TOP SECRET

COPY

13 March 1947

MEMORANDUM

From: OP-20

TO: Fleet Admiral Nimitz
Via: OP-02, OP-03, OP-09

Subject: Collaboration between British and U.S. on Development of a New Combined Cipher Machine

1. During recent discussion between U.S. and British representatives, the British proposed collaboration on the development of what they termed a new and revolutionary idea for a cipher machine. This visualized a 24-wheel machine. Our opinion was that cryptographically the proposed British machine was good, but it would be highly complicated, and not practical for engineering and maintenance reasons.

2. Our counterproposal was the introduction of modifications to the existing Combined Cipher Machine which would greatly strengthen it cryptographically. The British will consider our proposal, making a detailed study thereof.

3. We proposed further that there should be better Security Rules to properly safeguard any combined crypto system. We feel that while the British are security-minded, they should provide better physical security for crypto machine.

4. The British crypto personnel have returned to the United Kingdom. They will make a detailed study of our proposals and formulate a new set of security regulations for submission to the CCB. We will throughly test our proposed modifications to the present combined cipher machine, and make the results known to the British. We will also submit a new set of security regulations to the CCB for consideration, in order to attain a mutually satisfactory security basis for any future collaboration.

5. The British indicated that they know a great deal about the ECM as a result of observations during the war. Actually, the British were never given the ECM officially, although it was used in certain British Commands with U. S. personnel provided

TOP SECRET

COPY

to operate and safeguard it. They have the highest opinion of it from a crypto security viewpoint and proposed that it (ECM) be used as the high-level combined crypto system, instead of trying to develop a new combined machine. We do not favor this, the principal reasons being-

a. We would lose control of its physical security - which we have thus far managed to maintain effectively.

b. If the ECM should get into the hands of any other nation, it might in the future be used for traffic which we probably could not read, if we so desired - at least not without a tremendous expenditure of funds for analytical machinery which does not yet exist and for employment of numerous personnel to operate that machinery.

c. We feel that the combined cipher machine (CCM) we now have is secure for combined use, and with proposed modifications should be secure for many years hence.

d. We have no better crypto device for our use than the ECM and if we shared it with any other nation we would have difficulty applying modifications to the ECM in the future. This last item is extremely important because our only present ideas for greater crypto security lie in the improvement of the ECM.

no! Army has plenty good ideas.

6. If the present combined cipher machine should be compromised, and if the British and U. S. are allied in a future war, we could give the British the ECM (if that should then be necessary). However, at this time, I recommend that our present policy of reserving the ECM strictly for U. S. military use be continued and any relaxation of this policy be resorted to at a later date only as an extreme emergency measure.

7. If we collaborate with the British in the future on a new combined cipher machine, the British will probably expect the U. S. to assume major responsibility for engineering development work. I do not believe that the British will reproduce our ECM for their own use - even though they claim to know the basic principles of the ECM because of expense and difficulties involved. However, this is a possibility, which we should not encourage.

8. This recent combined crypto conference was of value to both British and U. S. I recommend that we (Army and Navy) continue present limited crypto collaboration with the British.

Respectfully,

/s/ Earl E. Stone