OFFICE OF THE CHIEF SIGNAL OFFICER

FROM: ~~TOP SECRET~~

SPSIS-3

TO BE HAND-CARRIED

NO: REF ID:A4148540

IS-3-03503

FILE DESIGNATION:

Draft Memo dd 15 Mar 45

Security of Our High-Grade Cryptographic Systems

TO:	TO:	TO:	TO:	TO:	TO:
IS-3	IB-2	IB-3			
DATE:	DATE:	DATE:	DATE:	DATE:	DATE:
14 Mar 45	15 Mar 45				

ACTION: DIVISIONAL FILE COPY

DRAFT 1945.

MEMORANDUM for Colonel Corderman.

Subject: Security of our high-grade cryptographic systems.

1. This question has recently been asked of SSA technical personnel by General Stoner, General Clarke, and you: "Why are you so confident that the Germans and/or the Japanese are not reading our high-grade machine cipher traffic, and how can you be as positive in your belief as you appear to be?" A statement on this subject in substantiation of oral remarks, was promised some time ago and is embodied in this paper. The statement is not made lightly, for the matter has been thought about for several years and its importance is realized. No shadow of doubt can be left in the case of the answer to such a question as this, involving as it does the success of our military operations and the lives of many thousands of men.

2. Evidence in a matter such as this can be classified into three types: (1) direct or positive evidence, (2) indirect or negative evidence, and (3) inferential evidence.

3. Direct evidence that the Germans have <u>not</u> been reading the high-grade traffic can be disposed of very quickly--there is, so far as we are aware, no direct evidence of any value. It is true that there have recently been isolated statements by German prisoners of war to the effect that no success had been attained by German cryptanalysts in their efforts to solve "the big machine"; also a similar statement from a Polish source (referred to us by the British) has recently come to hand. However, such statements are of no value because the trustworthiness of their authors cannot be guaranteed, they were probably not in a position to <u>know</u>, and their evidence may be considered pure hearsay. So much for direct evidence--little enough, it is granted.

4. a. In the realm of indirect or negative evidence it may be noted that many authentic German documents have been captured. These have been scanned very thoroughly. Not a shred of evidence has ever been found in them to indicate that the Germans have solved any of our machine traffic, except that of Converter M-209. And the data we have in respect to what they have or can do in respect to the M-209 indicates that they know only how to solve cases in which messages are similarly keyed and how to recover the complete key in such cases, thus making it possible to read all messages for the day in that key. There are other methods of solution known to and practiced by us, but we do not know whether the Germans know these methods.

b. Not a shred of evidence has ever been seen in any solved German messages that would indicate German ability to solve high-grade cipher machine traffic, whether it be Typex (British), Sigaba, or CCM traffic. We have been challenged with these questions: "But what if the Germans have an inflexible rule that Ultra will never be passed by any signal communication agency susceptible to interception by the enemy? What if they must use only wire circuits? This they can do because all their provinces are contiguous and they have excellent internal communications. The fact that no Ultra is seen in what we are reading would prove absolutely nothing, would it not?" These questions are not difficult to answer.

c. Let us consider the indirect evidence based upon Ultra intelligence derived from reading German E and Fish traffic. Several million high-echelon German secret messages have been read in the past few years. In them has been found information on every conceivable subject. German confidence in the security of their cryptographic systems appears so great that no restrictions have apparently been imposed on the type of

information that may be passed in E and Fish traffic. Strategic as well as tactical plans of the greatest importance to their own operations--more important than even Ultra intelligence would be--are freely discussed. Messages to and from Hitler himself are not infrequent. "Y-service" reports, i.e., signal intelligence of the type we designate as Ultra, pass freely; in fact, one E key (Mustard) is exclusively devoted to "Y-service" traffic. Reports of cryptanalytic success on M-209 and other traffic have been found on numerous occasions. It is difficult to imagine, in the light of this evidence, that there is one subject and only one which may not be mentioned in E or Fish messages. And if such a rule existed, it is hard to believe that the Germans would draw a line of demarcation between the M-209 and what we consider high-grade machines. Incidentally, it may be observed that it is only very recently that evidence has appeared indicating that the Germans may have a suspicion that their E and Fish traffic is being read: In at least one case a prohibition was placed upon any communication regarding a forthcoming operation. (But this was accompanied by a requirement that all persons let in on the secret take a special secrecy oath!)

d. As for their being able to pass Ultra over internal wire circuits because their provinces are all contiguous, it need only be pointed out that when in 1942 the Germans were operating in North Africa they did pass Ultra from Berlin to Rommel--Ultra that came out of the "Cairo Episode", involving U. S. Military Attache and U. S. Military Mission messages read by the German cryptographers by means of a compromised code and cipher table applicable thereto. Also, the "Y-service" reports referred to above deal largely with Ultra coming from Russian messages. These reports certainly could be sent over wire circuits only--but they pass, as a matter of fact, over radio circuits. It is clear, therefore, that the forwarding of Ultra by radio is not prohibited by the Germans.

e. The Germans have passed certain Ultra to the Japanese, who have forwarded it to Tokyo. The practice of passing this Ultra to the Japanese and of allowing the Japanese to forward

it by radio is evidently satisfactory to the Germans. In all that Ultra, not a shred of material in the past has come or comes now from any of our high-grade machines. If there were such material there can be little doubt that some evidence of it would be found in these Tokyo-Berlin communications.

