ONI "Brief of Telegrams of Department of State"

Colonel
1 Corderman

1. The problem as to whether the Navy should furnish a summary of State Department despatches to the British is one which cannot be positively answered by this office. No need can be seen for furnishing this information, however, it is possible there is a valid reason.

2. The State Department is using cryptographic systems with a reasonable degree of security. Most messages handled on the Washington-London circuit are cryptographed in a system which is highly secure from cryptanalytic attack. Most other State Department holders use cryptographic systems which are reasonably secure although not of the order of the London-Washington circuit. The general quality of the State Department systems has improved immeasurably since the beginning of the war. All State Department installations in the class of embassies, legations, plus some councils hold strip or machine systems for handling secret traffic. Further, all secret traffic is handled in a machine or strip system.

3. It is entirely true that paraphrases of messages would be of great value in breaking into a cryptographic system, and this case is no exception. It is entirely possible that given sufficient "crib" (which these paraphrases could well be), the daily keys for the generally held strip system could be recovered. It is not believed the system used on the London-Washington circuit could be broken cryptanalytically in this manner. Of course, any of the systems are susceptable to physical compromise.

4. Assuming it is desirable that the British be furnished the information in our State Department despatches, there should be no great concern over the se-

ONI "Brief of Telegrams of Department of State"
(Cont'd)

1
(Cont'd)

curity of the cryptographic systems with respect to the British providing these systems can be changed immediately should it be decided to no longer publish the despatches. The systems in use in the State Department could be easily changed providing sufficient time were given for the distribution of new keys.

5. As a recommended solution to the problem, the form of the daily summary might be changed to a digest in which all references to dates, message numbers, etc., would be eliminated. All messages should be thoroughly paraphrased with all quotes removed. This would greatly increase the difficulty of using paraphrases as a "crib" and would offer a middle course causing the least amount of embarrassment to those concerned.

Attached:
#1 Memo for Col Clarke
dtd 15 June 1945
#2 Memo for Col Clarke
Dtd 11 May 1945
w/ Encls. A & B
#3 Buck Slip frm Col Clarke
#4 Buck Slip frm Col Corderman

Charles H. Hiser
Major, Signal Corps
Cryptographic Branch
19 June 1945

SIS

Sig. C.A. Date. 19 June 45

SECRET

COPY

June 15, 1943

COPY

MEMORANDUM FOR COLONEL CLARKE

Subject: Atached Papers from Commander Wenger

I suggest that Commander Wneger's memorandum and the accompanying two papers be referred to Colonel Corderman for his opinion.

The Navy's reply strikes me as not responsive to the questions which we raised. I directed Commander Wenger's attention to the fact that the British Admiralty Delegation was getting the Navy Department's summary of State Department cables, pointing out that the summary was not devoted to material of purely naval interest, but covered in general all intelligence that was found in the State Department communications, and that this was a very questionable way of giving State Department information to a foreign organization.

On the specific question of possible compromising of codes, I neither said nor had in mind the matter of paraphrasing. It may be that our State Department codes are so secure that they cannot be broken evey by one who has knowledge of the contents of particular messages. To my mind, however, it would be foolhardy to make that assumption; and if that assumption cannot be made, then the point that I wanted to raise was whether we were not making it easy for the British to read State Department enciphered messages. I should suppose that a cryptanalyst would get off to a pretty good start on reading ciphers if he received from day to day even good paraphrases of messages containing specific information, naming names, giving numbers and containing information that sometimes can be identified in terms of specific words.

It may be that the interests of this country would be best served by a complete interchange of original messages with the British, even to the point where they could read our enciphered material any time they wanted to. Personally, I do not think that that would be a good policy, and moreover it is not the policy that the British Government pursues toward us. What I think is our valid objection to the Navy's course, in relation to the Admiralty Delegation, is that the Navy Department is pursuing its own private policy in this matter without consultation with Arlington Hall, (which sustains some degree of responsibility for the security of State Department communications), and that the policy seems, at least to me, to be contrary to the policy that is pursued by branches of the Government other than the Navy Department.

In this connection, among the facts that I wanted to report to you and Colonel Corderman, which I learned in England, were the following:

SECRET

Commander Denniston, when he gave me the organization chart of this outfit and told me the history of its operations since the last war, said that he thought he should be perfectly frank with me and therefor wanted to admit that, up to the time when we entered the war, Berkeley Street had an American Section which devoted its attention to our State Department communications. He said that when we entered the War, Mr. Churcill had personally ordered Berkeley Street to stop working on American codes, and that the Section had been dissolved. He says that since we entered the war they have not attempted to raad any United States communications. I have reflected a good deal on this statement, in the light of everything that I saw in England and of my own estimate of Denniston, and I personally have come to the conclusion that it is correct. In other words, I believe that the British are not attempting to read our State Department communications.

The British, however, are very realistic people, and depending on the course of events will certainly at some time -- possibly while the war is still on -- resume work on United States communications. There is no doubt whatever in my mind that our communications, a very substantial part of which pass through London, are received by the British censorship along with the communications of all other countries, and are being kept on file. The Navy Department, therefore, is supplying the British Government, through the Admiralty Delegation here, with paraphrases of a substantial portion of our State Department Traffic. If and when the British resume work on our ciphers, they will have quite a file of messages, the general contents of which they will know. Will this not be of use to their cryptanalysts?

The following is another bit about past British activities in reading our code:

The present head of the Beau Manor intercept station is Commander Illingworth. From what he told me about himself I concluded that he had been a cryptanalyst in the Navy until the early of middle 30's, when he retired and immediately joined the Foreign Office. In telling me about his past activities he said that he used to read the U. S. State Department ciphers and remarked jokingly that it was "lots of fun".

A. McC.