Box 74

~~TOP SECRET~~

TOP SECRET

21 January 1949

From: R. I. Meader, Captain USNR

To: J. N. Wenger, Captain USN

Subj: 14 Days Training Duty, Report of

1. Attached is a report covering my assignment during my training duty period 7 January to 21 January 1949.

2. May I express my appreciation for the complete and cordial cooperation I received while carrying out my assignment.

R. I. Meader
Captain, USNR

ATT.

~~TOP SECRET~~

[redacted]

FOR OFFICIAL USE ONLY

PART I

of Report to Captain J. N. Wenger, USN

At the beginning of World War II, the personnel assigned to Naval Communications Intelligence were faced with the tremendous problem of acquiring from scratch the highly complicated analytical equipments required to cope with the then existing sophisticated systems of enemy encipherments. Except for certain IBM equipments, only one major device was in process of design at the time of Pearl Harbor. This was a project originated through the Bureau of Ships under an NDRC Contract with M.I.T. Early in January 1942, a survey of the then known urgent requirements of CNO was made. The Bureau of Ships immediately started action to acquire equipments by placing contracts with Eastman-Kodak Company, IBM, Gray Manufacturing Company, and the National Cash Register Company in the established methods of the Bureau.

It soon became apparent that the peculiar needs of NCI were such that due to continually changing requirements and to the necessity of instituting extraordinary security measures, special treatment had to be devised if equipments were to be obtained in time to be useful in the active prosecution of the war, and if security were to be maintained.

The following examples are given to illustrate the difficulties of applying standard procedures of procurement for the specialired equipment required by Communications Intelligence:

1. Japanese Speech Privacy

It was known before Pearl Harbor that the Japanese used a particular type of speech privacy system for overseas circuits. This speech privacy system was comparatively simple and offered no difficulty in theoretical breaking. The matter of equipment development to exploit the theoretical method of breaking was handled through the National Defense Research

[redacted]

taking over. Conditions under which this work is accomplished must be as attractive to the contractor as any other wartime endeavor in order to get the complete utilization and cooperation of the contractor and his facilities.

2. The mixture of Naval personnel with civilian personnel continued to be a bone of contention with the management of the contractor. The contractor objected to having personnel in his plant over whom he did not have complete control. It should be borne in mind that the civilians employed under this contract by the contractor, who were subject to draft under selective service, were deferred solely at the request of the Navy and solely for the purposes of working under this overall project. This applied even to the head of the department processing this contract. This situation became critical when certain civilians refused to work overtime even when such overtime was deemed absolutely essential to the successful prosecution of the war. However, nothing actually was done except to handle each case individually and to continually pacify the civilians as much as possible. Some method should be devised, however, to overcome a repetition of this condition. Certain alternate suggestions will appear later in this report.

When the need for training naval personnel at the plant of the contractor was recognized, CNO requested Secretary of Navy to establish the activity known as the United States Naval Computing Machine Laboratory at Dayton, Ohio. On December 9, 1942, an officer attached to the Bureau of Ships was ordered to Dayton, Ohio, for additional duty as Officer in Charge of this new activity. This was the same officer who had been administering for the Bureau of Ships the Navy contract with the National Cash Register Company.

At this point all the facts leading up to the establishment of NCML should be reviewed and re-emphasized. This, of course, covers the basic functions it

was intended to have this activity perform. Up until this time, the administration of the research and development contract between the Navy Department and the National Cash Register Company had proceeded along established lines under the direction of a representative of the Chief of the Bureau of Ships who also acted as the representative of the I.N.M. This contract administration continued as before. However, the National Cash Register Company requested the representative of the Chief of the BuShips to provide an armed guard 24 hours per day as a security measure. The company also requested the Bureau representative to take over in large measure the growing procurement problem. Because of these requests of the National Cash Register Company, in addition to the problems of handling the personnel sent to Dayton for training purposes, the Ship's Crew at the USNCML grew to a point where at the peak of operations there were attached:

Officers - Officer in Charge
Executive Officer
1 Medical Officer
2 Navy Nurses
4 Officers assigned to procurement
1 Officer - Cost Accountant

Enlisted Personnel - 17 Marines
4 Pharm. Mates
4 Hosp. Corps.
8 Yeomen

Except for the members of the Medical Department and the executive officer, the above "Ship's Crew" would have been absolutely essential in the administration of the National Cash Register Company contract even though no naval personnel had been sent from CNO for training or other duty. However, in June 1943 there were some 65 officers and 500 enlisted personnel stationed at the USNCML for training purposes. To reiterate the fundamental purpose in asking the Secretary of Navy to establish the activity at Dayton was to provide the proper authority for the complete military administration of naval personnel sent on temporary additional duty orders for training duty. It had nothing to do whatever with the administration of the National Cash Register Company contract. However,

because of the existence of this activity in Dayton, those officers assigned to procurement and to expedite purchases of materials, the officer assigned for accounting duties and the Marine Guard were attached to the NCML.

During the summer of 1945 the Chief of Naval Communications, Admiral J. R. Redman, made one of his periodic inspections of the activity at Dayton. At that time he requested the Officer in Charge to start planning a peacetime equivalent of the combination of the National Cash Register Company and the USNCML. As a result of this request, the present ERA, Inc., was organized and located at St. Paul, Minnesota. Engineering Research Associates, Inc., took the place of the National Cash Register Company and the USNCML was transferred from Dayton to St. Paul.

