MINUTES OF ARMY-NAVY MEETING
16 FEBRUARY 1948

TOP SECRET

12 March 1948

A conference of Army and Navy representatives on the subject of CCM modification was held in Room 117 Hq., Arlington Hall Station at 1400 on 16 February 1948. The following were present:

ARMY

| | |
|---|---|
| Mr. William F. Friedman | - AS-14 |
| Mr. Mark Rhoads | - AS-14 |
| Major J. G. Moak | - AS-23 |
| Dr. S. Kullback | - AS-70 |
| Mr. Leo Rosen | - AS-70 |
| Mr. H. C. Barlow | - AS-74 |
| Dr. A. Sinkov | - AS-80 |
| Mr. H. L. Clark | - AS-80 |
| Mr. F. C. Austin | - AS-83 |
| Mr. K. Kuhn | - AS-85 |

NAVY

| | |
|---|---|
| Captain M. R. Gerin | - Op-20-Y |
| Captain L. F. Safford | - Op-20-D |
| Comdr. A. M. Patterson | - Op-20-R |
| Captain L. W. Parke | - State |
| Comdr. D. W. Seiler | - NCSL |
| Lt. Comdr. J. C. Hargreaves | - Op-20-Y |
| Mr. R. H. Shaw | - Op-20-K |
| Mr. L. D. Whitelock | - BuShips |

The chairman opened the meeting by indicating that its purpose was to discuss two papers: (1) the British document entitled "Services Cypher Policy Committee Paper No. 3," of 29 October 1947, and (2) the letter dated 30 January 1948 from the Chief of Naval Communications to the Chief, Army Security Agency, subject: "Comments on Army Proposals Regarding the CCM."

Taking up the first document, the chairman referred at once to Par. 11 thereof and opened the meeting for discussion of the British "conclusions." In the absence of technical data concerning the nature of the British Typex Mark 22, referred to in Pars. 5 and 11(a) of the British document, it was agreed that a satisfactory assessment of the degree of security aimed at by the

TOP SECRET

British was impossible and that the chairman would seek further information from the British Liaison Officer in Washington as to the Mark 22.

As regards Par. 11(b), Capt. Safford wished to defer discussion thereof for a few minutes.

All present agreed on the validity of the British conclusion stated in Par. 11(c).

Capt. Safford asked that consideration of Par. 11(d) also be deferred for a few minutes.

As for Par. 11(e), the chairman stated that obviously that conclusion was not a new idea--it motivated the Combined discussions early in 1947.

The Navy representatives then introduced into the discussion certain ideas, both old and new, concerning possible CCM modifications. Among the former was the idea, originally put forth in 1942 and soon abandoned, of modifying the Typex machine itself to convert from mechanical to electrical control of rotor stepping. Authority to reopen this line of investigation had been obtained and Comdr. Seiler, who thereupon produced drawings, some of which were dated as early as 1942, stated that he was planning to have one modified Typex completed in July or August 1948. It was also stated by Comdr. Seiler that all required changes to Typex, such as an encipher-decipher switch, provision for the new stepping action, and reversed motion of two rotors could be incorporated in the adapter unit. The chairman raised the question as to whether the British would be willing to spend a considerable sum of money in modifying their Typex, in view of their reiterated statements that they were opposed to major changes in the present Typex and wanted a new machine. Capt. Safford stated that he had reason to believe that the British attitude on this point has changed recently and that they might be amenable to considering such a change as was now envisaged by Navy. The chairman thought it might be advisable to consult with the British before doing much work on this line, but Capt. Safford indicated a preference for completing one model so as to be in a position to convince the British, by means of the model, of the feasibility of the proposal.

It was also pointed out by ASA representatives that if the Navy's new idea for rotatable and interchangeable cam rings were adopted, serious changes in the Army's SIGROD machines would have to be made, and there is doubt whether such changes could be made. The same applies also to the SIGIVI components.

Some discussion of the proposal to incorporate reversed motion of rotors into the modified Typex led to a general review of the reasons for the Navy having embarked on the CSP-2900 program. It

was pointed out by the chairman that one of the principal reasons was a desire on the part of Navy to have a machine embodying some principle or principles not known to the British and reversed stepping of rotors was one of these principles; if now that principle were incorporated in the CCM, one of the prime motives for the CSP-2900 program was eliminated.

The Navy representatives pointed out, however, that the principle of reversed stepping had already been incorporated by the British into RM 26 and RM 32, and was therefore not unknown to them. Furthermore, since reversed stepping is only one of several improvements incorporated into CSP-2900 its disclosure, by itself, would not permit reconstruction of the machine. In any case, the Navy was already committed to the CSP-2900 and the change would cost a relatively small amount, $10 or $15 per machine, if done now. They had built special jigs and tools to facilitate the change, and they were going ahead with the making of the CSP-2900. Comdr. Seiler indicated that it takes 36-man hours to recondition one machine and only 2½ additional hours of labor and $10 worth of parts are needed for the CSP-2900 changes.

At this point, the chairman speaking for the Army representatives stated that he regretted to have to say that the ASA position with regard to CSP-2900 remains unchanged.

