

Report On
E Operations of the GC & CS
At
Bletchley Park
By
William F. Friedman

Copyright Colin MacKinnon 2016

COLINMACKINNON.COM

DECLASSIFIED

Authority NND 963016

By wp NARA Date 6/6/03

SECRET

TD-1218

SECRET

REPORT ON
E OPERATIONS OF THE GC & CS
AT
BLETCHLEY PARK

Signal Security Agency
Arlington Hall Station
Washington

(This report consists of 116 pages)

SECRET

DECLASSIFIED

SECRET

Authority NND 963016By Wp NARA Date 6/6/03

TABLE OF CONTENTS

	Page
I. Introduction.....	1
II. Preliminary Talk with Mr. Welchman.....	2
III. The Control Party.....	10
A. General.....	10
B. Traffic Research.....	11
C. Intercept Control.....	17
IV. The "Central Party".....	23
A. General.....	23
B. Indices and Records Section.....	24
C. Log Reading Section.....	24
D. The "Fusion Room".....	32
V. Cryptanalytic Research.....	35
VI. The Cryptanalytic Operational Watch.....	41
VII. Operations Under Mr. Fletcher.....	50
A. General.....	50
B. Watch Registration.....	50
a. The Flow of Traffic and the Identification Party.....	50
b. Watch Registration Operations.....	52
C. Research Registration.....	56
D. The Registration Room School.....	57
E. Bombe Operation, Control, and Testing; "Duds" and Railway E.....	59
a. General.....	59
b. The Bombes and the Bombe Rooms.....	59
c. Bombe Control: The Netz Room.....	62
d. "Duds" and Railway E Traffic.....	66
F. The "Decoding" of Traffic.....	67
a. The "Decoding Room".....	67
b. Training Course for Typex Operators of the Deciphering Room.....	69
VIII. "Intelligencing" of E Traffic.....	70
A. General.....	70
B. The Operational Watch.....	84
C. The Intelligence Sections.....	86
a. Military Section.....	86
b. Naval Section.....	89
c. Air Section.....	91
d. The General Intelligence Section.....	93
D. The Liaison Section.....	99
E. The Signals Section.....	103
F. The Traffic Analysis Section.....	107
G. The German Book Room.....	110
Appendix.....	112

SECRET

DECLASSIFIED

SECRET

Authority NND 963016By 46 NARA Date 6/6/03

SECRET

S. C. ...
By Amber
Chief Signal Officer

Initials

Date

WJZ12 Aug 43

WAR DEPARTMENT

HEADQUARTERS, SERVICES OF SUPPLY
OFFICE OF THE CHIEF SIGNAL OFFICER
WASHINGTON, D. C.

SPSIS-3

SPSIS 311.5-Gen.

12 August 1943

Subject: Report on E operations at BP

To: Commanding Officer, Signal Security Agency

1. In the preliminary report dated 8 July 1943, it was stated that a series of detailed reports on the operations observed during my visit to GC & CS, 25 April--13 June 1943, would be submitted as soon as possible. Since it is believed that the E operations there are of greatest and most immediate interest, the report thereon was undertaken as the first of the projected series. The complete report on those operations is submitted herewith.

2. This work was done under considerable pressure and at such intervals as freedom from more pressing matters permitted. It undoubtedly contains a few errors of fact but it is believed that they are of a minor nature. If the story appears somewhat complicated, it is because the operations are interrelated in a complex manner, and necessarily so because of the nature of the problem itself. Every effort to simplify the picture has been made, but, it is hoped, not at the expense of accuracy.

3. This report does not go into details with respect to the technical aspects of the Enigma machine itself, nor of the "bombs" which are used in the solution of the keys for messages enciphered by that machine. These are difficult matters which should form the subject of special reports devoted solely thereto. In any case those technical details are not of general interest to those for whom the present report is intended.

4. The preliminary draft of this report was read by Captain Roy D. Johnson, who was most helpful in clarifying certain minor points on which my hurriedly-written notes were rather obscure and which therefore were doubtful in my own mind



SECRET

DECLASSIFIED

SECRET

Authority NND 963016


By wp NARA Date 6/6/03

SPSIS-3

-2-

12 Aug. 1943

when I came to transcribe those notes. He tells me that the report is fairly complete and gives a good picture of the operations as he saw them over a considerably longer period of time.


William F. Friedman
Director of Communications
Research

Incl: Report
"Cryptanalysis of
German Army and German
Air Force Enigma Traffic"

SECRET

DECLASSIFIED

Authority NND 963016

SECRET

By wp NARA Date 6/6/03

CRYPTANALYSIS OF GERMAN ARMY AND GERMAN AIR FORCE

ENIGMA TRAFFIC

I. Introduction

A detailed account of the manner in which the British operate in the solution of German Army and Air Force Enigma communications must be preceded by the statement that their success in this field represents a remarkable and extremely important cryptanalytic and intelligence achievement.

As a preliminary statement it should be noted that the British tackled and successfully solved a cryptographic system which apparently presents insurmountable and impenetrable bulworks against attack by pure cryptanalysis and that the solution was attained by exploiting to the fullest degree possible the weaknesses injected into the system by the methodicalness of the Germans in their formulation and operation of the system, by studying and making use of the well-known German addiction to fixed habits, and by taking advantage of the occasional carelessnesses and blunders on the part of German cipher clerks.

The success the British have attained and continue to attain in this field is noteworthy also because they have been able to keep the whole operation utterly secret from the enemy for so long a time, despite the fact that almost two thousand people are more or less intimately involved in producing the intelligence, that several hundred more receive and make direct use of the intelligence, and that the threads upon which these operations rest are so very tenuous that they might be broken by a mere whisper in the proper place at any moment. Indeed, the E operations may be said to constitute Churchill's "Secret Weapon" and their very existence constitutes the most carefully guarded secret the British have.

The complicated operations involved in this exploitation of GA and GAF Enigma communications require the coordination of the intercept activities conducted at many stations and of the efforts of several thousand people, but this report will concern itself almost entirely with the work at BP, where the cryptanalytic and intelligence operations are conducted. Although the work there is done in two principal, more or less physically distinct centers, one, where the cryptanalysis and traffic analysis is done, and another, where the "intelligencing" on the product is done, it must be noted that both centers are now in the same building, despite the fact that the names of the locations they formerly occupied (Hut 3 and Hut 6, respectively) are still attached to them. It must also be emphasized that the

DECLASSIFIED

SECRET

Authority NND 963016By Wp NARA Date 6/6/03

activities are most carefully integrated and coordinated. They comprise an operation that is really effectively unified, by insisting and insuring that all the personnel involved act as a closely-cooperating team and that the efforts of all of them are directed against the solution and exploitation of one problem.

* * * *

Before entering into details it is prudent to remark that the British organization is not a rigid or inflexible one, but quite fluid. Changes are continuously in progress, so that what was true in the spring of 1943 may not be true in autumn of the same year.¹ For this reason it is important to note that the organization and operations herein described are as they existed in June 1943.

I shall first take up the activities of the first group (the T/A and cryptanalytic in Hut 6), since they are basic.

* * * *

The operations in connection with the traffic analysis and cryptanalysis of GA and GAF Enigma traffic are organized under five divisions, the chiefs of which constitute the governing board for the work of this whole group. Attached hereto is a chart showing the organization in its broadest outlines, together with the personnel assigned to each division.

It is difficult to get a good picture of the entire operation and the flow of material from the raw traffic stage to the finally processed translations until one has studied the work done by the principal sections within these main divisions. I will try to indicate in some detail the various steps in the complicated flow of traffic, the responsibilities and activities of each of the sections handling it, and how the activities are connected up and integrated for most efficient operation. It will be noted in the attached chart that the total number of people involved in Hut 6 operations alone comes to almost 1300 and this does not, of course, include the large staff of intercept personnel involved in obtaining the raw material.

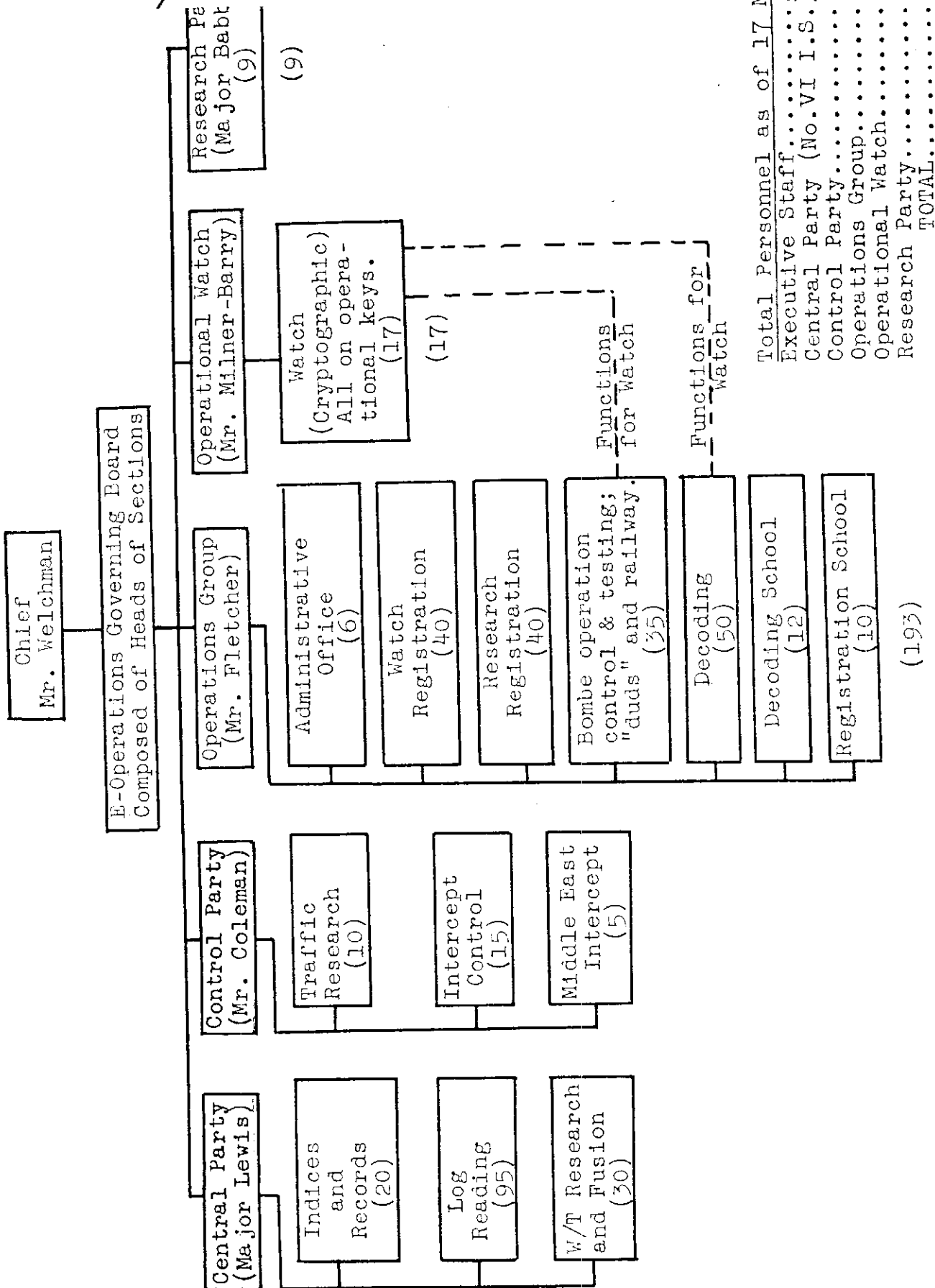
II. Preliminary Talk with Mr. Welchman

On Monday, May 10, I was taken into the office of Mr. Welchman, who is in charge of cryptanalytic operations in Hut 6, a name taken over from the original frame building in which the work was first organized and which is nevertheless still applied to that portion of the one-story, multi-wing, brick structure which now houses the activity. Mr. Welchman made an introductory statement the substance of which is covered in this section.