PART II OF REPORT TO J. N. WENGER, CAPT. USN

RESUME OF THE DAYTON, OHIO
ACTIVITY DURING WORLD WAR II

Early in 1941, Op-20-G began work on German Naval Cipher, and a cooperative effort was attempted with GC & CS. Complete cooperation was not achieved, and in April 1942, Col. John Tiltman of GC & CS sent a dispatch to Commander Travis stating in part

> "Unless a rapid and satisfactory solution is found, the high command will insist on their Naval Cryptanalysts attempting to duplicate our work on 'E'".

The reply from Commander Travis contained a statement that the 4-wheel submarine traffic was, for the time being at least, unreadable. This failure to receive anything assuring from the British and the urgency of the situation led to the establishment on 1 July 1942 of a development contract (#NKs 7892) with the National Cash Register Company, Dayton, Ohio for the investigation of a high speed cipher machine of the Enigma type.

During July 1942 and early August 1942, the NCR Co. Engineers indicated that proposed electronic equipment (necessary to the solution of the 4-wheel traffic) would use vast quantities of critical material and that the successful maintenance of such electronic equipment was highly doubtful. Therefor, an electro-mechanical approach was substituted and on 15 Sept. 1942 an outline of a design plan was submitted to Op-20-G by the NCR Co. This plan was approved on 23 September 1942. The scope of Contract NKs 7892 was enlarged and actual development work started. The design of the Bombe eventually required material and components from some 12,000 different suppliers. Certain components had to be designed and developed, and production equipment obtained and put in operation. Among these were the

4 section diode, the 2C4 miniature gas tube, and a commutator capable of taking 104 inserts and designed to rotate at 1850 R.P.M. while in contact with 104 carbon brushes. Personnel in the Electrical Research Department of the NCR Co. had to be increased from 17 in August 1942 to 800 in May 1943, a period of 8 months. Furthermore, segregated areas had to be arranged for in order to maintain the high degree of security required. Facilities for messing and housing, etc. WAVE officer and enlisted personnel was arranged for at the "Sugar Camp" of the NCR Co. A folder is attached showing in part these facilities and a report submitted by the S. O. P. to the Commandant of the 9th NAVAL DISTRICT.

This Bombe program was carried on under Contract NKs 7892. This contract was dated 1 July 1942 and terminated 1 December 1943. The entire Bombe technique was developed there including components which heretofore did not exist. Two experimental Bombes were put into operation at Dayton just seven months after the Military Characteristics had been approved. These were followed by a production of 99 Bombes under this same contract, all of which were delivered and in operation during 1943. In addition to the regular Bombes, two double Bombes were designed, built, and put into operation and 35 M-9 machines with their associated wheels were produced. A total of $4,599,685.32 was expended under this contract. In as much as 103 Bombe units were constructed, this represented a total unit cost (including development) of approximately $45,000. each. However, included in this cost was $281,076.80 worth of Navy owned capital equipment, all costs of maintenance parts, design changes, etc. up until December 1943.

Contract NKs 7892 was followed in December 1943 by Contract NKs 49702 which ran from 1 December 1943 to 1 July 1945. The total expenditures under this contract were $2,466,671.67. For this amount, NCR Co. designed, developed, fabricated, and put into operation the following equipments.

Copperheads I	5 Scanners 6 Punches
Vipers	10
Mike	1
Pythons	6
Rattler	3
Gypsy-Topas	2
Duenna	5
Statistical Bombe	1
Double Bombe	1
Asp	1
Sliding Grenade	2
M-9	60 (506 extra wheels)
M-8	8
Parallel Grenade	1
Mamba	1
Wave Filters	30
Boa	60
Special Boa's for Duenna	10
Satyr	1
Pluggable Reflectors	495

Standard Grenades	4
Drag Grenade	1
Coast Guard Grenade	1
Cilli Grenade	1
Inverted Bombes	8
Bombes modified for double input	25
Special Cryptographic model for DNC	2
Squelcher Circuit	

In addition to the above, development work on Copperhead IV & V, Mona, Recording Devices, Special Chassis #7 for Bombes, Electronic Roto, Electric Hagelin in process, General Purpose Comparator in process, Slide Grenade for Jap Enigma in process, Geheimschreiber in process, and Subtractor Ciphers--studies in process, was accomplished.

The magnitude of the above equipments is a matter of record and need not be amplified here, other than to give one example. One Duenna contained 2,000 relays and 3,000 tubes. In the overall performance at Dayton, over 200,000 items were shipped to Washington from Dayton. Some 56 carloads weighing 17 tons each were sent.

The speed and efficiency with which these projects were processed is indicated in a letter of 30 January 1945 from DNC to OinC, USNCML stating in part

> "The skillful and expeditious handling of a special project for the Asst DNC, Op-20-G, during the month of December 1944 is an outstanding example of magnificent accomplishment and

a most important contribution to the war effort".

And the endorsement forwarded by the Chief of the Bureau of Ships stating in part

> "The Chief of the Bureau of Ships notes with complete satisfaction the continued accomplishments of the personnel and the management of the U. S. Naval Computing Machine Laboratory in providing highly specialized equipment to the DNC in record time".

A continuation of the Research and Development work at Dayton was covered by a third Contract, #NKs 9581 dated 1 July 1945 and terminated 15 August 1946. Under this contract, a total of $369,024.54 was expended. For this amount, the NCR Co. developed and produced

6 Special Counter Printer Punches

1 Full Selector

2 Amber Projectors

12 Morse Printers, and continued development on the Electric Hagelin and General Purpose Comparator.

Simultaneously with the processing of the above, two contracts were carried on for "Replacement Parts, Services in Repairing, Altering, Overhauling and Maintaining equipments designed and constructed" under the Research and Development contracts.