5. The following indirect or negative evidence is offered for what it is worth--others may be in a better position to add to or subtract from it: Although it is possible that the Germans may have obtained bits of tactically useful information now and then from the solution (or compromise) of such things as M-209 keys, or low-grade tactical codes, voice codes, and the like, we know of no case in which the Germans have given any indication in their own large-scale operations or in their reaction to our large-scale operations that they knew anything about our plans and that the source of their information was cryptanalytic in nature. Indeed, the evidence is the other way around, as witness the strategic surprise obtained in the landings on North Africa, on the continent, etc. Furthermore, in the world-wide peregrinations of our highest ranking military and diplomatic officers, including the President, there has never been a hint that the details of the journeys have been known in advance and it is certain that these details involved a great many communications. So much for indirect or negative evidence.

6. a. We come now to what, in the circumstances, must be considered as the strongest and most reliable evidence--that which is inferential in character and is based upon German cryptography itself. We know so much about their cryptographic practices that we can deduce and assess their cryptographic theories and thus determine the stage of development they have reached not only in cryptography but also in cryptanalytics. The overwhelming evidence is that they are far behind us and have no appreciation of solution techniques which we now regard as commonplace. We can see from their security precautions just what they are trying to guard against and can thereby reconstruct their cryptanalytic theories. A recent change in

the method of selecting E indicators (designed to prevent the possibility of cillies) shows a very belated appreciation of the dangers inherent in the old system. The "CY" procedure indicates that they are blissfully unaware of the cryptanalytic techniques that have proved most successful in reading E traffic. In the case of Fish, the introduction of the auto-key feature shows that they may have appreciated that machine settings could be entirely reconstructed from messages in the same key. The introduction of daily-changing wheel patterns in the summer of 1944 indicates that they may have finally realized the possibility of statistical solution despite their careful efforts to make the generated key completely random. But at the same time, it shows that they have no conception of the possibility of rapid statistical solution with the aid of high-speed machinery because they continue to send transmissions thousands of groups long without changing settings. Numerous other illustrations could be cited--the foregoing are merely isolated bits of evidence.

b. Although we have frequently heard of German use of IBM equipment in cryptanalysis, there is no evidence whatever that they possess any high-speed machinery of the type that would be essential to attempt solution of some of our machine ciphers.

7. If the Germans were reading our high-grade traffic they would inevitably realize that we are reading theirs. They would know this both from the content of the messages (because we pass Ultra by radio) and from the techniques which they themselves would have to employ. In such event, even though they were unable to adopt improved cryptographic systems and procedures, they would certainly impose drastic restrictions on the topics permitted to be discussed in radio messages. As has been pointed out in par. 4, no such restrictions have been imposed by them.

8. a. Another question has been posed: "The Germans have been constantly improving their cryptographic methods and related procedures. Recently they eliminated discriminants, they are enciphering call signs, changing frequencies, and so on, making the task of allied cryptanalysts extremely more difficult. Why have the Germans been acting in this manner? Isn't it possible that they have learned things from their solution of our high-grade machines and are striking at the weaknesses in their cryptography which are the weaknesses that enable them to solve our high-grade traffic?"

b. It is granted that continuous improvement in cryptographic methods and related procedures implies continuous study in cryptographic security, including monitoring and cryptanalysis of your own communications. But the recent improvements introduced by the Germans have, with two exceptions, had no really serious effect upon the cryptographic weaknesses inherent in their own machines and their methods of using them, weaknesses which are exploited by the British and ourselves. Elimination of discriminants, encipherment of call signs, rapid changes in frequencies, and the like have not closed the door to E-solution; they have merely made it harder to intercept and to segregate the traffic desired. The two exceptions referred to above have to do with E-machine modifications called "Enigma Uhr" and "Uncle D". As regards the "Enigma Uhr", this causes difficulty in some cases; had the Germans introduced this modification in the manner in which they are now using it, the British would possibly still be struggling with it. As regards the "Uncle D", this involves the use of a variable reflector on the E machine, a feature which they began introducing last year and which has not yet been completely distributed. It is very doubtful if the Germans realize the adverse effect that the use of the variable reflector has exercised on cryptanalysis, otherwise they would not use it as they now do, in a more or less hit and miss fashion--some circuits using both the fixed

and the variable reflector on the same day, when messages which used the variable reflector have to be forwarded to units not provided with this feature.