¹Confirmation of the validity of this remark is found in the news (4 Aug. 43) that No. VI Intelligence School has been abolished as such and that two sections thereof, vitally concerned in E operations, have now been definitely assimilated as parts of those operations. They are no longer echelons of an institution which at one time really existed as an entity but which later for all practical purposes had been reduced to merely a "paper" organization.

SECRET

Personnel, Organization and Functions of Hut 6 on GA and GAF E Operations



DECLASSIFIED
Authority **NND 963016**
By **46p** NARA Date **6/6/03**

Total Personnel as of 17 May 43

Executive Staff.....	6
Central Party (No. VI I.S.)..	14
Control Party.....	3
Operations Group.....	19
Operational Watch.....	1
Research Party.....	40
TOTAL.....	40

SECRET

DECLASSIFIED

Authority NND 963016
By 46p NARA Date 6/6/03 **SECRET**

The problem of solving the GA and GAF E traffic is by no means purely a cryptanalytic problem.¹ The traffic analysis or T/A side is of extreme importance, because with the very large number of cryptonets and stations involved, which do not operate upon any fixed schedules and which constantly change their call signs and often their frequencies, it is first of all a problem to identify the particular group of units which form each cryptonet and to isolate daily the messages that are in the same key. Moreover, the Germans have introduced very complicated radio procedures having as their purpose the suppression of characteristics by means of which nets and stations within nets may be identified. Elaborate measures are taken to preserve communication security and to prevent the enemy from obtaining valid information which may be used as a basis for identifying the transmitting and receiving stations, the units which they serve, their locations, and the stations with which they communicate. So far as possible, they try to suppress everything which might give clues leading to the interpretation of their signals and messages. Not only that, but in addition to meaningful messages they transmit many meaningless ones for practice, for deception, and so on. In short, great efforts are made to camouflage the communications as much as possible and while the task of the German communicators has been made more difficult by these measures, the latter have indeed greatly complicated the work of the British in their attempts to intercept and to learn the contents of the messages.

In these camouflage measures and in general communication and cryptographic security, the German Army is much better than the German Air Force, and were the latter to tighten up and get so proficient as the former, the British source of most valuable tactical and strategic information would dry up to a mere trickle.

The problem would, of course, be very simple if there were only one, two, or three cryptonets involved but as a matter of fact there are at the present moment almost 75 different main cryptonets, each having a key of its own. The recovery of each key presents a separate problem and the latter is one that recurs every day. In some cases, solution of a key is possible

¹Naturally the British do not use the terms traffic analysis, cryptanalysis, cryptonets, etc., but I shall employ our own terminology in this report, for purposes of clarity.

SECRET

DECLASSIFIED

Authority NND 963016 **SECRET**
By 40p NARA Date 6/6/03

only by intercepting one specific message out of several hundred, and locating or identifying that specific message is often a complicated piece of business. The particular message may be the basis of a "crib"—text that is suspected or known to be in that message because it has been found there many times before in exactly similar circumstances, and because of the well-known German addiction to fixed habits in language as well as in procedures.

During normal operations the traffic intercepted by the several stations amounts to over 6,000 message-parts¹ a day, a good many of which are, of course, duplicates, but in some cases the duplication in coverage is quite essential. However, the very effective intercept control which they have established enables them to concentrate on the traffic which is of vital interest, insure that they get the messages of vital importance, naturally neglecting traffic which is of little importance. This is, of course, essential because even though there are about 260 receivers at intercept stations in the U.K. and about 75 receivers at intercept stations with overseas forces, all now devoted exclusively to the E coverage, this represents only a fraction of the total E traffic. It would be impossible to get all of the traffic, even if it could be processed, which is out of the question despite their present large staff.

When the British started E operations they commenced assigning color designations to the different cryptonets but soon ran out of colors and now have adopted all sorts of names such as the names of animals, plants, insects, etc. [Hereafter these names will be used by me as references to the cryptonets.] From small beginnings in the early months of 1940, when an occasional key was solved, they have been able to go further, adding new cryptonets to their stock of daily solvable keys, until now they are able to handle most any of them in which they are interested. A great deal of very valuable information is now being produced every day by the whole group.

Each section in Hut 6 produces periodic and special reports and Mr. Welchman showed me samples of some of the various types of reports.

First there is a report called the "Central Party Report", which is put out by the T/A Research Party under Major Lewis.

¹German messages longer than 200-250 letters are invariably broken up into parts or sections, just as is the case in our practice.

DECLASSIFIED

Authority NND 963016
By wp NARA Date 6/6/03 **SECRET**

It gives the weekly story on each GA and GAF frequency that has been heard, together with details of anything of unusual interest that may have happened during the week in connection with each frequency.

One of the main jobs of the T/A Research Party, Mr. Welchman stated, is to study and seek out the most fruitful sources of "reencodements" (in our terminology: "reencipherments"), that is, messages which have been set up in one key for transmittal over one cryptonet and then have to be reenciphered in a second key, when the message has to be passed to another cryptonet having a different key. He stated that these reencipherments are not easy to spot and that there is nearly always some paraphrasing in connection with them, inasmuch as the German regulations required paraphrasing when a message had to be enciphered in a different key.¹ The T/A Research Party searches for new sources of reencipherments by a study of the interrelations among cryptonets, although the actual search for specific cases is made systematically by the log readers in the fusion room. The search for these reencipherments involves comparing messages with approximately or exactly the same time of origin. The lengths of two messages suspected to be related in this way is also a very important indication. Furthermore, it must first be established by the T/A Research Party that there is a proper radio link present for passing the message from one net to another and also that it is the sort of message that must or should be passed on.

By careful study of the logs it is also sometimes possible to find that a message has been sent by error to a station not having the key indicated in the message and therefore has to be repeated in the correct key, thus giving two messages with identical or nearly identical text in two different keys.

The Central Party Report has a good deal to say about "duds". These are messages that do not yield to decryptographing by means of the key indicated, which means that some error is present in the message indicator or in the "discriminant" or system indicator. The error may have been committed by the German cipher operator, by the German radio operator, by the British intercept operator, etc. Mr. Welchman stated that there were at the present time about 10% duds in the whole of the E traffic, that they caused a good deal of trouble, and that they tried very consistently to read every one of them.

¹The paraphrasing rule is, however, not strictly followed and usually such paraphrasing as occurs is accidental, introduced by the changes made when a clerk changes the spelling of a punctuation symbol or writes out a number in a different way than it appears in the first version.

DECLASSIFIED

Authority NND 963016 SECRET
By Wp NARA Date 6/6/03

The Central Party Report also contains considerable information about routine messages, which are always a potential source of important cribs. It also deals with receipts given for messages. The present practice on many circuits when receipting is to send the time of origin, group count, and indicator of the message. Sometimes the message itself has not been heard but merely the receipt therefor. A study of these receipts is very useful because having the indicator they often get information in connection with "Cillies", which I will describe later on.

Another report called the "Research Report", produced weekly, deals not so much with the elaboration of new solution methods based upon cryptanalysis as with research intended to find new cribs, or new procedures and "tricks" based upon the habits of German cipher operators. These studies are principally useful especially in the case of what they call "research" or "non-operational" keys¹. For example, in the report which Mr. Welchman showed me there was a paragraph devoted to the finding of a new crib in "Wasp" traffic, the crib consisting of a large number of letters found never to be varied for a whole month. As a result of this discovery they were able to solve, during the month of May, a total of 8 keys in "Wasp"; only on two occasions did the crib fail. When I inquired as to how many letters a crib should contain to be useful I was told that "they needed a crib of 30 letters to be happy", but they can work on as few as 15. Cribs of 75 and more letters are not at all uncommon. Mr. Welchman indicated that continuity in the study of cribs is absolutely vital, since they are constantly changing and for technical reasons it is necessary that the crib be "letter perfect". Even such a simple matter as replacing a German cipher operator in a net may change the crib, and for this reason the Research Party has an important part to play in maintaining continuity of successful operations in the case of the non-operational keys, each of which is operated upon at least once a week for this purpose.

Another report, known as the "Weekly Watch Report", deals largely with important information concerning the operational and research keys. For example, in the one report shown me

¹This distinction between "operational" or "current" keys and "non-operational" or "research" keys will be explained later. The word "research" is not an apt term in this situation.

DECLASSIFIED

Authority NND 963016
By wp NARA Date 6/6/03 **SECRET**

considerable attention was devoted to five different cribs which have been successfully employed on "Red", which is the principal GAF cryptonet for general communication and is the most important of all the E nets from the intelligence point of view. These cribs were identified as (1) "Iraklion numbers", (2) "Muffelbericht", (3) "Hippobericht", (4) "Zusauf", (5) "Gruenmeldung". The foregoing are merely short identifying names for the cribs themselves. The report deals in great detail with the most minute changes that were noted in the operational cryptonets during the week.

As to how many of the 70 or more different cryptonet keys they are able to follow daily, I was told that this varies. For example, when the North African campaign began, BP was able to operate only on the traffic of a few of the main cryptonets and had to give the others up as a daily operation. For May 6, 1943, the data were as follows:

Total number of message parts.....	3292
Number of operational keys solved.....	54
Number of non-operational keys solved.....	41
Number of other (back) keys tried.....	53
Number of bombe hours applied.....	4399

Mr. Welchman emphasized that the obtaining of specific cribs requires first class intercept control but that one could never be certain, except by most careful research, when and on what circuit a useful crib for a difficult cryptonet key might be discovered. He cited as an illustration of the latter fact that one day the key for a German Army cryptonet in the Mediterranean known as "Phoenix", very important in the Tunisian campaign, was solved by means of a reencipherment from "Chaf-finch", found in tank traffic in North Africa, but this traffic was heard only by an operator at the RAF Beaumanor intercept station in England. Occasionally the crib studies and operations at BP were vitally affected by "unfortunate" incidents in the operations in North Africa, as for example, when a certain unit led by a general who invariably reported every morning "Nacht verlauf ruhig" (- "Quiet night") was captured, the most fruitful source of cribs in an important cryptonet absolutely disappeared and other means of solution had to be found—that is, new cribs, which meant considerable trouble and delay. (Mr. Welchman expressed the wish that he might be able to control who should be taken prisoner in such cases.) Another instance of this same sort will be related later on in connection with "Zenits". Just how this intercept control is accomplished

SECRET

Authority NND 963016By Wp NARA Date 6/6/03

SECRET

will be seen in connection with the operations in the Intercept Control Room under Mr. Coleman, who issues a weekly "Intercept Control Room Report". This deals with the activities of the group which directs the day-to-day and, in fact, sometimes the hour-to-hour intercept missions of the various stations covering E traffic.

Mr. Welchman then made a rough diagram somewhat in the nature of an organizational and traffic flow chart showing the general nature of the set-up and the relations between the various units comprising the whole E operation in Hut 6. I have added a few notes thereto and append it to this page.