Contract NKs 46045 - 1 Dec. 43 to 30 June 45 -		$455,140.63
NKs 9580 - 1 July 45 to 31 Dec. 46 -		50,762.26
	Total	$505,902.89

Another contract was entered into providing for "Services of Procuring and Purchasing Material for Naval Personnel Projects". Contract NKs 9582 from 1 June 1946 to 31 December 1946 - $90,597.10. Work done by Naval personnel for which this contract was utilized included 15 Recorders, 10 Amplifiers, 10 Morse Printers, and certain phases of a Full Selector.

The NCR Co. also processed a fixed price contract calling for 50 Bombes. The contract was cut back after 29 Bombes had been delivered.

Contract NKs 53322 - 29 Bombes delivered @ $36,000.		$1,044,000.00
Cancellation charges		315,731.79
	Total	$1,359,731.79

Contract NKs 25120, a fixed price contract calling for 3 Counter Printer Units and 3 Relay Control Units, was also processed.

Contract NKs 25120 - 3 Counter Printer Units at $38,750 each	$116,250.00
3 Relay Control Units at $4,800 each	14,400.00
	$130,650.00

A recapitulation of these various contracts is made on the last page of this report.

The phenomenal record made at Dayton, Ohio may be challenged on the grounds that during war-time it was possible to work 24 hours a day and 7 days per week. While this is true, it must also be borne in mind that work being done by Engineers in Research and Development cannot be passed on shift to shift. Engineers must personally see their work thru to a conclusion and obviously no engineer could work 24 hours a day nor seven days a week. The advantage of the full time operation was really effective only in the production of parts and the assembly of components. It is felt

that the important factors which combined to make possible this war time record were:

1. All possible Bureau red tape was eliminated.
2. Direct liaison and mutual understanding between BNC (Op-20-G) and Dayton.
3. Overall administration of all work vested in one head.
4. Complete flexibility of the entire engineering force.
5. The efficiency of the maintenance and operating plan which was originated at Dayton.
6. Readily available facilities for production and assembly.

Council and a contract with the Bell Laboratories. Excellent theoretical results were obtained from Bell Laboratories. However, the equipment for exploiting this speech privacy system was delivered in 1945, long after the usage of the system had ceased. Therefore, although from a long-range point of view excellent basic work was carried out, from a practical point of view, the results obtained were zero.

2. Photographic Scanning Machines

In the fall of 1941 it was decided that as a result of lengthy discussions between the Army and Navy, optical scanning techniques provided an effective means for performing certain basic analytical processes. Contractual relations were arranged with the Eastman Kodak Company to develop two machines of this type - (a) the Tetrograph Detector, and (b) the Index of Coincidence machine. The protracted correspondence in order to establish the specifications of these proposed devices is a matter of record.

The first model of the Tetrograph Detector did not perform. It was necessary to return it to the contractor for revision and even on the second delivery it still did not perform. In order to get any results from the equipment, it was necessary for technical personnel assigned to the Naval Communications Annex to completely rebuild the device.

The Index of Coincidence machines achieved some success. However, their history was one of constant difficulties and continual changes by Annex personnel in order to achieve any significant results.

3. Radio Fingerprinting

Early in the war it was realized that methods short of analysis must be applied to get any information concerning submarine activities in the Atlantic. The art of radio fingerprinting had been pursued by

[redacted]

RECAPITULATION OF FUNDS EXPENDED
AT LAITON, OHIO

Contract	Date Began	Date Ended	Purpose	Navy Owned Equipment	Total Amount
7892	7-1-42	12-1-43	Research & Development	$281,076.80	$4,599,685.32
49702	12-1-43	7-1-45	Research & Development	9,177.60	2,466,671.67
9581	7-1-45	8-15-46	Research & Development		369,024.54
			Total	$290,254.40	$7,435,381.55
46045	12-1-43	6-30-45	Replacement Parts	$ 4,638.73	$ 455,140.63
9580	7-1-45	12-31-46	Replacement Parts		50,762.26
			Total	$ 4,638.73	$ 505,902.89
9582	6-1-46	12-31-46	Procuring & Purchasing Material for Naval Personnel Projects		$ 90,597.10
			Total		$ 90,597.10
25120			3 Counter Printer Units @$38,750.		$ 116,250.00
			3 Relay Control Units @ $4,800.		14,400.00
			Total		$ 130,650.00
53322	3-1-44	Cancelled	29 Bombe Units @ $36,000		$1,044,000.00
		10-1-44	Cancellation charges		315,731.79
			Total		$1,359,731.79

[redacted]

Naval Communications Annex personnel both at the Annex and at the Naval Research Laboratory. In order to supplement this activity and bring to bear the best talent, a contract was arranged with the Bell Laboratories and extensive researches were carried on at the Bell Laboratories and at Holmdel, New Jersey. These investigations extended over a period of about two years and the results obtained were extremely weak. The principal reason for the lack of results was undoubtedly the unfamiliarity of the Bell Laboratories personnel with the practical aspects of the problem.