c. It may be legitimate to infer that the major changes referred to in paragraph a above were introduced as a direct result of what the Germans were getting out of traffic analysis and cryptanalysis of low-grade systems of the Allied forces--Pearl and Thumb intelligence, in other words. And when one considers how much useful intelligence they can get out of our traffic because we do not make much of an attempt to hide or disguise call signs, change frequencies, and so on, one need not be at all astonished to find the Germans introducing these improvements--because they undoubtedly assume that if they can get so much out of our traffic, surely we can get an equal amount out of their traffic. So they proceed to plug up these sources of leakage, remaining supremely confident that the E and their Fish machines are invulnerable to cryptanalysis.

9. Another source of inferential evidence is this: If the Germans were cryptanalytically competent they would not tell some of their most important secrets to the Japanese, for the latter promptly forward them to Tokyo in the Purple machine, to our great advantage. Either the Japanese have given the Germans the details of the purple machine, in which case the Germans are satisfied as to its security and feel they are taking no chances in talking as they do to Oshima; or, if they do not know these details, surely they must have tried to solve it, failed in the attempt, and then concluded that we could not solve it. Otherwise, it would be absurd to think that the Germans would tell their most important secrets to the Japanese. (The number of times the Germans have told the Japanese something, with strictest injunctions as to the importance of keeping the matter secret, is astonishing!) If the Germans cannot solve the Purple, after

all the traffic that was passed in it, traffic the contents of which must often have been known to them, they are not good enough to solve our high-grade machines, which are cryptographically far superior to the Purple machine. To carry this argument a bit further, one could get a pretty good estimate of the cryptanalytic competency of the Germans by studying the communications out of Berlin from neutral representatives, for in some cases they pass communications (which we read) quite harmful to German interests, which they would certainly stop if they could read them--or else they would see to it that these representatives are not in a position to know certain things. Do we or the British allow such leakage of information to continue? The answer is obvious.

10. a. Of the ineptitude of the Japanese military people in cryptographic and cryptanalytic work little need be said. They are not so far along as the Germans. Their cryptography is unwieldy and very difficult for them to manage, as is abundantly clear from the texts of many messages solved by us. They have been getting good results from traffic analysis, because of our failure to take proper counter-measures until quite recently. They have also been getting some information from the study of very low-grade Allied systems--and that is all. They apparently are unable to conceive of refined methods and application of machine methods to solving their cryptographic systems which they regard as complex and secure. Their notions of cryptographic security, a definite reflection of cryptanalytic knowledge, are puerile and practically non-existent. Any difficult Allied systems which may have been read by them were undoubtedly read as a result of physical compromise; this has given them food for serious thought and has resulted in their adoption of many measures relative to physical security. Their most recent changes, enciphered disciminants, etc., which have really increased their cryptographic security were introduced to gain greater traffic analytic security with no apparent conception of their cryptanalytic consequences. Apparently absolutely convinced of the impossibility of cryptanalytic solution

of their encoded and enciphered communications, they repeatedly commit that most flagrant and most appalling violation of cryptographic security, viz., sending new keys by radio in old keys. Having adopted a basically strong cryptographic system--if properly used--they have as a consequence of cryptanalytic immaturity so abused the system as to reduce its security in many cases to almost the zero point. When bad luck pursues them, they consistently attribute palpable evidence of leakage of information to the operations of enemy agents, or carelessness on the part of their cryptographic personnel!

b. Japanese Foreign Office cryptography and cryptanalysis are a bit better than this. That office has been using a fairly good cipher machine for some years and a few fairly high-grade enciphered code systems, all of which are being read by us, with possibly one or two minor exceptions. We have clear evidence from our own Ultra that they are able to solve certain Chinese and French systems, but these are of medium or low-grade nature. Much of what the Japanese have been able to do in cryptanalysis has been the fruit of collaboration with the Finns and the Germans. It is doubtful whether they could have attained much success by their own efforts.

11. To summarize: At the risk of sounding boastful, it will be stated that the Japanese are not as good as the Germans, and the latter are not as good as we are in cryptography and especially in cryptanalysis. If either of these governments were reading our high-grade traffic they would inevitably realize that we are reading theirs--and they would change something in a very radical manner, not in piecemeal fashion. They would either set up rigid restrictions on what could be transmitted by radio by their present systems, or they would adopt systems we could not read. They have done neither of these things and the conclusion must therefore be clear: <u>They cannot read and are not reading our high-grade cipher traffic.</u>

12. In the enclosure there are given some calculations of a speculative nature thought to be of interest in this connection.