The Navy representatives then displayed two samples of the embodiment of a brand new idea for variable and interchangeable cam contours, an idea of very recent origin. This consisted of a split ring of tool steel which could be mounted on one rim of the standard rotor, the ring fitting into a narrow groove cut into the rim. The outside periphery of the ring is contoured for camming purposes and the ring, once mounted, could be fixed into position by a spring clip. It was pointed out that the new rings, while mounted only on one side of a rotor, did not interfere with inserting a rotor in the reverse position, since the roller riding the cam contour of the ring could be elongated so as to make the cams effective whether the ring was on the right or left rim of the rotor. The Army representatives stated their opinion that since rings were to be installed on one side of the rotor only, the potentialities of variable and interchangeable cam contours were therefore reduced. The Navy did not concur in this opinion.

The chairman requested the Navy representatives to provide ASA with some of these new rings and grooved rotors, together with a modified SIGIVI, so that studies could be made at ASA as to the feasibility of the new idea. It was agreed that the reply to the British document would be held up until these studies have been completed.

The chairman proposed next to discuss Admiral Stone's letter and read over pertinent parts thereof, adding comments. He

indicated his fears that the Army and Navy might be drifting apart in their respective programs to a point where after about five years the Army and the Air Force would have several new and radically different machines, but would not be able to intercommunicate with Navy. Army and Air Force requirements were such that they could only be met by making new, smaller, more compact, and more secure machines; minor modifications of existing machines would not meet the requirements and moreover the Army directive on research and development discouraged work having as its end product merely minor improvements. The Army position as regards the CSP-2900, for example, was in line with the directive; the proposed modifications of SIGABA/ECM to make CSP-2900 represent only minor improvements of insufficient value to justify the expense, which Army felt would be nearer $100 per machine than the $10 or $15 Navy estimated. Also, the proposed incorporation of reversed stepping into the CCM negates one of the original reasons for the CSP-2900. The argument that the British could not incorporate reversed stepping into their own machines had no application here, since a knowledge of reversed stepping would be useful in a cryptanalytic attack on U. S. traffic, and mechanisms to take care of reversed stepping could be incorporated in British cryptanalytic machines, if they were really desirous of attacking U. S. traffic. The chairman, as spokesman for Army, regretted that he could only reiterate that ASA could not accept CSP-2900 in principle and would not undertake the conversion of SIGABA's in connection with its own rehabilitation program, as urged by Navy.

Referring to Par. 2 of Admiral Stone's letter, the chairman requested further details concerning Navy's Cryptographic Research Program. Capt. Safford indicated that this is a 5-year plan and does not involve any new or radical developments; the principal points in the plan are those set forth in the letter; the Navy will be glad to examine any new Army equipment for ground use (Marines) whenever such equipment became available; Navy with limited funds, could at this time only go in for modifications of existing equipment and hoped that Army would accept Navy results along those lines.

The problem of more frequent changes of CCM rotors was then discussed. The chairman indicated ASA's hopes that Navy would complete its development of automatic rotor wiring, which would greatly simplify the problem. Comdr. Seiler then displayed one of the new bobbins and a rotor embodying this new feature, stating that Navy has tested a set of these new rotors under 1,500,000 steppings and found they worked well. The Navy expects to have two of their automatic winding machines operating by August 1948. The chairman expressed ASA gratification with this progress and looked forward to being able to get some of these new machines. The chairman also said that ASA agrees with the Navy that twice-daily changes of key list would be confusing, and therefore not desirable.

Referring to Par. 4(a) of Admiral Stone's letter, the chairman asked whether Navy apprehensions as to CCM security were really warranted. Capt. Safford replied that Navy was contemplating being ready for any emergency requiring greater security, say by 1953. In response to the chairman, who pointed out that all the studies of CCM showed that only highly specialized solutions were possible now and that these special cases arose very infrequently, Capt. Safford stated that Navy feels that modifications should be made to eliminate all possibility of these special solutions just to be on the safe side. Capt. Safford further stated that numerous restrictions on CCM operation, such as limited message length, had created the impression throughout the service that the Navy Department mistrusted the security of the CCM, and this mistrust was prevalent throughout the Pacific Fleet.

As for Par. 4(b) of Admiral Stone's letter, the chairman stated that ASA will be very glad to explore the possibilities of the Navy's new proposals for CCM modification and will look forward to receipt of a model.

The chairman passed over Par. 4(c) with the statement that the Navy position was well understood and needed no further discussion, although ASA did not share the same point of view.

As for Par. 4(d) the ASA agrees with Navy. As for Par. 4(e) the Army shares the Navy view on the inadvisability of adopting new equipment before fully tested and pointed out in this connection that this applies, so far as ASA is concerned, also to CSP-2900. He felt that the practicability of reversed stepping had not been adequately tested out and, moreover, the cryptographic security of the principle had not been thoroughly tested out by long continued studies; it is really not known what weaknesses are introduced by reversed stepping, which may cure one weakness but bring in another. However, the Navy representatives stated that they felt their tests adequate and that it was inadvisable to await completion of studies which might take 15 years; such delays are unwarranted and would constitute a block to the introduction of any new machine.

Referring to Par. 5 of Admiral Stone's letter, the chairman felt he could only repeat what was stated before; much to his regret no change in the ASA position could be indicated.

Referring to Par. 6, the chairman stated the Army shares the Navy point of view. Summarizing the discussion, he stated that the ASA will await a model of the new modification of the CCM proposed by Navy and in the meantime he would try to obtain further information regarding the British Typex Mark 22, reporting thereon at the next meeting.

William F. Friedman

WILLIAM F. FRIEDMAN
Chairman

TOP SECRET