There was also a definite inter-relationship between the various types of equipment needed. This fact had a great bearing on the decision to concentrate our efforts in one activity. In order to successfully develop machines in the quickest possible time, it would have been necessary to divulge to the engineers of the various contractors considerable highly classified information. Widespread knowledge of the purposes of these machines was an extremely dangerous procedure and in fact, it was not deemed feasible to permit this. By concentrating in one contractor, a very few persons needed the whole story. Complete control could be maintained. The project engineers could be given such information as was necessary to develop their projects so long as the top technical level administering and guiding all the projects had complete knowledge of the basic requirements. Had we continued to spread the work through several contractor organizations, many more people would have to be let in on the "inside" and our danger of compromise would have been very real.

In attempting to procure equipments of practical value quickly, there was a continuing problem of security. Relationships with the Eastman Kodak Company, the Electromatic Division of IBM, Gray Manufacturing, and others illustrate these difficulties.

The knowledge that equipment produced by the Eastman Kodak Company was not

meeting the requirements of performance was, of course, transmitted to the Eastman Kodak Company. The primary factor causing the lack of performance as indicated by the Eastman Kodak Company was the unfamiliarity of the Eastman personnel with the operational requirements. It was extremely difficult to furnish these personnel with sufficient operational requirements to make their equipment effective and yet not overstep the bounds of security.

The same situation occurred with the Electromatic Division of the IBM Corporation. In this case there were other complications. The high classification of the equipment made it very difficult for that company to carry out the work since they had no area segregation in their plant. In order to get the equipments completed, it was necessary to reduce the classification and make special arrangements so that the work carried out would in no way reveal the end use. These arrangements, of course, reduced the efficiency of performance of the contractor.

The relationships with the Gray Manufacturing Company showed strongly the necessity for having this type of equipment developed with sole responsibility on a single contractor. The Gray Manufacturing Company developed the comparator portion of the 70 mm. comparator equipment. The National Cash Register Corporation developed the printer counter unit. The tape punching equipment was developed at M.I.T. There were tremendous difficulties in integrating these three portions into a single system. Upon delivery of the first comparator unit, it was necessary for engineers from the Gray Manufacturing Company to work at the Naval Communications Annex in revising the equipment so that it would work with the printer counter unit. The punch developed at M.I.T had to be completely abandoned because the results did not perform in the scanning unit of the comparator. This experience can be paralleled by others which prove definitely that all components of a single system must be either developed by a single contractor or the complete responsibility placed on a single contractor for subassemblies of the complete system.

In addition to this, procurement of components and raw material presented a great problem. All branches of the armed services were competing with each other for the acquisition of essential material. In a great measure the same components and materials were common to all projects. Tubes, resistors, wire, switches, relays, chassis, cabinets, etc., were just a few. By organizing one central group to handle the procurement, priorities, expediting, etc., this service was performed for all projects; orders were combined and materials switched as the necessity arose from one project to another. In fact, this group would have had to be duplicated in certain measure for all projects had they been separated in various contractors' plants. It is useless to think that such an important function could have been taken over by regularly constituted agencies such as the various INM - Electronics Control Board, etc. These agencies had to serve many activities of the Navy - CI procurement was just one more added to their list. Even with one group organized for this purpose, it was found necessary to appeal to the CNO for aid. This resulted in Admiral Horne, of CNO, directing Rear Admiral Kelsher to step in, without disclosing the end use of the material, wherever our deliveries were unsatisfactory and to break bottlenecks by ordering other Naval procurement agencies to give way to this all-important business of CI.

A still further advantage was derived from the fact that the entire staff engaged in this work was very flexibly organized and large groups of personnel could be pulled off one project and concentrated on any other that had suddenly become imperative. The information necessary to accomplish the actual fabrication and assembly of equipments was, in many cases, of a Top Secret nature. This work could only be done by qualified Naval personnel for security reasons. By concentrating our efforts in one location, it was possible to assign Naval personnel to this work under ideal conditions. Security control, military control, morale and health conditions could be maintained at very high levels.

There is ample evidence to support these contentions. The fact that all during the war not one leak in security was traceable to this activity was evidence of our ability to maintain security. The morale and living conditions existing at Dayton, Ohio are shown by the report of Captain Allen which is attached. The speed with which tasks were accomplished is evidenced in the record of the activity at Dayton which is made a part of this report.

Experience gained during the first six months of the war indicated that the following fundamental essentials are absolutely required as a foundation upon which to build this type of a war time organization:

1. One contractor should be selected having competent and completely cleared development engineering personnel, large manufacturing and assembly capacities available for this work, and located within easy distance to the Central Naval Intelligence Group (Washington D. C.) for liaison.
2. The key personnel of the contractor must be willing to accept rapid and repeated changes in end specifications (forced on the CI group by enemy action).
3. Local conditions at the contractor's plant must lend themselves to complete security requirements.

After a careful study, it was decided that the National Cash Register Company fulfilled all of the above initial requirements. A "best efforts" development contract was entered into between the Bureau of Ships and the National Cash Register Company in the late spring of 1942. Steps were taken to immediately enlarge the engineering staff of the contractor. The development engineers went to work on the problems submitted to them by the CI group in Washington. While equipments were in the early design stages, it became more and more apparent that the end result would be equipments of a highly complicated nature unlike any other apparatus that had as yet been constructed. Even

in those early stages the problem of operation and maintenance of such gear loomed up as a major problem. A decision was made to institute a plan of sending Naval personnel into the plant of the contractor during the early assembly stages of the equipments and having these Naval personnel actually work under the direction of civilian engineers in assembling, testing, debugging and operating the equipments. When the equipments were ready to be delivered to CNO in Washington, these Naval personnel were transferred back with the gear to Washington to maintain and operate the equipments. In addition to the above, jobs such as the wiring of cross wired wheels could only be done by Naval personnel directly under the jurisdiction and control of authorized Naval officers.