A bird's eye view of the whole operation in Hut 6 may be useful. The messages, of course, come from the various intercept stations. The first thing which must be done, naturally, is to sort the messages into their respective cryptonets. Technical data for this step are provided by the Traffic Research Group under Mr. Coleman. The messages themselves are sorted in a section under Mr. Fletcher, called Watch Registration. In the Watch Registration the large volume of messages is divided up into two principal classes:

- (1) Those which are "operational" in character—known to be such from previous studies of the traffic in the cryptonets concerned. These messages must be processed with the utmost speed.
- (2) Those which are "non-operational" or deal with matters that are not of an urgent or operational nature. These messages are processed as time affords, usually within a day or two.

The messages of the first class are examined immediately by the Operational Watch, and certain of them are selected and used as the basis for constructing menus which are then sent to solution machines or "bombes" so that the keys for the cryptonets to which they apply can be obtained. Having the key for each operational cryptonet, the other messages in the same key are sent to the "Decoding Room", where they are promptly deciphered and the German texts sent to Hut 3 for translating, emending, "intelligencing", and dissemination. As regards the messages in non-operational or "research" keys, as soon as the bombes are available certain messages in each of the cryptonets in this class are selected and sent to the bombes, solutions obtained, and so on. The procedure is

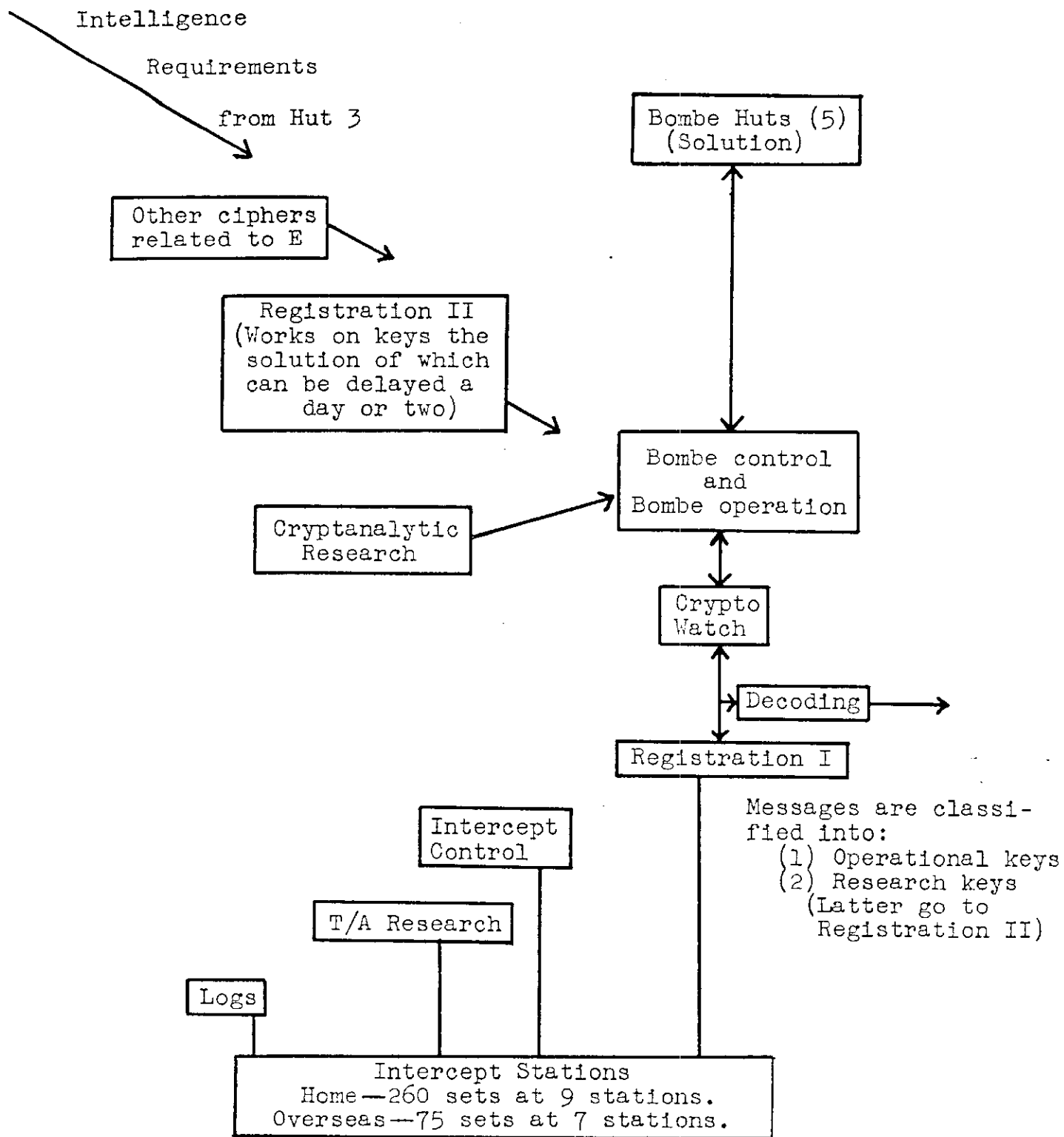
SECRET

DECLASSIFIED

Authority NND 963016

CRET

By Wp NARA Date 6/6/03



DECLASSIFIED

SECRET

Authority NND 963016

By wp NARA Date 6/6/03

exactly the same as in the case of the messages of the operational cryptonets except that the former are processed with a lower priority than the latter, that is, they are handled if, as, and when bombs are available, and the operational messages have been cleared.

At the present moment there are about 70 bombs in operation, and more are coming every few days. They are installed in several places, a few in Hut 11A at BP, more in "out-stations" within a radius of 50 miles of BP. Direct telephone and teleprinter service between Hut 3 and these out-stations is vital.

In addition to the bombs, the E operations require a good deal of IBM work equivalent to the full time of about 40 people. Also, for the rapid communications required in disseminating the fruits of the operations there are about 250 or 300 teleprinter, Typex, and cryptographic people required in the communications unit.

All in all, the total number of people involved in E operations is about 1700 but this figure does not include intercept personnel, nor overhead direction or training personnel. There are in this 1700 about 900 WRNS women and 75 mechanics employed in keeping the bombs going. The military and air force E operations are organized as a separate unit employing about 400 people in Hut 6 and 325 in Hut 3 on "intelligencing" the processed messages. Naval and submarine E operations are also organized as a separate unit with about 140 people engaged in cryptanalyzing the messages.

The policy with respect to E personnel is that no person who has participated in the E operations at BP can be sent out to combat areas or assigned to duty where there is any possibility of his being taken prisoner. According to Mr. Welchman and others with whom I talked it seems that Mr. Churchill himself has taken a deep interest in these operations and sees to it that no obstacles are put in the way of their execution. His policy has been to get the most competent people in England into the operations and to keep them there.

A schedule of my proposed tour of Hut 6 operations had been prepared and was now shown to me. I attach it merely to note that it was expected that I complete the tour in three hours! It became apparent within a few minutes, however, that this schedule would hardly suit my purposes and it was accordingly revised; but the revision was also impossible to follow

SECRET

DECLASSIFIED

Authority NND 963016

By 40p NARA Date 6/6/03

SECRET

PROGRAMME OF VISIT OF MR. FRIEDMAN

1. Major Lewis ($\frac{1}{2}$ hour)

German use of call-sign books.
Stern-Kreis-Netz. Frequency changes.
Work of log readers and Fusion Room.

2. Major Babbage ($\frac{3}{4}$ hour)

Example of hand break.
Stecker knock out.
Crib-menu-bombe-testing-break.
R/Es (or leave to Milner-Barry).
General description of work and policy.

3. Mr. Winton and Mr. Braithwaite ($\frac{1}{2}$ hour)

Key records.
Discriminants.
Methods of identifying traffic.
Control of interception.

4. Mr. Milner-Barry ($\frac{3}{4}$ hour)

Watch organization for current breaking.
Log books, folders etc.
Examples of cribs and R/Es. (Find out how much Babbage has done.)
Problems of bombe management and general policy.

5. Mr. Fletcher ($\frac{1}{2}$ hour)

Flow of traffic through Hut 6.
T/P - R.R.I. - D.R. - N.R.
I.P. - R.R.2.

REVISED PROGRAMME

- | | |
|---------------------|------------------------------------|
| 1. Major Lewis | Log Reading and Fusion Room. |
| 2. Major Babbage | Cryptographic Research. |
| 3. Mr. Milner-Barry | Cryptographic Watch. |
| 4. Mr. Fletcher | Bombe Control. Visit to Bombe Hut. |

POSTPONED

- | | |
|-----------------------------------|------------|
| 5. Mr. Winton and Mr. Braithwaite | As before. |
| 6. Mr. Fletcher | As before. |

DECLASSIFIED

SECRET

Authority NND 963016By Wp NARA Date 6/6/03

and we soon gave up any idea in trying to adhere to a rigid time schedule. As a matter of fact I spent about a week on Hut 6 activities and at the end I felt I had only just about obtained a general picture of the operations.

It will be noted that in general the schedule was designed to outline a logical tour of the activities: first a look into the matter of the gathering of the raw material, then a review of the principles of solution, followed by a survey of the manner in which messages are sorted into classes corresponding to keys, then a look into the bombe operations, and finally a look into the flow of traffic through the hut. Although it was found impractical to follow this logical sequence in making the tour, it is the sequence which will be followed in this report.

No attempt will be made herein to describe the E machine or the technical details of the cryptanalysis itself, or of the bombes, all this knowledge being assumed to be in the possession of the reader.

III. The Control Party

A. General

The Control Party, under Mr. Coleman, comprises three sections: (1) Traffic Research, the principal function of which is the provision of basic technical data required for the primary sorting of the E messages into their respective cryptonets; (2) Intercept Control, the principal function of which is to direct the operations of the E traffic intercept receivers in a very detailed manner—sometimes on an hour-to-hour or even a minute-to-minute basis so as to insure that the desired messages are actually obtained; and (3) Middle East Intercept, the principal function of which is to coordinate E coverage in that area with intercept in the U.K.

An outline of the organization under Mr. Coleman is shown below:

FLt. Davies Middle East Intercept (6 persons)

Mr. Braithwaite Direct control of duty officers in the control room. (8 officers, 6 women)
--

Mr. Winton Traffic Research (1 man, 6 women)
--

SECRET

DECLASSIFIED

Authority NND 963016 **SECRET**
By Wp NARA Date 6/6/03

B. Traffic Research

As noted above, the principal function of the Traffic Research Section is to provide basic technical data essential to facilitate the primary sorting of the messages into their respective cryptonets. This is not an easy matter, considering the number of messages and cryptonets and their external similarities.

In order to understand why it is difficult to sort E messages into the 70 or more German cryptonets, a few words must be said about the message and system indicators used by the Germans.

The indicators for GA and GAF Enigma messages require two groups, the first group consisting of 6 letters which give the machine setting, the second group consisting of 5 letters of which the first and second are nulls, the third, fourth, and fifth, are the letters forming the "discriminant" or what we call the "system indicator". (In recent days, however, the use of nulls is dying out and the discriminant is being sent as a 3-letter group just before the message indicator.) The letters of the discriminant may be given in any order, and there are every day four variant discriminants for each cryptonet key. Since each cryptonet has its own key, the discriminants are absolutely essential to the quick recognition of the specific cryptonet or key in which a message has been enciphered. This is true not only so far as the British cryptanalysts are concerned but also as regards the Germans themselves. The latter, of course, have the discriminants provided them in the form of lists, so that there is no difficulty about the matter so far as they are concerned. But the British, not being on the "distribution list", have to identify the discriminants for each of the 70 or more cryptonets daily. Until this is done, it is impossible or impractical to try to segregate the messages into the different systems, which, of course, is the first step in their solution.

