Delivered by Mr. Friedman
4 June
1
First SCAG Conference

~~TOP SECRET~~

With the agenda before us, it won't take much time to review briefly the ground to be covered in the technical sessions of this Conference.

It is hardly necessary to say that AFSA has many problems of current interest and that these are all of importance. If it were possible, I'm sure we would find it useful if at this first Conference SCAG could look into several of these problems. But we know that every member who has consented to serve on SCAG is a very busy man, and can devote only a quite limited amount of time to a consideration of AFSA's problems. Hence, it is advisable that we present at this first Conference only one of AFSA's problems, and for this reason have selected not only the most urgent one but also the one to the study of which the members of SCAG, by virtue of their special experience and capabilities, can bring knowledge to bear and suggest techniques which may be conducive to its early solution.

The technical sessions will therefore be confined strictly to the presentations required to develop the technical background SCAG will need in order to understand the nature of that problem, and in broad outline to present the directions in which our past experience with similar problems

~~TOP SECRET~~

indicates the research should travel. The specific problem is one which involves a cipher machine of apparently quite complex construction. I say "apparently quite complex construction" because not only have we never seen the machine but also we have been unable to gather by covert intelligence any information whatever concerning its construction. What little we know about it has been derived by deductive and inductive reasoning, based upon our studies of the cryptograms produced by the machine and collected for us by our intercept stations.

However, our inability to gather by direct or covert operations the technical details as to the construction of the machine need not constitute a frustrating bar to success in its solution. We have a good precedent for this statement, from our experience back in the two or three years preceding the attack on Pearl Harbor, during which period we were able to solve and reconstruct the complex cipher machine used by the Japanese Foreign Office and a similar machine used by the Japanese Navy for their highest echelon secret radiocommunications. We not only did this without preliminary knowledge of these machines but also we built analogs which were better than the Japanese machines themselves, as we learned after VJ-Day, when at last

we were able to pick up one of the Japanese Navy machines intact. We never did pick up one of the Japanese Foreign Office machines intact - we found a badly damaged one in the ruins of the Japanese Embassy in Berlin, in 1945.

Turning now to the agenda for the first technical session, LCDR Gleason is going to tell you immediately after lunch something about the way in which a complex problem was successfully handled in World War II. That problem also involved a cipher machine, one of German origin, used by all the German Armed Forces, and although we knew practically all the major details of its construction and method of operation, the problem nevertheless was one of great difficulty. Not wishing to intrude on Commander Gleason's preserve I won't say more about his presentation except to indicate that it is principally intended to provide general background as to crypt-analytic techniques in actual practice, as against purely theoretical approaches or methods.

Following his presentation there will be a tour at this station to take a look at several analytic or cryptanalytic machines, designed to meet general or specific specifications dictated by the nature of the crypt-analytic problems, to which the machines are addressed.

The technical session and tour this afternoon are intended to serve as immediate background for the specific problem we think you can assist in solving; and tomorrow morning we shall begin on the problem itself.

At the end of each presentation or tour there will be opportunity to ask questions. These we welcome and, in view of what Admiral Stone has said regarding the security bars having been let down so far as SCAG is concerned, I hope that the informality of our meetings will be conducive to your feeling utmost freedom to ask any questions you deem pertinent. We will answer them to the very best of our ability. There is, however, one point in this connection that I must mention. Admiral Stone has indicated why we have found it essential to apply a rather strict compartmentation upon the activities, operations, and results obtained in certain areas of AFSA's work. It will be perfectly permissible to ask questions when we are assembled in a conference room; but when we are making the tours of actual installations it will be necessary that you reserve your questions until we reassemble in a conference room, because, strange as it may appear, many of the people who actually operate some of our machines

TOP SECRET

do not know the details of the problem in connection with which the machines are being employed.

Tomorrow afternoon there will be further presentations directly involving the specific problem. At that time will be a good opportunity to make a tour of machines at our other cryptanalytic center, the one at Arlington Hall Station, across the Potomac. After that tour, there will be a discussion period on one subject, and then SCAG will be divided into two sub-groups, one consisting of those who are especially interested in the mathematical aspects of the problem, the other, of those who are especially interested in the electronic components of the analytic machines which we think may help us reach the solution to the problem.

The final session will be at Arlington Hall Station and will be devoted to discussing, in a preliminary way, the paths along which, having learned of our various approaches, you think our research might be directed. We feel sure that you will be able, if not at this time then after you have thought the matter over, to make valuable suggestions toward the solution of our most pressing problem. Its urgency is one that claims all our best efforts.

TOP SECRET