The advantages which were gained by the foregoing procedure follow:

1. Complete control over a group of technically trained personnel to accomplish the needs of the CI organization.
2. Uninterrupted applied research and development along lines applicable to RAM equipment for CI use.
3. Complete control over security.
4. Responsibility for procurement of raw material and components necessary to RAM rested in one head.
5. Efficient training of maintenance and operating personnel, trained by actually assembling, testing, debugging and operating the equipment before the equipment was delivered to CNO.
6. The closest kind of liaison between the contractor and CNO's CI group, making possible the rapid and repeated changes necessary as information was obtained.
7. A minimum of delays due to red tape, etc., in a mission where time was of the very essence.
8. The use of Naval personnel in manufacturing procedures, knowledge of which in the hands of unauthorized persons could be disastrous to the

whole program.

In order to accomplish the above objectives, it was necessary to contract with a civilian organization having:

1. Competent engineering staff flexible enough to permit great expansion. Note that the National Cash Register Company's Electrical Engineering Department in July 1942 was composed of 17 individuals. This department was increased to some 1200 persons at the peak of operations.
2. Relatively large manufacturing facilities--the National Cash Register Company is in peace time one of the country's largest manufacturers of small parts. In addition, this company is located in Dayton, Ohio, where there are hundreds of small shops experienced in precision work and available for subcontracting.
3. A location within the contractor's plant for the processing of this work under adequate security conditions. A building isolated from the main buildings of the National Cash Register Company was devoted to this work and placed under a 24-hour Marine guard.
4. Proper housing and recreational facilities for Naval personnel. This was extremely important inasmuch as enlisted personnel were doing the same kind of work that civilians were doing but the civilians were receiving two and three times as much take-home pay. To compensate for this pay differential in some measure, living conditions and recreational facilities had to be the best possible. To this end the Naval personnel were housed in "Sugar Camp", an NCR facility at Dayton. Adequate housing (six Waves to a cottage containing two rooms, shower and toilet facilities) was available, as well as a large outdoor swimming pool, baseball diamond, dining hall, dance hall, auditorium wired for sound projection and a general lounge.
5. Proper medical care of the Naval personnel. A building located within

the confines of the National Cash Register Company's "Sugar Camp" was utilized as a sick bay, containing examining rooms, 10-bed hospital and laboratory spaces in addition to Medical Department administrative offices.

6. Proper housing facilities for the Marine Guard. This was accomplished in spaces within the building occupied for this work at the National Cash Register Company. It was found highly advantageous to have the guards housed on the premises where the work was done.

7. Location at Dayton, Ohio, was within 12 hours by rail and 3 hours by plane from Washington, D. C., making the necessarily close liaison extremely easy.

There were certain factors, however, that gave rise to considerable difficulty and if possible should be avoided in any future mobilization of this wartime effort. The outstanding causes of trouble were:

1. The contract written with the NCR was of the "no profit" type. While this was done at the request of the contractor in the spring of 1942, it was definitely the wrong thing to do. The contractors, as their lucrative fixed price war contracts increased, were very reluctant to use their personnel and facilities for no profit at the expense of increasing their profitable work. We reached a stage where 93% of all our specially designed parts were let out to subcontractors. Many of these contractors were incapable of executing precision work and their equipment was such that delays which were intolerable resulted. This became so serious that a meeting was held at the Navy Department in Washington, at which the management of the NCR Company was directed to be present. It was necessary to direct the contractor to prosecute whenever possible the work in his own plant under threat of the Navy exercising its wartime perogative of

(G-50 10/7/44 RS#42937)

31B
A6-3(8)
8 OCT 1944

~~TOP SECRET ULTRA~~

Op-20-G-md
(SC)A6-2(8)

SECRET
HVCCO

~~TOP SECRET ULTRA~~

From: OP-20-G-1.
To: OP-20.

Via: OP-20-G.

Subj: Review of Activities and Future Plans at the U.S. Naval Computing Machine Laboratory, Dayton, Ohio.

Ref: (a) Comdr. Wenger's memo to DNC, dated 30 May 1944, under cover memo dated 31 May 1944.
(b) VCNO's memo for Chief Naval Personnel dated 11 November 1942.
(c) Comdr. Wenger's memo to OP-20, dated 10 May 1944.

1. The U. S. Naval Computing Machine Laboratory, Dayton, Ohio, was set up by a request of the Vice Chief of Naval Operations dated 11 November 1942, reference (b).

2. The primary function of this Laboratory was the design and construction of the Bombe equipment necessary for the solution of German cipher systems. The outstanding points in the history of the Bombe project are contained in reference (a). The purpose of the present memorandum is to formulate the present status of plans for the activity.

3. The major projects carried out by the Laboratory at Dayton were the original Bombe development which included the production of ninety-six (96) units and the contract for fifty (50) additional units which was initiated at the request of the British in March 1944. The latter contract was cancelled, after twenty-five (25) units had been produced, at the direction of the Director of Naval Communications with the concurrence of the British.

4. Because of the introduction by the Germans of a pluggable reflector in the Enigma machines used on certain German Air Force circuits, a project for the construction of a special machine, called the DUENNA, for the solution of this system was placed at the Laboratory. The present status of the DUENNA project is as follows: one unit has been completely assembled and is undergoing operational tests.