Fortunately, however, in this first step the British have at this stage of the game a great deal of help as a result of their past studies of the system used by the Germans in assigning the discriminants. It appears that in the German Army at the present time the cipher compilation center has a set of approximately 250 cards on each of which there are 31 lines corresponding to the days of the month and on each line there are 4 discriminants. In making up the monthly list of

SECRET

DECLASSIFIED

Authority NND 963016

By Wp

NARA Date 6/6/03

SECRET

discriminants for each cryptonet all they do is to select one of these cards and assign it to a specific cryptonet. Since the frequencies used by the different cryptonets are fixed,¹ it is not a difficult matter to correlate on the first day of each month a particular frequency or set of frequencies with a particular cryptonet and then since the discriminants to be used for the day are found in the beginning of the texts of the messages in that cryptonet the identification of the card selected becomes a fairly simple matter.

With slight modification this same system is used by the GAF. Instead of selecting one out of approximately 250 cards as the source of the discriminants for the whole month for a given cryptonet, they may select the discriminant for the 3d day on 30 (or 31) cards chosen at random from among the whole deck; or it might be the 11th day on the cards, or the 18th day etc. In any case, the row-number (=day) stays the same for the whole month on a given cryptonet.

It is obvious, therefore that the only difficulty which the British encounter in this respect is on the first of the month in the case of both the GA and GAF, but so long as the frequencies allotted do not change from day to day the problem presented on the first of each month is not serious. However, in the case of the air-to-ground communications in the GAF the frequencies do change and here the problem is considerably more difficult. On this point I shall have more to say in another place.

The segregation or sorting of the E messages into their respective cryptonets on the first day of each month, or when a new key list goes into effect,² requires a thorough knowledge of the organization of the communications networks of the GA and GAF, how their call sign systems work, how their radio nets function, how frequencies are allocated, etc.

The very first and basic job of the people in the Traffic Research Section is to identify the call signs of the stations

¹The frequencies (except in air-ground communications) change only occasionally, but this phenomenon is under constant observation and study by the T/A people. It is an important function of the search log readers in Major Lewis' party and therefore gives rise to little difficulty except for the first few days of its entrance upon the scene.

²As for example, when the Tunisian Campaign was over, about May 15, 1943, the Germans shifted to the next or reserve key list.

DECLASSIFIED

Authority NND 963016

By wp NARA Date 6/6/03

SECRET

in communication, in order to find out who is communicating. When the stations have been identified, and the outlines of a cryptonet ascertained, by assembling the traffic of stations in the same cryptonet the four discriminants for the day on that cryptonet are noted and they will usually conform to the "predictions" made on the basis of the information noted above with respect to the discriminant allocations. Thus, any further messages containing these discriminants can be immediately classified and sorted—a process done for the bulk of the messages in another section of Hut 6, to be described later. Of course, after the first day of the month, when data are at hand for the prediction of call signs, the initial identification of discriminants is not difficult, and the work is done promptly. But on the first day of the month or when a change is made in the frequency allotted or in the cycle or serial¹ from which the call signs are taken, and predictions can no longer be made as to what discriminants and call signs will be used by a given unit on a given day, the work of the people in the Traffic Research Section begins.

To begin with, the people in the Traffic Research Section must, of course, know a good deal about the various types of radio working employed by the Germans. There are four of them, viz., (1) the "Linie" or "Line", (2) the "Star" or "Lateral", (3) the "Kreis", and (4) the "Netz".

The first type is largely used for point-to-point communications with or without a single or double call and on one or two frequencies. It is employed only between a few large fixed stations having, as a rule, high-speed automatic transmitters.

In the second type (Star or Lateral), if there are 4 stations (A, B, C, and D) reporting to a single superior or control station (X), and if A wants to send a message to B he cannot do so direct but normally must pass the message to X for forwarding to B. In this case there is usually but one day frequency (with one alternate) and one night frequency (with one alternate). This type of working is the most common in the GAF but little used in the GA. The out stations call the control station by sending their own call. If the message is to go to another one of the out stations the calling station makes its own call and adds "For ABC (call of station for which message is intended)". If ABC hears the message he can receipt for it to the control station, making the relay unnecessary. However,

¹These terms will be explained later.

DECLASSIFIED

Authority NND 963016 **SECRET**
By Wp NARA Date 6/6/03

in some cases A can send direct to B (lateral working) if permission is first obtained from the control station.

In the third type (Kreis), the stations have separate call signs and may communicate freely with one another. In this type of working the net uses only one frequency at one time, any station calling any other but each station having its own call. This is like the lateral working mentioned above except that prior permission of the control station does not have to be obtained.

In the fourth type (Netz), each station in the net has an individual frequency on which it may receive, but for transmitting it must transmit on the receiving frequency assigned to the station to which it is going to transmit, employing its own call sign; in other words, each station in the net has a fixed receiving frequency but variable transmitting frequencies and there are as many of the latter as there are stations in the net. Thus each station in the net must keep one receiver on its own receiving frequency on which all of its own incoming traffic will come, and it must have a list of the respective receiving frequencies of all the other stations in the net. This system is used by the whole of the Wehrkreis, or high command net of the GA home forces, by all of the Vulture cryptonets on the Russian front, and by most of the GA groups in France.

This last type of working gives the British most trouble because it is hardest to intercept. For example, in the Wehrkreis there are approximately 22 stations in the net and because of the method of working it may be necessary to use as many as 24 different receivers for intercepting its traffic. It is also the most difficult as regards identifying the stations that are in communication, because of the manner in which the call signs are used. The most feasible way of identifying the stations, if their location or the unit which they are serving is unknown, is to take D/F bearings. The Army, Navy, RAF, and P.O. intercept stations in the U.K. are all connected up by land lines to D/F control stations so that any signal upon which a "fix" is required can be transferred from a receiver at any station to two or more D/F station receivers. The operator at the D/F station receives, by telephone in one of the earphones of his headset, the signal from the receiver at the intercept station; on the other earphone of his headset he gets the signal from his own receiver, which he must search for on the basis of telephonic information given

SECRET

DECLASSIFIED

Authority NND 963016 **SECRET**By wp NARA Date 6/6/03

him by the intercept station. Having found the correct transmitter by thus matching the two signals, he operates his loop gonio and reports the bearing to D/F control, where the bearings from the several D/F operators at work on the same signal are plotted on a map. In difficult cases, or in the case of a new station coming up, it is necessary to ask for D/F bearings to be taken, in order to identify and locate the station.

Next, the people in the Traffic Research Section must, of course, understand thoroughly the method of assigning call signs and how the pertinent call-sign books (the so-called "B" or "Bird book" used by the GAF, and the "E" or "Elephant book" used by the GA) works. It must be understood that each such call sign book consists of 200 pages on each of which there are 200 call signs making 40,000 call signs available in each book. Each call can be referred to by row and column coordinates giving its position in the book. Now the territory occupied by German forces in Europe is divided up roughly into territorial areas or districts called "Funkverkehrbereiche". In these districts each unit or headquarters is assigned a row in the book and this row stays the same for a long period. The number assigned to this row forms one of the coordinates determining the call sign. The unit is, however, also assigned a sequence of "columns" for 365 successive days, that is, a series of specific points irregularly distributed in the row from which the unit takes its call signs for the 365 days throughout the year. This sequence of daily changing positions in the row is called a "cycle" in the case of GAF communications and a "serial" in the case of GA communications. Therefore, when a "funkplan" or radio net is established the call sign of each station in the net is fixed for a considerable length of time, and since the row seldom changes but only the specific position in the row varies, to ascertain the latter for each day the Germans refer to a table called "Die Zuweisung der einzelnen Funkverkehrbereiche", or "the indicators for the respective radio districts". This table looks like the following:

Die Zuweisung der einzelnen Funkverkehrbereiche

Cycle Nos.	Jan.	Feb.	Mar.	...	Oct.	Nov.	Dec.	1	2	3	4	5	6	...	30	31
	1	9	18	...	78	87	96	85	172	13	41	189	9	...	73	28
2	10	19	...	79	88	97	16	43	127	13	95	83	...	3	67	
	11	20	...	89	89	98	131	26	39	112	65	73	...	122	91	
150	8	17	...	77	86	95	Each row is a "cycle". In each row, numbers from 1 to 200 in random order.									

DECLASSIFIED

Authority NND 963016

By 46p NARA Date 6/6/03

SECRET

Each sequence of numbers in the rows in the right-hand side of the table is a cycle. Having been assigned a cycle number, say cycle 11, the operator refers to the left-hand section of the chart, finds the position of the number 11 in the pertinent month, and moves to the right-hand side of the table where on the first day of the month (say February) he sees the number 131, on the second day, the number 26, etc. Then having the row also more or less permanently assigned, for example row 15, he proceeds into the call-signbook itself, finds row 15 and column 131 (for February 1), and takes as his call sign the call determined by these two coordinates (15 and 131); on February 2, he would take the call sign designated by the coordinates 15 and 26; on February 3, the one designated by the coordinates 15 and 39, etc.

On the surface the constantly-changing call signs look as though they had been assigned at random but in reality everything about the method is very systematic, in accordance with the usual German way of doing everything. (There is even a relationship between the sequences of numbers within the cycles, governed by a "Zeitenverteiler", which consists of two concentric discs for producing mixed sequences. These discs provide for 200 settings which is as though one had two sliding strips containing two primary mixed sequences of 200 elements, the two sequences being juxtaposable at 200 positions and thus yielding 200 secondary sequences.) The normal time for changing the entire system of call signs is April 1, but this year it happened on May 1. The assignment of rows and cycles for the GA is done by the OKH (= Oberkommando des Heeres = Army High Command) and for the GAF by the OKL (= Oberkommando der Luftwaffe = Air Force High Command).

As regards the changes in radio frequencies, it was stated that the frequencies employed for larger units or headquarters do not alter frequently, but as regards the forward units there is a daily change in frequency as well as in call signs for every unit. The system of assigning frequencies for tactical units of the GAF is different from that for tactical units of the GA and a complicated scheme which the British call the "FAGS" is now in effect. I will describe this later on.

The manner in which the Traffic Research Section identifies the discriminants may now be described briefly. Coming from the various intercept stations in a more or less steady stream by teletype are the sheets containing merely the preambles to be messages intercepted. (The messages come afterwards,

SECRET

DECLASSIFIED

Authority NND 963016

By 40p NARA Date 6/6/03

SECRET

also by teletype, as soon as possible, but the preambles are given priority in transmission.) If it is not the first of the month, then, as explained above, the discriminants to be expected on each frequency or cryptonet are known, and it is merely necessary to check in each cryptonet. Hence, this being more or less of a routine job, it can be done on the messages themselves by "lesser-powered" people in the Identification Party of the Watch Registration, who are provided with the "predictions" in advance by the Traffic Research Section. How the Identification Party works will be told in its proper place under the activities of the Watch. But if the first of the month has arrived, and a new key list, as described above, is in effect, the Traffic Research Section has a bit more trouble, since they must identify which of the approximately 250 discriminant cards has been selected. How this is done has already been explained.

C. Intercept Control

This activity is a branch of Mr. Coleman's group and is under the direct charge of Mr. Braithwaite. In his absence Flight Lieutenant G. T. Davies was designated to outline the work of this section.

