SPECIAL CONFERENCE ON M-209 SECURITY

Attached are minutes of a meeting held 12 October 1950
at 1400 hours at the Naval Security Station, Building 19,
Room 230, to discuss general aspects of the security of the
American cipher machine M-209, and German cryptanalytic work
on traffic enciphered by this machine during World War II.

SPECIAL CONFERENCE ON M-209 SECURITY

Minutes of meeting held 12 October 1950 at 1400 hours at the Naval Security Station, Building 19, Room 230. At the invitation of Mr. William F. Friedman, Technical Consultant to the Director, AFSA, those present were:

> Mr. T. R. W. Burton Miller
> British representative
>
> Mr. Kenneth L. Perrin
> British representative
>
> Dr. Abraham Sinkov, AFSA-04T
>
> Mr. Frank Austin, AFSA-41
>
> Dr. k. W. Pettengill, AFSA-14 ·
>
> Captain Mary C. Lane, AFSA-14
> (Recorder)

Opening Remarks by Mr. Friedman: Mr. Friedman opened the meeting by stating that the purpose of the gathering was to discuss in general the security of the American cipher machine M-209, and in particular the amount of M-209 traffic solved by the Germans during World War II and the amount of intelligence they obtained therefrom. Mr. Friedman said that the question had arisen during a recent discussion in which the British representative, Mr. Miller, had referred to the "vast amount of intelligence which had been obtained by the Germans from the reading of traffic encrypted with the American cipher machine M-209", a statement the validity of which Mr. Friedman had questioned and which he had asked Mr. Miller to discuss with him. Mr. Miller had in turn asked Mr. Perrin to gather information on the matter from TICOM sources. American representatives from AFSA-04 and AFSA-14 had been invited by Mr. Friedman to join in the discussion. Mr. Friedman added that, although the question was largely academic, the M-209 being non-operational, he believed nevertheless that the discussion would prove of interest and benefit to the participants.

Remarks by Mr. Miller: Mr. Miller remarked that the discussion might well have a certain amount of operational value, since he understood that at the present time the M-209 machine was being used for communications by the U.S. Army in Korea. With the participation of British forces in Korea, the question had arisen of a common cryptographic system to be employed by combat units. Whereas the British are using Typex and would be prepared to use the CCM at Brigade level, the M-209 is at present the only system available to U.S. forces at the equivalent U.S. level. Unless the U.S. Army were prepared to put the CCM further forward, therefore, it appeared that there might be a possibility of having to use the M-209 as a combined system. A discussion of its security was thus a matter of considerable interest to both parties at the present time. This statement was corroborated by Mr. Austin. Mr. Miller then introduced Mr. Perrin, who had prepared remarks on the solution of M-209 traffic as noted in TICOM sources.

Remarks by Mr. Perrin: Mr. Perrin explained that he had divided his statement into four parts:

A. How much M-209 traffic was read by the Germans;

B. How much time was consumed in the reading of the traffic;

C. How was the traffic read; and,

D. What were the intelligence results of the reading of the traffic.

2

A. **How much M-209 traffic was read by the Germans:**

Statement by Mr. Perrin: Various figures were given by the Germans who were interrogated concerning the amount of M-209 traffic which was read. Mr. Perrin affirmed his belief, however, that these discrepancies reflected actual differences and that the reports, while varying, were true, since apparently the amount of traffic solved differed according to the originating service. Thus, for instance, almost no U.S. Naval M-209 traffic was read: firstly, because there was little traffic, and secondly, because there was a relatively strict cipher discipline in that service. On the other hand, most of the sources stated that from 6 - 10% of U.S. Army M-209 traffic was read. One analyst of the German Army Cryptologic Agency, Rudolf Hentze, had boasted that 30% of M-209 traffic was read. Mr. Perrin admitted that Hentze was possibly an unreliable source. A German Army officer, Lt. Schubert, had stated that M-209 traffic was read for about 20 days a month. Although this might imply that two-thirds of the total traffic was read, Mr. Perrin stated that the figure presumably related to solution of occasional keys running concurrently during the month rather than to the total amount of daily traffic enciphered, and did not therefore imply that two-thirds of the total traffic had been read. Somewhat greater success was claimed by the senior cryptanalyst of the German Air Force, Voegele, who said that from 6 - 8 days of M-209 traffic on the Western Front was read each month by his unit, and some 1 - 2 days traffic in the Mediterranean area.