1 Enclosure.

ENCLOSURE

1. The following question has been asked: "Well, maybe you cryptanalysts are right in what you say and we have full confidence in you as cryptanalysts, but this may, in the final analysis, be a matter of accuracy of judgment. Men have been known to make serious errors in judgment before this, and the matter we are considering is extremely important. Just suppose you cryptanalysts are wrong and that the Germans not only do have rapid analytical machinery such as we have at their disposal but also understand how to apply them to cipher machines of the CCM type. How long would it take them to solve a message and recover the keylist, after they have captured a machine and have the whole set of rotors but do not have the new keylist?"

2. Let us assume the Germans have "bombes" of the rotating wheel type, the fastest of which (Navy machines) can make a complete run applicable to a 3-wheel E machine (17,576 steps) in about 50 seconds, and a 4-wheel E-machine (456,976 steps) in 22 minutes. (The working rate of speed of rotation is approximately 350 steps per second.) At this rate, a full run of a 5-wheel machine (11,881,376 steps) would require 33,947 seconds, or 565.8 minutes, or 9.43 hours. Call it 9½ hours, to be on the conservative side. That is, for one wheel order (or particular permutation of rotors) it would take one machine 9½ hours to make a full run. The CCM has 10 rotors, 5 of which can be put into the machine at one time, and these can be inserted either right side up or upside down. There are therefore 20 x 18 x 16 x 14 x 12 or 967,680 possible wheel-orders available for selection--and therefore for trial by cryptanalysts who want to solve a message. It takes 9½ hours to make one run and there are 967,680 of these runs to be made, if you are so unlucky as to find the correct combination only by going along to the very last run. On the average, the correct one will be found say at the half-way mark or on the 483,840th run. Of

course, if there were 483,840 bombes available, you would not have to stop after each run to change your wheels to make up a new wheel order, but obviously it is absurd to imagine the Germans having anything like that number of bombes. Let us assume they have 1000 bombes--a great many. (Time must be allowed for changing from one wheel order to the next, but suppose this can be done merely by pressing a button, so that only a second or two need be allowed. This amount of time can be disregarded, so that the 9¼ hours still stand as the time to make a run.) The total number of bombe-hours required is 483,840 x 9.25 or 4,475,520 hours. There are 1000 bombes, hence the work can be divided among them, giving approximately 4475 hours. If the bombes are worked 24 hours a day, day in and day out, this would take 186 days or approximately 6 months. Six months to solve one message and recover the rotor combination for that one day--because the next day's traffic presents a similar problem.

3. The fastest bombe conceivable is one that would be electronic in nature and the fastest of electronic cryptanalytic machines known to us is the "Colossus", which operates at approximately 4000 steps per second, but it would <u>not</u> be applied to this problem. The SSA has consulted the best electronics engineering staff in the world (Bell Laboratories) who could not see their way clear to devising an electronic bombe to duplicate the workings of an E machine, a 3-wheel affair only. What the problem would be with a 5-wheel machine can be imagined. But let us assume the Germans <u>are</u> supermen, have been able to build such bombes, and that they have 100 of them (each one involving tens of thousands of vacuum tubes). Each bombe is operating at 4000 steps per second. This is 11.4 times as fast as the type of bombe assumed above; hence, if they had 1000 electronic bombes, we can take the 186 days and divide by 11.4, giving 16.3 days, but with a complement of only 100 electronic bombes, it would take 10 times 16.3 or 163 days before a single message could be solved,

or a little over 5 months--provided a perfect crib were available and could be "set" perfectly to the cipher text. But the CCM does not allow this so easily; it is not like the E machine, where a letter cannot be represented by itself in the cipher text. Hence, in trying to fit a crib to the cipher text in the case of the CCM there can never be <u>any certainty</u>, and dozens, hundreds, maybe thousands of attempts would have to be tried--each one taking 5 months. Thus, the matter reduces itself to an impracticability, something altogether beyond our capacity to do, and therefore, in the light of the discussion in the basic paper, beyond the capacity of the Germans or the Japanese.

4. The cryptographic principle upon which the Sigaba is based is far superior to that of the CCM. Our own studies indicate that even if high-speed cryptanalytic machinery were employed we know of no method of solution that does not require possession of at least 17,000 consecutive letters of correctly matched plain and cipher text before the attack can even be initiated. If the Germans or Japanese cannot solve the CCM, they certainly cannot solve the Sigaba.

5. "Why then do we have to change rotors in the CCM or in the Sigaba? The Germans have never changed rotors in the military E-machine; why should we, if you are so certain that they cannot solve CCM or Sigaba messages?" The answer is: Only to take care of the contingency which would arise if the Germans or Japanese should obtain a key list and rotor wirings, by capture or other compromise, for then they are in a position to read the traffic sent in the compromised key list and rotors, thus destroying the security of messages which may involve operations either in progress or set for some future date.