elaborated upon at length in Appendix A, in a survey somewhat similar to that prepared by the AdHoc Committee of USCIB. The surveys are different in that theirs is based primarily [redacted] and in the lack of any specific span of time in the U.K. study whereas the U.S. study covered a six month period. Examination of cited examples reveals that their selection is considerably less rigid in terms of what is damaging. I think it probable that examination of the complete texts would reveal many instances of messages which sound serious in the extract but are rather trivial in the whole. Some are highly questionable even from the extract, as for example:

Annexure 2 item	4c	
	4d	
	4e	
	4f	
	5b	
	5c	(30 Jan 53)
	6b	
	6d	
Annexure 4 item	4c	
Annexure 6 item	4c	
Annexure 7 item	3b	

~~U.S. OFFICIAL EYES ONLY~~

Nevertheless there is no doubt that a quantitatively small but nevertheless real leakage of intelligence is taking place. With respect to

Tab 1

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

[illegible] SECRET [illegible]

[redacted] the U.K. goes so far as to state that the amount is small. In this and in the appraisal of potential, the U.S. and U.K. are essentially agreed. The divergences are in estimates of degree.

5. Point 3B is the fundamental questionmark in the U.K. position. This statement made without qualification or further comment in any form represents an assumption rather than a fact. This assumption runs counter to the known:

a. Communist infiltration of France and other NATO nations.

b. Elaborate public press and radio reporting of all NATO nations - particularly the U.S.

c. Recent oral report by Mr. Elliott and Mr. Keay.

6. Point 3B is essential to the U.K. position, since unless it is very nearly true, the course of action which the U.K. insists upon would mean that Point 3C would be a burnt offering to an unresponsive deity. In addition if 3C is untrue to the extent that our attempts to inform the NATO nations leaked in their turn, we would hand the USSR a picture of our own cryptographic (and by inference, cryptanalytic) abilities.

7. The fundamental problem is not answered by the U.K. position paper. It remains a cold fact that someone with the requisite authority must make a command decision in which only part of the factors are known, a few can be guessed at and the remainder are hidden in the future:

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

a. Known - NATO national systems are not secure to us
   Infer - They are also not secure against the USSR

b. Known - The quantitative leakage is not dramatic as of now
   Infer - It could grow worse - particularly in war

c. Known - Western open sources leave relatively little work for USSR intelligence as of now
   Infer - We might not cut off much intelligence by securing NATO ciphers

d. Known - USSR espionage of all types is very widespread and quite effective
   Infer - We might not accomplish much and might have disclosed [redacted]

e. Known - [redacted]
   Infer - Who can judge its value to USSR?

U.S. OFFICIAL EYES ONLY

~~TOP SECRET~~
~~SECURITY BRANCH~~

QUERY ? - Will one or more NATO nations go communist? France? Italy? England?

" ? - Will at least the elements of existing cryptography remain if they were forced into Vichy positions?

" ? - [redacted]

" ? - [redacted]

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

8. In one sense the die is cast. All we can do is control the speed of the eventual loss. When modern devices were given NATO by the U.S. and U.K. we set in motion [redacted] This process will be relatively slow. We can accelerate this or let nature take its course. The decision must wefgh the possible gain against the accelerated loss.

a. One final thought: If we are going to do anything more at this moment, let us improve the COMSEC only of those of our NATO partners of whose constancy we feel more or less certain and whose COMSEC needs improvement. For example: Turkey.

L. E. SMITH

~~EYES ONLY~~