[redacted]

Op-20-G-md
(SC)A6-2(B)

Subj: Review of Activities and Future Plans at the U.S. Naval Computing Machine Laboratory, Dayton, Ohio.

- -

machine. It is proposed to build an electric Hagelin which can operate on punched tape for rapid cryptanalytical analysis and exploitation of Hagelin material.

d. GENERAL PURPOSE COMPARATOR.

The experience with general purpose cryptanalytical machines developed under contracts with Eastman Kodak Company, Gray Manufacturing Company, and the I.B.M. Corporation, has been studied carefully. Although the present equipment has proved invaluable in the analysis and solution of certain cipher problems, some problems have shown the necessity for a machine of more general nature. It has been attempted to incorporate in a single unit many of the important processing methods which present equipment has failed to accomplish.

e. SLIDE GRENADE FOR JAPANESE ENIGMA.

The captured model of the Japanese Enigma machine indicates that multi-notch wheels will be used. Present Grenade equipment must be modified to handle the problem on a production basis. It is planned to equip up to four (4) Bombes with the necessary attachments.

13. There are many cryptanalytical problems requiring further machine and development research, as follows:

a. STATISTICAL BOMBE.

Present Bombe equipment requires a crib. Theoretical studies have been made which indicate that it is definitely possible to construct equipment which will do all that a Bombe does but which will need no crib, the statistics of the language serving instead. Japanese practice of varied start positions in their messages makes placement of cribs difficult and the need for a statistical approach stronger. In any diplomatic usage of the machine the crib situation will probably be poor.

b. GEHEIMSCHREIBER.

This is a German cipher machine based on the

SECRET
Hicco

[redacted]

Op-20-G-md
(SC)A6-2(8)

Subj: Review of Activities and Future Plans at the U.S. Naval Computing Machine Laboratory, Dayton, Ohio.

- -

five (5) units of Baudot code. The British have constructed special machinery for the solution of this problem but their efforts have not been successful on the later models of the device. From various sources it has been inferred that the Germans were contemplating the Naval use of this device. As modern communication methods tend toward radio teletype, it is felt that encipherments similar to the GEHEIMSCHREIBER are of increasing importance and efforts should be made to standardize the solution.

c. SUBTRACTOR CIPHERS.

Rapid changes in Japanese cipher systems make a present appreciation of the situation difficult. Whatever direction these changes take, special equipment will probably be necessary. Theoretical studies are continuing in order to be in a position to take immediate action as soon as the Japanese policy becomes clear.

14. Reference (c) requested authority to pursue developments along electronic lines and was approved by the Director of Naval Communications. The fundamental points in the above discussion, upon which approval is assumed in accordance with reference (c), are as follows:

a. Maintenance of the present Naval staff at the U.S. Naval Computing Machine Laboratory, Dayton, Ohio, as outlined in paragraph 11 above.

b. Specific projects enumerated in paragraph 12 above.

Specific problems for future projects as outlined in paragraph 13 will be submitted when present theoretical studies are completed if the situation appears to demand action.

J. N. Wenger
Commander, U.S. Navy

SECRET Hicco

SECRET
Hucco

[redacted]

TOP SE[redacted]LTRA

SECRET

Op-20-G-md
(SC)A6-2(8)

Subj: Review of Activities and Future Plans at the U.S. Naval Computing Machine Laboratory, Dayton, Ohio.

- -

The second unit is in assembly. Materials for five (5) units are at hand and certain critical items for a total of ten (10) units are on order. The distribution of this pluggable reflector by the Germans has not been as wide as was expected. Unless the European situation changes rapidly, two DUENNA's should be sufficient.

5. The primary function of the Bombe equipment is the determination of the plugging and wheel setting at which an assumed crib will produce a given cipher text. The DUENNA function is similar with the additional factor of determining the required reflector plugging. The fundamental cryptanalytical principles, of which the Bombe is an electro-mechanical representation, were used by the British for three-wheel Enigma machines, and were discovered independently by American cryptanalysts. The cryptanalytical principle behind DUENNA was the subject of research by American cryptanalysts beginning about June 1943, and had been successfully established before the Germans introduced the pluggable reflector. Although the fundamental principles involved in both Bombes and DUENNAS have been firmly established, varied usage by the Germans has necessitated intricate modifications on certain units in order to handle special problems quite different from straight cribbing of special messages. These modifications have been carried out partially at the Dayton Laboratory and partially by the maintenance force at the Naval Communications Annex. A fundamental distinction between American and British equipment is in the number of Enigmas contained ina Bombe unit. British machines contain thirty-six (36) Enigmas while the American machines contain sixteen (16). The decision to restrict American Bombes to sixteen (16) units was based on calculations which established that a sixteen (16) letter crib was sufficient to determine the unknown factors in the problem and hence the use of more than sixteen (16) Enigmas was wasteful of equipment under normal circumstances. The sixteen (16) unit Bombe proved extremely effective for a large percentage of German cipher problems.

6. Several German cipher systems which were intercepted by our own stations had never been solved by the British,

SECRET
Hucco

SECRET
HUCCO

[redacted]

~~TOP SECRET ULTRA~~

Op-20-G-2md
(SC)A6-2(8)

Subj: Review of Activities and Future Plans at the U.S. Naval Computing Machine Laboratory, Dayton, Ohio.