Davies began by indicating what the intercept sources and where the stations are located. Those in the U.K. have been built up over the past four years upon a framework of intercept stations which were available at the beginning of the war. The intercept stations belong to the Army, Navy, the RAF, the Post Office, and the Foreign Office. BP allocates tasks to certain of the stations which are devoted exclusively to E intercept and smaller E tasks to other stations, but the stations themselves still remain under the administrative control of the service which owns and operates them. Colonel Sayre under Commander Travis is in charge of the entire Y intercept for BP. All policy problems must be taken through Colonel Sayre such as the question of additional sets, moving sets, etc. The stations in the U.K. doing intercept work for BP are as follows:

- (1) WOYG (War Office Y Group) at Beaumanor: 105 receivers for E; tends to specialize on German Army E, but takes some GAF material as well.
- (2) RAF stations at Chicksands: 99 receivers for E, specializing on GAF but not wholly. BP can only

SECRET

DECLASSIFIED

Authority NND 963016
By 46p NARA Date 6/6/03

SECRET

suggest what might be done in the way of administration, personnel, etc., but with reference to what shall be taken on the sets is under the full control of BP.

- (3) Army station at Harpenden: 23 receivers for E which are concentrated on GA or GAF on the western front.
- (4) Post Office station at Whitchurch: 21 receivers for E. This is a new station and has far less experienced personnel so that they devote their attention to material of lesser importance at present and do not specialize.

The foregoing are the four main intercept stations for E but in addition there are the following in the U.K.:

- (5) RAF station at Shaftesbury. This is a subsidiary of Chicksands and is run by the same directing personnel as the latter. There are only 4 receivers on E.
- (6) Post Office station at Cupar: 1 receiver on E.
- (7) RAF station at Wick in northern Scotland: 5 receivers specializing on E traffic to, from and within Norway.
- (8) Post Office station at Denmark Hill: 7 receivers, 5 of which are auto. (There are only 3 stations which can take auto, Denmark Hill, WOYG, Whitchurch.)

The receivers on E working at overseas stations are as follows:

- (1) Fixed Army station at Heliopolis: 10 receivers for E.
- (2) RAF fixed station at Alexandria: 22 receivers for E.
- (3) Six Army B-type mobile intercept groups: 2 receivers at Alexandria and 4 at Derna.
- (4) Army fixed station at Sarafand: 4 receivers on E.

(The preceding four groups consist of four units under the control of what is called No. VII Intelligence School at Cairo.)

- (5) At Malta there are 12 receivers and at Gibraltar there were about 14 which have been moved to Bizerte. This new station at Bizerte is going to be a rather

DECLASSIFIED

Authority NND 963016
By wp NARA Date 6/6/03

SECRET

important affair. It is to get 12 receivers from Tripoli, the 14 mentioned above from Gibraltar, 12 sets which are to be allocated from American mobile units, and an unspecified number of B-type mobile units.

It will be noted that there are at present approximately 265 receivers in the U.K. and about 75 receivers at overseas stations all on E work.

BP has absolute control over what shall be taken on the receivers allocated to its work. There are direct telephone and telegraph lines to all stations in the U.K. except those at Wick, Cupar and Shaftesbury. There is, however, teleprinter service to the latter places through a switchboard at Chicksands. Each station sends its traffic by teleprinter, the messages themselves being preceded by a register containing merely the preambles which are transmitted in a constant stream just as soon as a page of preambles is ready.

The decision as to the number and location of receivers that shall be allocated to each intercept problem on which BP works is a responsibility of Colonel Sayer, who is in charge of all intercept. But having allocated the receivers to a job, the assignment of specific tasks is a responsibility of intercept control people in the group working on the problem. Thus, it is the function of the intercept control group under Mr. Coleman to assign specific tasks to the receivers which have been allocated for E coverage at the above-mentioned stations, to see that the specific E cryptonets are properly covered, and to help the intercept stations on E coverage in every way possible. The intercept coverage is a result of the consideration of the following three factors: (1) the cryptographic requirements; (2) the T/A requirements; (3) the Intelligence requirements. Of these the cryptographic cover has absolute priority because without this the other two are of little value. Mr. Coleman has the last say as to what shall be covered and uncovered by what stations and to preserve a balance as between the cryptographic, the T/A and the Intelligence requirements. It is his job to supply information and directives to the intercept people and to see that they are executed properly.

The cryptographic requirements do not generally alter from day to day, but nevertheless they are reviewed regularly once a week, as this is the only way of insuring that commitments which should be dropped are actually dropped. The intelligence requirements are reviewed daily. The intelligence people in Hut 3 send daily a list of frequencies, usually GAF, which they want covered. On receipt, the items on the list are checked off against the previous daily list and changes are

DECLASSIFIED

Authority NND 963016
By Wp NARA Date 6/6/03

SECRET

noted. The control officer must see to it every day that each new frequency is covered and that none are omitted. It allocates the new jobs to the stations and therefore must have detailed knowledge of what every set is doing and what the cryptanalytic, the T/A, and the intelligence people require. It takes six to eight months or more to be able to assume the control officer's responsibilities. He must acquire knowledge of all Hut 6 work and in respect to cribs, he must know what messages must be copied absolutely accurately. This often necessitates what they call double and triple banking, that is, two or three different receivers listening to and copying the same message so as to insure accuracy. All direct telephone lines to the various intercept stations are centralized in the control room and the control officer in addition to being responsible for all changes in assignments must be able to answer queries coming from the intercept stations. He must be able to tell them instantly what should be dropped in case of emergency, for example. He must be informed by the intercept stations when plain language is being copied, when any QTA (cancelled message) is intercepted; QZL (unreadable); QMO (code compromised); etc. He must know all about log reading and radio procedure. One of his most important jobs is to see that the cryptographic frequencies are covered adequately and whether there shall be single, double, or triple banking. (Sometimes an important crib message requires even more than triple banking in order to insure 100% accuracy in its interception. This may seem wasteful of sets and operators but is absolutely necessary at times.) He must check periodically each circuit being covered to insure that the station or stations are on the job. This as regards the priority traffic is accomplished by a telephonic check every hour with the largest intercept stations; in this check the intercept station calls off each frequency and gives the number of message parts taken on that frequency. The totals are entered on a form showing clearly what message parts have been taken by the different stations allocated to the same frequencies, so that comparison can be made periodically to insure that the stations are on the job. For example, if it becomes noticeable that one station on a double banking job has failed to report two or three messages reported by the other intercept station on that same job the control officer phones at once to learn the reason. In this work he must, of course, be very tactful. On the other hand, the intercept stations are bound to report by telephone at once anything unusual that is happening, as for example, an "STW" message. This is the signal for the German word meaning "Am changing station" and is, of course, of immediate

SECRET

DECLASSIFIED

Authority NND 963016By W/p NARA Date 6/6/03**SECRET**

interest to the intelligence people. An unusual plain language message may be important. The story connected with the interception of such a message will be told later on.

The foregoing represents the operational side of a control officer's job. He must have plenty of background in the way of documents supplied him by the T/A people, the cryptanalytic people, and by the intelligence people. He must read all the traffic that comes out in final form and must look through all of the decipherments to keep up with the relative importance of the various keys. He must read the report issued weekly by the Central Party under Major Lewis, which constitutes, I was told, the "Intercept Bible". Finally he must keep up-to-date records on messages heard on all frequencies and maintains an "encyclopedia", which is a loose leaf book containing this information.

The control officer's job is accomplished in three shifts, the first one from 9 a.m. to 6 p.m., during which he has an assistant; the second, from 5 p.m. to midnight, during which he has only one telephonist, and one discriminatrix; and finally from midnight to 9 a.m., during which he is assisted by only one discriminatrix.

There are now eight experienced intercept control officers and each one tends to specialize in a particular field. One of them, for example, may specialize in GAF communications organization; another may specialize on that of the German Army; another, in radio procedure; another on discriminant blocks; another, on the preparation and use of call sign books. This specialization has been developed on the initiative of these officers themselves.

I visited the control room one afternoon and the following are some of the highlights:

A log book contains notations of all important events for the period being recorded and one of the chief duties of the day control officer is to go through the log kept by the night control officer and clear up any points requiring attention.

A very interesting point was brought out showing how important the intercept requirements in regard to E coverage are regarded. In the case of what they call "red hot" German E cryptonets, if a local Army, RAF, Navy, or Post Office radio

DECLASSIFIED

Authority NND 963016By wp NARA Date 6/6/03

SECRET

station is causing interference, BP can request that the British station shift frequency. An inter-service agreement in this regard has been arranged with regard to 33 frequencies and this list is revised every Saturday morning by conference in London.¹ Incidentally it is to be noted that on the principal GA and GAF circuits there are four main frequencies: a day frequency and its alternate, a night frequency and its alternate.

A card index of all frequencies covered on priority assignments is maintained in order of ascending frequency. This index is in the form of a Kardex system with colored tabs and the data on the cards indicate whether the frequency is important as a source of "cribs" or "cillies", or whether it is an intelligence cover; which intercept station is covering it and whether on part time or full time, etc. The intercept station has, of course, a duplicate file. Every morning an assistant to the control officer going on duty telephones the intercept stations and goes over the entire cover in the case of all of these frequencies.

A record is maintained of the changes in cover during the period. These changes are written in the intercept station log during the day and are carried over into the Kardex the first thing the next morning. The item in the log is then checked off to indicate the entry has been made. A priority or "Cousens" list, (first produced by a Captain Cousens) comes to the control room between 6 and 7 p.m. daily. It shows the intercept priorities desired by the intelligence people, these being arranged in two categories and each frequency being noted together with its cycle or serial. On first priority missions, frequencies must be double banked. This list is merely by way of confirmation, because Hut 3 telephones the changes to be made from the previous day's coverage direct to the control room and then sends the confirming list over by messenger. If changes in allocation of sets are necessary the control officer makes the necessary alterations, is responsible for making the shifts in the sets, and for getting the proper coverage. In the case of frequencies on automatic circuits, the indication from the intelligence people as to first priority is also accompanied by the German recognition symbol in use to indicate such a priority.

¹BP does not have the power to force the station to shift frequency but unless there are weighty reasons to the contrary, the shift is made.

SECRET

DECLASSIFIED

Authority NND 963016
By wp NARA Date 6/6/03

SECRET

With regard to the control and coordination of the E coverage in the Middle East, Flight Lieutenant Davies indicated that BP maintains a radio link with Cairo, Malta, Tripoli, Constantine, and Ft. DuKebir. There will also be a radio link with the new station at Bizerte; with Gibraltar there is a cable link. At all of these places the intercept control group at BP maintains representatives. All of these stations have been provided with copies of the secret call sign books. At Cairo and Bizerte there are T/A centers on a large scale and they also solve low grade German and Italian on the spot.

Between BP and Cairo there are two main links; first there is a series of telegrams called "cover telegrams" which deal with the cryptanalytic and radio coverage desired. Second, liaison is maintained on all T/A matters, new frequencies, data from log readings, etc. The main station at Cairo sends back by radio, enciphered of course by Typex, registers of preambles of all intercept messages, just the same as the stations in the U.K. do. At the moment, however, Cairo does not send back all of the traffic, but twice a day on a request from BP they send the messages desired by the latter. The tasks allocated to these stations are constantly under revision as to priorities and BP indicates the priorities as they do in the case of the home stations. Some of these intercept stations centering about Cairo or controlled by Cairo do not send their registers by radio; for example, Malta and Tripoli do not, but their messages are Typexed and sent to BP. From the station at Sarafand in Palestine, messages are sent to Cairo and are then Typexed to BP. The logs are not sent.

The T/A people at Cairo and at the other stations are in frequent contact with Hut 3 people in full exchange of data and results.