Remarks by Mr. Austin: Mr. Austin pointed out that the solution of traffic for 20 days a month, provided that Schubert's figure referred, as Mr. Perrin suggested, to the solution of occasional keys, did not represent a large percentage of the total amount of M-209 traffic passed, since at sometimes during the war as many as 75 different keys were being used simultaneously, each division and corps being provided with its own set of keys, as were the numerous Military Police battalions and units of the Army Air Force.

Mr. Austin then stated that U.S.A. monitoring of the M-209 traffic of an American Armored Division in England prior to D-Day had resulted in the reading _cryptanalytically_ of 29 days' traffic a month. Although corrective measures had been taken before the invasion, the heavy casualties among U.S. communications personnel after the invasion had made necessary the use of untrained Army personnel as cryptographic clerks, with a consequent decline in cipher discipline. Overall estimates by American experts on the amount of M-209 traffic probably read by the Germans during the war was set at 10%, including physical compromises, of which several cases were known. An estimate of 6% is accepted for the reading of M-209 traffic by purely cryptanalytic means.

Reply of Mr. Perrin: Mr. Perrin agreed in substance with Mr. Austin's remarks but set the reading of M-209 traffic at 10% _without_ including that resulting from physical compromise, believing that the figure with physical compromise included would be somewhat higher.

B. **How much time was consumed in the reading of the traffic:**

Statement by Mr. Perrin: Mr. Perrin stated that, although there was no information from TICOM sources about the amount of time required for the reading of messages in depth, it was presumed that this would take some two or three hours. There was, however, general agreement in TICOM reports as to the time consumed in breaking _relative settings_: this was usually set at two or three hours (two hours were given by Luzius, three by Hentze, two to three by Barthel, all German Army cryptanalysts). Estimates on the amount of time required to obtain the _absolute setting_ varied: 12 hours was given by Hentze (Army), 1-2 days by Barthel (Army), 22 hours by Voegele (Air Force),

72 hours by Schultze (Navy). Mr. Perrin suggested that 24 hours might be taken as an average "if one were lucky". Thus, a total of approximately 28 hours would be needed after the messages were received by the section charged with solution of the traffic, and it was generally admitted by the German cryptanalysts that the M-209 traffic was received several days after interception (according to Voegele 7-8 days).

Remarks by others: Mr. Friedman remarked that, since conditions were usually unfavorable, a time lag of two or three weeks between interception and the obtaining of the absolute settings for the M-209 traffic would not be improbable. Mr. Austin voiced the opinion that the obtaining of the absolute setting would require at least 18 hours, or more often up to four days, after the messages were broken in depth. In support of this view Mr. Austin noted that the absolute setting had been obtained by U.S. cryptanalysts in 18 hours under the most favorable circumstances; Mr. Austin also cited the German Army cryptanalyst, Graupe, who gave an estimate of 5 - 7 days as the time necessary for obtaining the absolute setting. Captain Lane remarked that the German source quoted by Mr. Austin was perhaps less reliable than those quoted by Mr. Perrin, a remark with which Mr. Perrin agreed.

General Agreement: It was generally agreed that the German crypt-analysts were hampered by two factors of decisive importance in their solution of M-209 messages. One was the lack of any cryptanalytic mechanical device for facilitating or expediting the solution, thus forcing all work to be done by hand; the other was the time lag between interception and receipt of messages by the cryptanalytic units in Berlin. In reply to a query from Mr. Friedman whether solution generally took place at the front or in the central units, Mr. Perrin said that frontal solution of the M-209 was apparently confined to the reading of messages in depth, the determining of absolute settings being accomplished at the central units.

