

MEETINGS WITH UK REPRESENTATIVES

28 January 1947

PRESENT

UK
 Capt. Wilson
 Col. Marr-Johnson

NAVY
 Capt. Smith
 Com. Hargreaves

ARMY
 Col. Bisher
 Mr. Friedman
 Mr. Sinker

The British position as explained by Captain Wilson can be summarized as follows:

From a long-range point of view neither the Typex nor the OCM can be considered sufficiently secure to withstand improving cryptanalytic procedures and high speed techniques. This remains true even after the security is improved by such ideas as changeable cam contours. The British are seeking a replacement for Typex and would like to solve the problem of combined communication at the same time. Otherwise they would require two distinct machines. The difficulty with making concrete suggestions is the lack of knowledge about our ideas for future communication.

a. If we do not insist on retaining the principle of a cipher maze with stepping actuated by a control maze, the British would like to present a wholly new idea. Their cryptanalysts consider it better than the ECM with the added advantage that it would be adaptable to low echelon use.

b. If we insist on the ECM principle, then it could go into the OCM. The British are familiar with this principle and are building it into a radioteletype device which has the additional feature of varying end plates by means of an insert. The device could be designed for non-radioteletype use.

In either case, the low echelon problem deserves urgent consideration. It requires high security because it is the biggest element of danger from cribs, stereotypes, and other aids. We must make systems secure enough so we need no longer be concerned with paraphrasing, stereotypes, reencipherment, difficult indicator systems, etc. Intercommunicability between low and high echelon is not insisted on but desirable.

When the question of low echelon compromise and loss of signal intelligence was brought up, Captain Wilson indicated that security was paramount and outweighed signal intelligence considerations.

TOP SECRET

Incl 10

U. S. representatives made the following points:

- a. A tremendous investment has gone into the ECM and the machine is considered entirely satisfactory.
- b. The GSP 1700 could be considerably improved and is mechanically satisfactory.
- c. The information obtainable from low echelon solution is not anywhere near as great as is supposed and further it ties up enemy personnel.
- d. An enemy would certainly copy a cryptographic device captured in lower echelons if there were sufficient incentive.

The meeting adjourned to allow U. S. representatives to get indication from higher authority of a policy decision regarding long-term retention or scrapping of the ECM principle.

~~TOP SECRET~~
~~TOP SECRET~~