IV. The "Central Party"

A. General

The activities in this division or group of three sections, which are under Major Lewis and form a part of what is euphemistically called "No. VI Intelligence School" but are physically located in Hut 6, are mainly of a T/A nature. As indicated in the organizational chart, the personnel of the Central Party deal with and prepare indices and records on the raw material;

SECRET

they read the logs on E intercept, which requires a thorough knowledge of the complications of German Army and Air Force radio communication networks, the German procedures and methods of working in the several different types of nets, the German use of constantly varying call signs and frequencies, the call-sign books, and so on; they do research in traffic analysis; and "fuse" information from traffic analysis, from cryptanalysis, and from the "intelligencing" of E traffic to give a very complete picture of E communications.

The personnel of the Central Party consists of a total of approximately 135 people. The latter comprise 15 to 20 clerks in the Indices and Records Section; 80 "Priority Log Readers", i.e., people who study the logs of sets on regularly assigned or operational frequencies; 15 "Search Log Readers", i.e., people who study the logs of sets on roving or search missions; and 20 "Fusion Room Specialists". The various sections work in three shifts, the largest of which is the day shift, from 9 a.m. to 6 p.m.

B. Indices and Records Section

The functions of this section are purely of a record-keeping nature. It receives the logs, keeps records pertaining to their receipt and disposition; it is the central bureau for receiving and forwarding maps, charts, and diagrams, and so on; it keeps track of personnel and equipment of the Central Party; and in general does the "house-keeping" for the whole group.

C. Log Reading Section

All of the 9 large U.K. stations with their 265 receivers and some of the 7 overseas stations with their 75 receivers send their logs to the log reading section for study. They come in batches, of course, in some cases within a few hours after the messages to which they apply have been intercepted, in other cases, after a day or two, and in still other cases only after several days, depending upon where the intercept station is located. On arrival the logs are primarily sorted into categories based upon geographical considerations. Some of the groupings now in effect are as follows:

Authority NND 963016By Wp NARA Date 6/6/03

- | | |
|---------------------|--|
| (1) Scandinavia | (7) Central France |
| (2) North Russia | (8) Southern France |
| (3) Central Russia | (9) The Low Countries (Belguim,
Holland, Denmark) |
| (4) South Russia | |
| (5) Mediterranean | (10) The Balkans |
| (6) Northern France | (11) Greece |

The log readers are primarily divided up into three large groups as follows:

- (1) Enigma log readers
- (2) Non-E log readers
- (3) Italian Army and Air Force log readers

In the present report we are concerned only with the first group.

The E log readers are, in turn, organized in groups which work on the traffic pertaining to these specific geographical areas and become specialists therein. Each group works under a junior officer and there are persons who coordinate the work of the different groups, but the groups work very closely together and there is a great deal of interchange of information among them, for reasons which will become apparent in connection with the discovery of "reencipherments". Each log reader is assigned one large or several small nets in his area to study and follow in detail so as to get the picture of the E communications of that corner of the world.

Before giving a detailed account of what the log readers do, a general statement of their functions may be useful. It is their primary function to provide information which will assist the cryptanalytic people and the intelligence people (Hut 3) in their job. To do so they build up graphically complete pictures of the various cryptonets using the Enigma, those of the GA, the GAF, the Abwehr (Secret police), the railway groups, etc. They must be able to answer any queries of a T/A nature that may be asked by the E cryptanalytic, the intelligence, or other parties at BP and that may have a bearing upon the communications of the GA or GAF group in question. A secondary function is to spot reencipherments, to give assistance in the solution of "duds" or messages with erroneous indicators, to spot routine or crib messages, to furnish data likely to identify messages with missing preambles so that the messages can be deciphered, etc. These duties will all be dealt with in some detail.

DECLASSIFIED

Authority NND 963016

By wp NARA Date 6/6/03

SECRET

To begin with, of course, the log readers must have as much knowledge about German radio procedures, net working, call signs, etc., as do the people in the traffic research room. For this reason they are given special training, about which something will be said later on. Just what the log readers do can be indicated by noting that first of all they are constantly on the lookout for anything new in the way of new stations, old stations dropping out, new procedure signs, etc. Every bit of unusual or novel behavior, as noted by them, is the subject of rumination and scrutiny.

As noted before, the log readers are of two general classes: (1) "priority log readers", that is, those who study the logs of sets on known current operational frequencies, and (2) "search log readers", that is, those who study the logs of sets assigned to roving or search missions, constantly on the lookout for new cryptonets.

The log readers study very carefully the receipts for messages. In German practice a receipt usually consists of the preamble of the message being receipted for and comprises (1) the time of origin, (2) the group count or check, and (3) the 6-letter key indicator. The discriminant is usually omitted. Generally no serial number is given. The log readers spend much time searching for "giveaways" and "cillies" in these receipts.¹

By "giveaways" is meant the disclosure of cryptographic information by plain-language "chat" between operators—such things, for example, as disclosing the wheel order. When, after considerable haranguing back and forth (especially between two operators one of whom is rather stupid) the better operator loses patience and gives the stupid one the wheel order in plain language, this is a simple case of a "giveaway". Sometimes even the steckers are disclosed in the same manner, especially when there is much laxity in cipher discipline. For example, in the cryptonet known as "Brown", which handles the cipher communications of the radar stations in northern France, this happened a number of times. I was told that "these people are experts in radar but very poor cryptographers". The manner in which the receipts are used to yield cryptanalytic information, in other words, "cillies", may best be described by

¹The origin of the word "giveaway" is obvious. The word "cillie" or "cilly" comes from CIL, the 3-letter group involved in the very first case of the phenomenon to be described.

Authority NND 963016By wp NARA Date 6/6/03

giving an example or two, and these examples can be understood only in the light of a knowledge of the present German method of deriving the keying indicator for a message. First of all it must be understood that the daily key given a German cipher operator shows the following:

- (1) The specific rotor combination—the particular selection and order of the 3 (out of the available 5) rotors which are to be used that day.
- (2) The "ringstellung"—the position or setting of the rotatable ring on each rotor, which determines when the next rotor to the left will advance one place.
- (3) The "steckerung" or plugging of the machine.¹
- (4) The "discriminants"—the 4 variant system-indicators.

The derivation and indication of the specific "message indicator" consists of 6 steps, it being understood that the daily key as described above has already been set up.

Having the machine rotors, the ringstellung, and the steckerung all set according to the daily key, the procedure is as follows:

1st step—Select 3 letters at random; for example, ABC.

2nd step—The rotors are aligned to ABC (from left to right).

3rd step—Three additional letters are selected at random, for example, PQR.

4th step—The letters PQR are enciphered at the initial (apparent) setting ABC. Suppose this gives XYZ.

5th step—The external indicator is written down as ABCXYZ.

6th step—The operator then resets the rotors to the alignment PQR and enciphers the message at the initial (apparent) setting PQR.

¹It is this element which greatly increases the difficulty of solution. Were it not for the daily changing plugging arrangement in each cryptonet the problem would be quite simple. The GA and GAF E machine has a plugboard with positions for 13 reciprocal pluggings but as a maximum only 10 of them are used at any one time. (In the Brown cryptonet a maximum of 6 steckers is used.) One might raise a question as to why this should be the case. The answer seems to be that apparently with typical thoroughness the Germans made a study of the matter and developed the fact that the maximum number of possible combinations is greatest when only 10 steckers rather than all 13 are employed. At the end of this report will be found a technical note on the subject.

DECLASSIFIED

Authority NND 963016By Wp NARA Date 6/6/03

SECRET

Now to explain the nature of the "cillies" and how the study of receipts helps in spotting them. Suppose that a first message has been transmitted and that the preamble (or the receipt) therefor consists of the following: 1725/157/HQRIPT. The 1725 is the time of origin, the 157 is the letter count, and HQRIPT is the indicator. Suppose that the next message sent by the same station shows the preamble: 1810/201/QCANPT. Let us assume that the cipher operator at the beginning of the encipherment of the second message did not follow the instructions relating to the selection of 3 letters at random for the initial alignment of the rotors (third step above) but instead used as the initial alignment the very letters showing through the key-wheel windows of the machine at the end of the encipherment of the first message. In this case (assuming this to be true) the letters aligned at the bench mark were QCA. Since the first message had 157 letters, then deducting 5 letters for the discriminant, one can count back 152 places from QCA (taking into account the nature of the motion of the rotors) and get, let us say, the letters QWE, which would mean, in the case of the first message, that in the third keying step (selecting three more letters, at random, to encipher at the random-selected base) the cipher operator must have selected the letters QWE. That is, in the indicator for the first message (HQRIPT), the letters IPT are the cipher equivalents of QWE at the setting HQR. But how can one be at all certain that this is true? It is after all, only a chain of reasoning based upon a bald assumption and the assumption may be unwarranted. However, there are indications that the assumption is not wrong! Note these letters QWE; they are not at random. They are, in fact, the first 3 letters at the extreme left in the topmost row of the keyboard of the cipher machine. That is, here is a good indication (not a proof by any means) that the cipher operator, instead of actually selecting 3 letters at random as instructed, might have fallen into a habit of following simple paths on the keyboard: QWE is a very easy path to select; so is any one of the following: QAY, XDR, HGF, ZHN. In fact, any 3 letters which are in some sort of a sequence or fall into some sort of definite pattern lend themselves readily to the methodical minds of the German cipher operators, so that they easily are led into foolish habits in this respect.¹ Another

¹In one case, I was told by our Captain Johnson, a certain German cipher operator used in sequence the following "random" 3-letter groups for enciphering 8 successive messages: PAW, RDX, VGZ, IJN, MKO, UHB, CFT, ESY! Note the route by following these letters through the keyboard diagram.

Q W E R T Z U I O
A S D F G H J K
P Y X C V B N M L

DECLASSIFIED

Authority NND 963016
By wp NARA Date 6/6/03

SECRET

type of habit indulged in very frequently by a German cipher operator, in regard to step number three above, is to select 3-letter words, simple proper names, the initials of his very best girl, or the first 3 letters of her name, etc. Some of the cipher operators, especially in the GAF, are particularly addicted to habits such as these. Some cipher operators, at the end of the encipherment of a message part, may merely shift the rotors one or two notches forward or backward and use this setting as the external message indicator for the next message part. This is a bit more difficult to identify than an ordinary "cillie" but often it is still possible to identify these cases.

As noted above, if QWE was actually the alignment of the rotors at the beginning of the encipherment of the first message, this means IPT represents the encipherment of QWE at the setting HQR. This, of course, is cryptanalytic information of considerable value in solution because it aids in the setting up of "menus". More than that, it aids directly in eliminating certain wheel orders and also affords a basis for "ringstellung" assumptions. Just what this means would require considerable explanation, and is beyond the scope of this report.

In connection with the search for reencipherments, which are necessitated by the multiplicity of keys, the log readers know that each "fliegerkorps", for example, has its own key and if a message has to pass from one "fliegerkorps" to another it must be reenciphered. The log readers, knowing the composition of the GAF thoroughly, and being familiar with the habits of cipher operators of the nets which the log readers specialize on, know when to expect reencipherments and make a search for them by closely studying the logs. The time of origin and length of message are guiding points in this search.¹ Suppose one of the messages is in a key that has been solved, the other in an unsolved key. It follows, of course, that having the text of the solved message immediately gives probable text for the other in the unsolved key, and this soon leads to the solution of the second key. It may and occasionally does happen that a single solved message forms the initial link in a chain of reencipherments leading to the solution of a series of three, four, or more keys. Immediate word concerning suspected reencipherments is passed by the log-readers to the fusion room.

¹All reencipherments show the original time of origin.