- -

notably the SEAHORSE traffic which is a Naval Attache circuit between Berlin and Tokyo and the SUNFISH traffic which is used by German units including blockade runners operating in transit or in the Far East. Cryptanalytical work leading to the initial break of both these systems was done by Op-20-G personnel. The solution of these systems is not one of cribbing but depends upon the knowledge that a message setting has been enciphered twice in the message. This problem of double encipherment can be handled by Bombe techniques but two Enigmas are necessary where one (1) suffices for a normal crib. Thus, these indicator or "throw-on" problems could not be handled on our sixteen (16) unit equipment. The initial runs on this traffic were made by the British at our request. However, British emphasis on European problems left them little time for this traffic, and hence it was decided to combine two (2) of our Bombes into a double unit. This was done in spite of British coolness to the proposal. The Laboratory was also instructed to combine two (2) of the additional fifty (50) Bombes into a second double unit. This course of action appears to have been justified because our one (1) machine, since going into operation seven (7) months ago, has broken out all the SEAHORSE traffic read seventy-two (72) days) since then, and thirty-three (33) of the forty (40) days of SUNFISH read since then. At the present we are reading SUNFISH traffic solidly, but at the expense of SEAHORSE which was being read several weeks ago.

7. In addition to the double unit modification, many special attachments for making Bombes more generally applicable have been carried out. Most important of these are the following:

a. STANDARD GRENADE.

Grenades are attachments to Bombes which determine the setting when the plugging has been recovered. A four-letter crib is sufficient for this purpose. Four (4) units are in operation.

SECRET
HUCCO

SECRET
Hicc

[redacted]

[redacted]

Op-20-G-md
(3C)A6-2(8)

Subj: Review of Activities and Future Plans at the U.S. Naval Computing Machine Laboratory, Dayton, Ohio.

- -

b. SLIDE GRENADE.

This device cuts the Grenade running time for Enigmas with rotatable reflectors by a factor of 26. They are of great interest at the present time because the recently captured Japanese Enigma has a rotatable reflector. Two (2) of the Slide Grenades have been completed.

c. DRAG GRENADE.

This Grenade applies a short crib to thirteen (13) positions simultaneously. It proves particularly useful when no crib is available, because such trigrams as "EIN" and "SCH" usually occur somewhere in a message. One (1) Drag Grenade is available.

d. PARALLEL GRENADE.

The Parallel Grenade provides four (4) standard Grenades which can be run simultaneously on a Bombe and thus uses the Bombe to full efficiency. This is of particular interest because the recently captured Japanese Enigma machine has five (5) notches on each wheel and therefore will be best handled by the Parallel Grenade. One (1) Parallel Grenade is available.

e. COAST GUARD GRENADE.

A special Grenade constructed for the solution of double encipherment problems occurring on certain clandestine circuits. This unit is near completion.

f. CELLI GRENADE.

This is a special Grenade which makes possible simultaneous running of several wheel orders.

SECRET
Hicc

SECRET
HVCO

[redacted]

[redacted]

Op-20-G-md
(SC)A6-2(6)

Subj: Review of Activities and Future Plans at the U.S. Naval Computing Machine Laboratory, Dayton, Ohio.

- -

g. SELF-DETECTION CIRCUIT.

This circuit was designed to eliminate certain extraneous stops called "boxing" stops occurring on indicator problems. Four Bombes and the double unit have been equipped with this modification.

h. SQUELCHER CIRCUIT.

This is a special circuit to eliminate stops which enables weaker cribs to be handled. This has proved particularly effective on certain paired day recoveries of submarine traffic.

i. INVERTED MACHINES.

It is found necessary to convert the wiring on certain Bombes in order to take advantage of turnover positions. These have been particularly useful for paired days on submarine traffic in which there is an unknown stecker but the wheel order and rings are known. Eight (8) machines are available.

j. PLUGGABLE REFLECTORS.

The reflector wiring on the Bombes is contained in a double-ended Jones plug. This arrangement permits change of reflector wiring but not rapid enough to cope with the probable German use of the pluggable reflector. To make rapid reflector changes possible, all Bombes are being provided with pluggable reflectors.

k. DOUBLE INPUT.

This modification was introduced on twenty-five (25) Bombes in order to be able to run certain weaker cribs.

8. In addition to the Bombe equipment, hand machines for secondary testing and breaking out Enigma traffic have been built. The following are some of the more important items:

SECRET
HVCO

SECRET
Hvcco

[redacted]

Op-20-3-md
(SC)A6-2(8)

Subj: Review of Activities and Future Plans at the U.S. Naval Computing Machine Laboratory, Dayton, Ohio.

- -

a. M-9.

A hand machine for testing results obtained from the Bombs. Approximately sixty (60) are on hand.

b. M-8.

Modified ECM's to carry out the Enigma decipherment from punched tape. Eight (8) machines are on hand.

c. BOA

A pluggable reflector for use in the M-9 machines. All M-9 machines have been so equipped and ten (10) special units have been supplied for use with DOLLERA.

9. Although the primary activities at the Laboratory at Dayton have been directed to the development of equipment for the solution of the Enigma machine, several projects have been placed at Dayton for machines aiding the solution of subtractor ciphers and other systems used by the Japanese. These projects are outlined as follows:

a. COPPERHEAD I.

COPPERHEAD I is an electronic tape passing device which lines up subtractor text in depth on the basis of double-repeat occurrences. This double-repeat search when carried out by IBM equipment is extremely laborious. The COPPERHEAD equipment will do a complete search on the two weeks' volume of JN-25 traffic in about twenty-four (24) hours. These machines are now practically complete; delivery is expected within two weeks.

b. MAMBA.