C. How was the traffic read:

Remarks by Mr. Perrin: Mr. Perrin stated that the German cryptanalysts never developed a general method of solution, although there is a description of a theoretical solution of the M-209, given a text of 3000-5000 letters. For practical solution of the traffic German cryptanalysts depended either on depth or on operators' errors.

Corroboration by Mr. Austin and Dr. Pettengill: Mr. Austin and Dr. Pettengill corroborated this statement of Mr. Perrin and agreed that the theoretical solution of the M-209 had been of no practical value. Dr. Pettengill added that the Germans had apparently developed a mechanical method of solution, but the principles of this method were obscure, and there was no conclusive evidence that it had actually been employed.

D. What were the intelligence results of the reading of the traffic:

Remarks by Mr. Perrin: Mr. Perrin remarked that, because of the time lag between the interception of messages and their receipt by the cryptanalysts, the tactical intelligence gained from the reading of M-209 traffic by purely cryptanalytic means was negligible. Nevertheless, there was an appreciable amount of strategic intelligence which was gained from the reading of the M-209 traffic, such as the effect of the German V-1 bomb, the building of new airfields, and Allied order of battle. Mr. Perrin pointed out that, had the Germans been able to organize their own intercept and relay services more efficiently, the solution of M-209 messages would have been of tactical value. As it was, he admitted that the value was mainly strategic.

4

Remarks by Others: Mr. Friedman hereupon interposed a question as to the readibility of systems used by the British in comparable echelons. Mr. Perrin stated that the British equivalent system, the Stencil Subtractor (SS) Frame, was never read by the Germans except for one month when the basic book had been captured. Dr. Sinkov remarked that the British cipher had two disadvantages from the American point of view. One was the cumbrous nature of the system; the other was the fact that American operators are not trained in sending or copying digits, and thus find a system like the SS Frame difficult to use.

Mr. Miller added that the Stencil Subtractor Frame had also been less used than the American M-209, since the British cipher machine Typex was used at a lower echelon than the comparable American device, and thus Typex relieved the Stencil Subtractor Frame of some 400 - 500 messages daily. Mr. Austin corroborated Mr. Miller's remarks and stated that the U.S. Army was so organized that the bulk of regimental and combat level traffic was necessarily encrypted with the M-209.

Concluding Remarks by Mr. Friedman and Mr. Miller:

Re-statement of Matter at Issue: Following a brief summary of the discussion by Mr. Friedman, Mr. Miller stated that the matter at issue concerned the remark he had made that "a vast amount of intelligence had been obtained from the German reading of the American M-209 machine", and it was now a question of whether in the light of the discussion he should withdraw his statement in whole or in part or whether he would defend it.

Mr. Miller considered that he should withdraw the word "vast" and asked that the following statement be substituted:

"Disregarding information obtained from the use of captured M-209 key lists, it is generally agreed that a considerable amount of American M-209 traffic was broken by the Germans during World War II, from which little tactical intelligence was deduced, but from which an appreciable amount of strategic intelligence was obtained. It is further agreed that, due to the inefficiency of the German intercept organization, the lack of modern cryptanalytic machinery, and the failure of the Germans at high levels to appreciate the value of speedy intercept, forwarding, and processing of traffic, the German success did not represent the maximum potential exploitation."

General agreement: The above statement was agreed upon by all present as representing a fair and reasoned resolution of the matter at issue.

Potential Usefulness of the Discussion: It was agreed that a record of the discussion should be made, and that such a record might be useful for:

(a) Future British-American discussions as to the use of the CCM at a combined Army echelon lower than that at which it is presently used;

(b) Background as to the possible solution by potential enemy agencies of systems such as the M-209 and comparable British systems;

(c) A source of reference for discussions pertaining to the proposed improved Hagelin device and its possible solution by cryptanalytic means;

(d) A record of interest in itself which should be added to the pertinent operational and historical records of the participating Agencies.

Approved: _____

T. R. W. Burton Miller

Approved: _____

William F. Friedman