SECRET

DECLASSIFIED

Authority NND 963016

By Wp NARA Date 6/6/03

SECRET

Reencipherments are more frequent at the beginning of the month, when a new key list goes into effect. Frequently one station fails to get the new list in time and must use the key for the preceding day. This, of course, gives the solution of the same message when it must be passed to another cryptonet but in the new key.

In the log reading section careful study is made of the message indicators and the discriminants in connection with the clarification of "duds", that is, messages having wrong indicators. For example, in the week of May 4, there were 352 duds; 214 of them were cleared up by studying the logs and noting the corrections that could be made from such study. Often they find that the call signs, discriminant, or indicator shown on the intercept have been garbled, and a simple correction leads to solution. Up to 1000 duds have been handled a week in this way, 60% of them being cleared up by the log readers.

The log readers must report the presence of what they suspect may be routine messages, that is, messages sent at a rather fixed time of the day and having characteristic lengths. Because such messages are usually stereotypic in their composition they afford excellent cribs. When such routine messages are suspected or noted the information is at once turned over to the fusion, research, and watch rooms.

The log readers also report anything new that they may note, such as changes in the volume of the traffic, the disappearance of old stations, the appearance of new stations, and changes in the stations which act as net control stations. However, it was stated that inferences of a tactical or strategic nature are no longer drawn from these observations since the information yielded by solving the messages is always much more reliable than any T/A inferences. There was a time, in the early days before the British were able to read much of the traffic, when T/A information or intelligence of the "inference" type was used to a large extent and was later found to yield erroneous information because the Germans were very skillful in regard to deceptive measures. In one case, after solution, it was found that the traffic was almost entirely "spoof" or practice, and that the British had been completely misled by relying upon the inferences drawn from T/A alone.¹ In this connection I may

¹The way in which one of the most experienced people at BP put the matter to me is very interesting. He said: "W/T I, that is, information, intelligence, or inference based solely upon W/T studies is of doubtful value nowadays but I W/T, that is, information or intelligence concerning the enemy's W/T network and procedures is extremely important."

DECLASSIFIED

Authority NND 963016

By Wp NARA Date 6/6/03

SECRET

add that in the early days after solutions were forthcoming the log readers did not see the decipherments and were not let in on the secret material but that this was found to be unsatisfactory. Now they are shown such messages as might be of direct value in their work but only those which contain information that is positive in nature, coming directly from the messages themselves. This is so that the log readers may not be misled or influenced by mere deductions from decipherments.

In the log-reading room are large charts outlining the various cryptonets, showing the location of each control station and its out-stations, the cycles and rows and frequencies used, etc. These charts are kept with up-to-the-minute accuracy. When the location of a station is unknown or doubtful, D/F information is applied and is of substantial aid. The bearings obtained have been found to be accurate for stations in France, but poor for those in Norway and Russia. Lines are also drawn on these charts, showing what stations pass messages, the direction of the messages, their number, etc. Comparison with the previous chart in each case shows when new stations come up or old ones disappear.

There is also maintained an index called "Index by cycles and rows" which shows for each frequency the cycles and rows used by stations employing that frequency together with other pertinent information. These data come, of course, from the call-sign books from T/A studies, and from the charts of the communication networks. This index is useful in reconstructing the call-sign books by permitting the equating of rows and columns in the book. It was stated that by this means over one half of the "B" or "bird book", which is used by the GAF, had been reconstructed before a copy was captured in Lybia in November 1941. (The "B" book is still in effect, although references have been found, in recently solved messages, to a new "C" book which may soon come into use.) As regards the books used by the Army, the "D" or "Dog" book was in effect from the beginning of the war to 1941 and was superseded in the spring of 1942 by the "E" or "Elephant" book. At present both "E" and a new "F" book are in effect. The "F" seems to be a rearrangement of the contents of the "E" book and the rearrangement, as might have been expected, is systematic. The nature of the rearrangement has just recently been ascertained, with the result that a complete reconstruction of the "F" book is expected within a very short time.

The log readers work up the information resulting from their study of the logs on sheets which are called "proformas".

SECRET

DECLASSIFIED

Authority NWD 963016

By Wp NARA Date 6/6/03

SECRET

These go to the fusion room together with general notes and indications made by the log readers as to links with other groups.

Each log reader makes up a weekly report which is assembled with the reports of other log readers and from them is made up the complete report of the log reading section. The daily reports of the log readers are merely amendments gotten out each day to the previous week's report and show the main changes that have been noted for the day. The data contained in one copy of the weekly report are cut up into small sections and pasted on cards in order to keep an up-to-date card index showing the history of each frequency, the discriminants, the calls, etc., encountered on the frequency.

D. The "Fusion Room"

As noted above, the log readers' proformas go to the fusion room for study in connection with the decipherments of the messages passed on each circuit. The personnel of the fusion room consists of the heads of the various E log-reading groups, plus a few others as assistants. The fusion room is the directing center, in fact, for the work done by the log readers. It is within this room that the information supplied by the log readers, the T/A information from the decipherments of messages, the information supplied by the intelligence people in Hut 3, the T/A information from Major Gadd's Research or Message-Analysis Section, and T/A information from various other groups at BP are "fused" into a complete picture of the communications of the GA and GAF, with the result that the fusion room, in turn, feeds back information to all the groups sending it information, viz., the cryptanalytic people in Hut 6, the log readers, the intelligence people in Hut 3, the T/A people under Major Gadd, and, finally, the people controlling the intercept. This is extremely important and a few more details may be useful.

There is, of course, a complete interchange and exchange of data among all the groups mentioned above, by means of the fusion room. For example, a copy of the original German text of every solved message having T/A information goes to the fusion room. The fusion room checks the call signs and correlates them with the unit designations, the known locations of the latter, and so on. The routing of messages is carefully traced and diagrams of the actual working of the radio nets are drawn up, these being naturally of use to the intelligence

SECRET

DECLASSIFIED

Authority NND 963016

By Wp NARA Date 6/6/03

SECRET

people in Hut 3, to the intercept control people, and to the cryptanalytic people in Hut 6. As a result of an intimate knowledge of what each cryptonet does, its methods of operation, the specific routing of its traffic, etc., messages which because of difficult intercept conditions lack indications as to origin or destination can be handled successfully. This is an important function of the fusion room. By studying the texts of solved messages in the light of the T/A information they contain, they add data of a T/A nature to their stock and at the same time furnish information of cryptanalytic value to the cryptanalytic parties. The latter, in turn, by means of their solutions help the fusion room people. Thus, information of use to all the groups concerned is "snowballed" and rolled up into one large mass.

The fusion room prepares a daily report giving all the significant changes in radio activity noted. A weekly report is made based upon the daily reports, and a summary of its contents, published weekly, constitutes the "Central Party Report" already mentioned. There is also a composite daily report based upon not only the information coming from the study of deciphered messages having a bearing upon the communication system but also upon the deductions of the log reading sections. A summary of this composite report is issued weekly.

A copy of the original German emended text of every deciphered message is provided for the fusion room by the "watch" on operational keys. These messages are in chronological order and form the basis for the search for reencipherments by the log readers. They likewise form the raw material for studies having as their object the learning of all that is possible to learn about the general content and character of the traffic in each cryptonet, the various methods of routing messages, the identity of specific individuals and units, their locations, etc. All this information is extremely useful to the Watch on operational keys, to the intelligence people in Hut 3, and to the cryptanalysts.

The following is a list of the various reports coming to or leaving the fusion room:

SECRET

DECLASSIFIED

Authority NND 963016

By wp NARA Date 6/6/03

SECRET

A. Incoming reports:

- (1) "Intercept Station Activity Reports". These give detailed information on the activity of each cryptonet.
- (2) "Intercept Station Weekly Reports". These contain general information summarized from the daily activity reports.
- (3) "Weekly Watch Reports". These deal with crib information derived from the week's traffic on each cryptonet.
- (4) "Research Party Reports". These contain information put out by Major Babbage's Research Party and deal largely with new cribs, new tricks, etc.
- (5) Summary of decipherments and decodes from the Air Section under Mr. Cooper.

B. Outgoing reports:

- (1) "Weekly Report on WT/I."
- (2) "Daily Report on WT/I"—showing changes in weekly report.
- (3) "Weekly Report on WT/I Information Disclosed by Study of the Decipherments of Messages."
- (4) "Weekly WT/I Report From Middle East".
- (5) Special Reports. These are intermittent and deal with subjects of special interest.

The main effort of the log readers and the people in the fusion room is made during the day shift. There is a small watch in the evening and at night but active work in log reading is done only during the day. Any important plain language bit that might be noted by an intercept station is phoned directly from the intercept station to the fusion room for immediate action, if this is indicated by the nature of the intercept. An excellent illustration was given me in the case of a message sent at the end of the Tunisian campaign. The story is as follows:

DECLASSIFIED

Authority NND 963016

By wp NARA Date 6/6/03

SECRET

About 2 a.m. one morning around May 7, an operator at the RAF intercept station at Chicksands intercepted a plain-language message (English) on a "Chaffinch" frequency. It read something as follows: "To the G.O.C. American II Corps and the G.O.C. British VIII Army: In _____ (a cove in the bay of Tunis) there is a ship with British and American prisoners of war locked in the hold. The officer having custody of the key thereto cannot be found. Do not bomb this ship as you do not want to kill your own men. From C-in-C of Axis Forces." This message was phoned immediately by the supervisor at Chicksands to the intercept control officer at BP, who in turn notified the Intelligence Group in Hut 3. The latter shot a message immediately via BP's own transmitter to North Africa, with the results that the bombardment of this ship was stopped within a very few minutes. Only one man was killed and one injured as a result of this quick communication. I cite this incident to show how well organized the communications system for BP operations really is. Incidentally it is interesting to note that the German Commander must have assumed (and correctly) that the British were listening in on that German frequency!

The training course for log readers is conducted under Lieutenant Colonel Lithgow at Hampstead and consists of five weeks. Most of the personnel selected for this work are high-grade, university people. I was not able to visit this training center but no doubt we could obtain a syllabus of the course of instruction given there if we do not already have it.

V. Cryptanalytic Research

The Cryptanalytic Research Party is under Major Babbage, who is a "don" (= our "professor") in mathematics at Cambridge, and is the son of a very famous mathematician. He has under him a staff of 9 people, 6 men and 3 women, all civilians. Although the workers in the various operating sections are constantly on the lookout for new tricks or procedures that may be helpful in solution, the principal function of the research section is, of course, to concentrate endeavors to seek out anything new which may help in the solution of the traffic. However, it also has a primary responsibility in connection with the solution of the non-operational or "research" keys.

Major Babbage began by discussing the E machine,¹ having

¹The machine and the wirings of the rotors are identical in the GA and GAF. We have two exemplars at Arlington Hall, one provided by the British, the other by our Colonel Hayes, in North Africa. Both were obtained by capture.

DECLASSIFIED

Authority NND 963016

By wp NARA Date 6/6/03

SECRET

a model before him, but as soon as I told him that I was familiar with it, he passed on to further matters.