MAMBA is a device for lining up cipher messages with respect to recovered portions of the additive book, a process which is now running by hand. MAMBA will do the same job with a great saving of time and personnel. Delivery of this equipment is promised within six (6) weeks.

SECRET
Hvcco

SECRET
HVCCO

[redacted]

TOP [redacted]

Op-20-G-md
(SC)A6-2(8)

Subj: Review of Activities and Future Plans at the U.S. Naval Computing Machine Laboratory, Dayton, Ohio.

- -

c. RATTLER

The RATTLER is a device which determines the settings of Japanese 157 cipher machine on the basis of a four (4) Kana crib. Modifications of the RATTLER which are now in operation are being made so that it may be applicable to the Japanese Naval Attache machine. The extended use of the 157 cipher machine appeared imminent in July when three (3) additional RATTLER units were ordered. There has been no evidence to date of the expected wider usage so that the RATTLER program is currently being reviewed.

d. VIPER.

VIPER is a representation of the Japanese 157 machine and is used in the decipherment of traffic after the keys have been recovered. Seven (7) of these units have been completed; two (2) have been shipped to Honolulu and two (2) to Melbourne.

e. PYTHON.

These machines are representations of the Japanese Naval Attache machine. Six (6) have been completed; five (5) are in operation at Naval Communications Annex and one (1) is on loan to the Army.

f. COPPERHEAD V.

COPPERHEAD V is an electronic unit designed for extremely rapid differencing of cipher test. It was conceived as a fundamental machine in the breaking of subtractor ciphers. This machine has not progressed beyond the design and experimental stage.

10. In addition to analytical machines for use on the German and Japanese cryptographic systems, various projects for equipment of a general nature have also been carried on at Dayton. Among these are the following:

HVCCO

SECRET
Hvrco

[redacted]

[redacted]

Op-20-G-md
[SC]A6-2(8)

Subj: Review of Activities and Future Plans at the U.S. Naval Computing Machine Laboratory, Dayton, Ohio.

- -

a. MIKE.

MIKE is a rapid digraph counter which takes its data from two (2) teletype tapes which run synchronously. It has proved extremely useful in the solution of the Hagelin ciphers.

b. RELAY CONTROLS AND COUNTING UNIT FOR THE GENERAL PURPOSE COMPARATOR.

These relay controls and counter units have been completed. Two (2) of these units are in operation at Naval Communications Annex, and the Army has been supplied with two (2) units.

c. GENERAL CRYPTOGRAPHIC WORK.

A special cryptographic project assigned by the Director of Naval Communications has been carried on at Dayton. Pilot models are now complete on this project.

d. ELECTRONIC ROTOR.

Approval has been granted for research on the problem of performing the functions of a commutator by purely electronic means using special tubes. Considerable thought has been spent in this direction but the research still remains in a fundamental state.

11. Curtailment of the contract for the additional Bombes has been accomplished. Cancellation of this contract resulted in the release of approximately two hundred (200) civilians and twenty-five (25) Waves from the Laboratory. These Waves have been returned to Washington. In estimating requirements after C-Day, the only feasible plan seems to be to maintain the Laboratory at its present level because of current projects assigned to it, either in connection with streamlining the Bombe equipment or developments in Japanese and general cryptanalytical fields. Present Naval staff at the Laboratory is as follows: two (2) Wave officers and fifty-two (52) enlisted Waves. The general personnel assigned to the Laboratory by ComNINE are as follows: 1 Ensign (Nurse), 1 Lt. (med. Corps), 2 Lts. and 1 Lt.(j.g.)

SECRET
Hvrco

SECRET
Hvcc

[redacted]A
Op-20-G-md
(3C)A6-2(8)

Subj: Review of Activities and Future Plans at the U.S. Naval Computing Machine Laboratory, Dayton, Ohio.

- -

Male officers, 2 Lt. (j.g.) Waves, 4 enlisted Waves (3 PhM, 1 Yeoman), 22 enlisted men. Should the load at Dayton increase or decrease, personnel may be sent to or from Washington on a temporary duty basis. It is true that the Laboratory facilities at Dayton may not be available in the post-war period. The only solution of the problem of keeping up-to-date with scientific developments and their applications to cryptanalytical problems is in maintaining a staff at the Naval Communications Annex who will develop projects to a point where they may be placed with private laboratories.

12. The following projects are planned for immediate assignment to the Laboratory at Dayton:

a. TWO ADDITIONAL DOUBLE UNITS.

Materials are available from the cancelled contract for the assembly of two (2) such units within two (2) months. As pointed out above, these double units have been particularly effective in connection with German U-Boats operating in the Far East. Recent KNOWledge of a German U-Boat operating in Australian waters came to light only through this equipment. Certain secret forms of the Berlin-Tokyo Naval Attache circuit can only be solved on this equipment.

b. PROVISION OF ADEQUATE MAINTENANCE STOCKS TO KEEP PRESENT BOMBE EQUIPMENT IN OPERATION FOR A PERIOD OF FIVE YEARS.

The provision of these maintenance stocks is felt justified by the threatened Japanese use of the Enigma as well as the use of the Enigma machine by other nations. New usage of the Enigma machine will probably necessitate certain modifications of the present equipment; materials and staff for these attachments should be available at the Naval Communications Annex.

c. ELECTRIC HAGELIN.

Present decipherment of Hagelin traffic in volume is extremely laborious using the general-issue Hagelin

SECRET
Hvcc