He indicated that the current methods of solution are four in number, or rather that they are based upon four special circumstances. These are the following:

- (1) The existence of "cribs". A most complete and detailed study is made to locate any new cribs. He emphasized the fact that the "constatation" or series of plain text-cipher equivalents indicated by a crib must be 100% perfect, otherwise no solution can be reached by the bombe. In other words, if a crib is 30 letters long every one of the 30 pairs of letters involved must be absolutely correct as the bombe cannot make allowance for a single-letter error. This fact means that the interception must be 100% correct in the case of the crib text and that such intercept requires excellent control not only to insure that the crib message is obtained but also that it is copied correctly.
- (2) "Cillies". These he explained with an example or two.
- (3) "Nearnesses". This refers to the phenomena resulting from the choice, by German cipher operators, of an internal machine setting which is near the external setting, and will be explained below.
- (4) "Ringstellung giveaways". These will be explained below.
- (5) "Psillies". This is an abbreviation for what they call "psychological cillies". For example, when they come across an indicator such as ROMXLV, they assume that the internal 3-letter group, which has been enciphered to form the external 3-letter group constituting the second half of the indicator, are the letters MEL, making the word which the operator has in mind when he made up the indicator the name Rommel. Other cases: TOBKST - TOBRUK; ARNUVL = ARNIMX. These "psychological cillies" are, of course, very much like the ordinary "cillies" and serve the same function in the solution of a key. They cut down on the number of wheel orders that must be tried and also on the number of ringstellung assumptions. In addition, of course, they provide data for "menus".

SECRET

DECLASSIFIED

Authority NND 963016

By Wp NARA Date 6/6/03

SECRET

At first, of course, the Germans used the same wheel order throughout the day on a given cryptonet, but in October 1941 the GAF introduced a change in this respect: at the end of twelve hours they interchanged the rotors on extreme left and right. However, no similar shift was made in GA practice. In May 1942, the GAF introduced a further step in this respect by making a change at the end of every eight hours. The GA adopted this new procedure at the same time. To give an example, suppose that the first wheel order, for the period 0000 to 0759 hours is I.II.III. The second wheel order, for the period 0800 to 1559 hours becomes III.I.II, and the wheel order for the third period, from 1600 to 2400 hours, becomes II.III.I. In other words, the rotor on the right is shifted to the extreme left at the end of each 8-hour period.

Major Babbage stated that at first the cryptanalysts depended almost entirely upon the presence of "cillies" for solution and they still do in cases where they have no cribs or where a new circuit comes up and the crib situation is entirely a blank.

Another source of information of considerable help in solution lies in what the British call "nearnesses". Suppose that a cipher operator, after selecting the external message indicator, calculates what the position of the rotors will be after enciphering three letters and proceeds to use these three letters as the interval indicator. (Some of the cipher operators may shift the rotors one or two notches forward or backward.) Thus the external indicator becomes very "near" the actual or internal indicator.

One additional source of help in solution lies in what the British call "ringstellung giveaways" and results from the laziness of some German cipher operators when setting up the machine for the first time in the day. This refers to the "ringstellung" or position of the rotatable ring controlling when the next rotor will step for each rotor. Having set the rotors in the required order, the cipher operator, instead of taking the rotors out to fix the ringstellung on each one, simply reaches down into the aperture, sets the ring on each rotor, and leaves the rotors in that position for the first message which he is going to encipher. That is, the initial horizontal alignment of the three rotors which is indicated by the first three letters of the indicator of the first message for the day will very often tell the ringstellung for the day. His failure to change the rotatory positions of the rotors after setting the ringstellung thus gives direct information as to the actual

SECRET

DECLASSIFIED

Authority NND 963016

By wp NARA Date 6/6/03

SECRET

ringstellung itself. By observing the indicators for a number of initial messages in the same cryptonet, very similar indicators on these messages will limit the ringstellung possibilities to a considerable degree. This makes it very important to be sure to get the first message in each cryptonet for by studying them the British are given clues to the ringstellung for the daily key on that cryptonet.

Another feature of GA and GAF cipher operations of considerable help in solution arises as a result to German misconceptions as to what "randomness" in cryptography really means. When it comes to drawing up the steckerung for the daily change in plugging the Germans avoid two things:

- (1) They apparently feel that it is unwise to repeat a stecker on two successive days. For example, if A and K are connected together today, they positively will not be connected together tomorrow. Indeed, this principle is extended in some cases to a point where repetition of steckers is avoided until all pairings have been made. This is, of course, of very great assistance in solution when the principle is carried to such lengths. German methodicalness is here again at the bottom of a very foolish cryptographic habit.
- (2) The GAF cipher compilation office apparently feels that it is unwise to connect any letter to the next in alphabetic sequence. For example, A and B are never connected, B and C, C and D, and so on. In fact, this is so certain that the British have introduced a special modification in their bombes called "Consecutive Stecker Knockout" or "CSKO", which takes advantage of this fact in bombe operation. If a "stop" or possible solution is reached which would require the steckerung of two alphabetically consecutive letters, the bombe automatically eliminates such a stop. Thus the number of false "stops" is materially reduced.

Major Babbage then showed by example how "menus" for the bombes are constructed, and discussed the general principles of the operation of the bombes.¹ (These fall outside of the scope of this report.)

¹The term "menu" refers to the "constatation" or set of plain text - cipher and cipher - plain text conditions set up on the bombe. These determine when the machine reaches a position at which the encipher-decipher conditions corresponding to the crib are satisfied, thus yielding a possible solution.

DECLASSIFIED

Authority NND 963016

By wp NARA Date 6/6/03

SECRET

He stated that they had been noticing a gradual improvement in the discipline of the GAF cipher operators and the problem was becoming more difficult every day. They are now noticing, in deciphered messages, rather frequent instructions to avoid stereotypy and stereotypic reports. Moreover (and this is a very important point) on some cryptonets, instructions have been given to insert "padding" at the beginning of the messages.¹ This, of course, makes the locating of a crib more difficult. The length of the padding varies, but in some cases it may run from 25 to 30 letters. I saw one case where the padding consisted of a single German word, but this word contains 41 letters: "Donaudampfschiffahrtsgesellschaftskapitaene".

Another thing which is causing some worry is the tendency to bury the addresses and signatures of messages. Whereas up until recent months these elements of a message were almost invariably at the beginning or at the end and thus afforded excellent cribs, the addresses and signatures are now being inserted within the body of the text, making their location much more difficult.

Major Babbage's group also does research in connection with the solution of "Rocket" traffic, that is, the messages dealing with railway movements. The Railway E machine has different wirings from the GA and GAF machine. In addition, the Umkehrwalz, or reversing rotor, is rotatable and forms a part of the series of stepping rotors. It advances one step in 26³ movements but, of course, the exact moment when it will advance depends upon the turn over point on the wheel to its right. In addition to the Railway E machine, research is, of course, done on the machine used by clandestine groups of the "ISK" series.² (To be discussed in another report.)

One of Major Babbage's leading assistants is a Dr. Aitken, who is the chess champion of Scotland. At the time I talked

¹At present there are only two cryptonets which use this procedure: "Mustard" (the German "Y" Service communications) and "Locust". However, during the African Campaign it was used by several GA cryptonets there, viz., Bullfinch, Chaffinch I, II, and III, and Phoenix.

²An exemplar of the "ISK" machine was captured by our forces in the Torch operation in North Africa. It was used by the German Armistice Commission there. It is now in custody of the British at BP and should be obtained from them.

SECRET

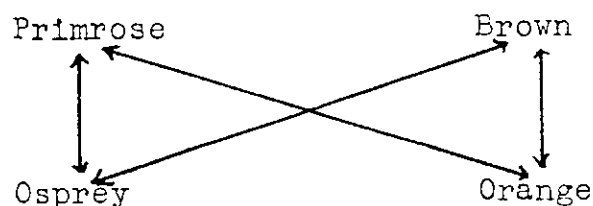
DECLASSIFIED

Authority NND 963016
By wp NARA Date 6/6/03 SECRET

with Dr. Aitken he was engaged in solving "by hand" a key on the "Brown" cryptonet, which is used by the German radar stations in northern France. As indicated in another place in this report, the people who are on this cryptonet are not very good cryptographers and, moreover, instead of using 10 steckers each day they use only 6. The messages are, therefore, solvable without going through the bombe operation, for a key can be obtained by using a hand-operated E machine modified for the purpose. This machine is very much like our own hand-testing Enigma machine and the principle of operation is, of course, the same. However, I was told that in some cases they solve the Brown key by tying together two such machines in a certain way so that when the proper steckers are assumed they get a lamp illuminated with a double brightness, indicating that current is going through both machines. This happens when the correct stecker is tried.

It was emphasized by Major Babbage how much more careful the GA cipher operators are in the use of the E machine than are those of the GAF. The traffic of the former shows few or no cillies, no stereotyped beginnings or endings, etc.

Another interesting thing I learned was that recently the person who makes up the key lists for the GAF cryptonets has become lazy and combines the steckerung set-up for one month with the wheel order and ringstellung positions for another month, giving what the British call a "quadrilateral". The result of this practice is to facilitate the solution of four keys. For example, it was found that in one case four keys were related as shown in the diagram below:



There was a bit of discussion as to the future. Major Babbage feared that if the present tendency to tighten up on the usage of the E machine were to continue, if cribs became more and more difficult to find in the GAF traffic, and if the addresses and signatures were going to be buried he could foresee the end of their current type of operations.

DECLASSIFIED

Authority NND 963016

By 46p NARA Date 6/6/03

SECRET

This, he stated, makes it very important to try to find new methods of solution not dependent upon cipher operators' habits and blunders. They themselves have been thinking about this but have not thus far been able to devise new methods of solution based upon pure cryptanalytic or statistical methods, were frank to admit this, and are looking forward to obtaining help from us.

My impression is that the people engaged in E cryptanalytic research are gifted, if not brilliant, investigators but their knowledge of cryptanalytic techniques in general, and of the history of cryptanalysis is not of the highest calibre. They know very little about modern high-speed cryptanalytic mechanisms and apparatus, except IBM. In matters of terminology and good nomenclature they show themselves to be rather whimsical, somewhat illogical most of the time, with no clear concept of the relations between various cryptanalytic systems and methods, nor of the accurate, descriptive terminology that may be used to describe them accurately. But nothing I can say in these respects could possibly dim the brightness of their remarkable, if not astounding, achievements in the E field.

VI. The Cryptanalytic Operational Watch

The chief of the "Watch" is Mr. Milner-Barry, a well-known British chess player and "chess editor" of the London Times. He is deputy to Mr. Welchman and has been on the job since May 1940.

Cryptanalytic operations on E traffic fall into two rather distinct categories. The first deals with what they call "current" or "operational" keys, the second, with what they call "research" keys. These change somewhat from time to time.

At the time of my visit the operational keys of the GAF and GA were as follows:

A. GAF keys:

- (1) "Red". This is the main GAF key used in common by all the principal stations and headquarters of the GAF. It yields by far the greatest volume of important messages.
- (2) "Locust". This deals primarily with GAF supply and administrative communications of an air force group in Sicily and Sardinia.

DECLASSIFIED

Authority NND 963016

By Wp NARA Date 6/6/03

SECRET

- (3) "Primrose". Similar to "Locust" but for the Mediterranean Area and Greece.
- (4) "Snowdrop". Similar to "Locust" but for France.
- (5) "Hedgehog". Similar to "Locust", but for South Russia. It is interesting to note that this key gives the British battle order information relating to German forces in the Russian front, information they are unable to get from the Russians themselves.
- (6) "Lobster". Similar to "Locust", but for the Norway area.¹

B. GA keys:

- (1) Chaffinch I. General army forward area.
- (2) Chaffinch II. General army middle area.
- (3) Chaffinch III. General army back area.
- (4) Bullfinch. Tunisian Army
- (5) Phoenix. Panzer Army
- (6) Goldfinch, Hawfinch, Bullfinch II. These were subsidiary keys used by the German Army in Tunis and were not all in simultaneous operation.

The Watch on the operational keys consists of five principal jobs, the nature of which will be outlined.

The "Number 1 man". He is known as "IC-OPS" [i.e. "in charge of operations"]. He looks after the preparation of the menus to be sent to the bombes and directs processing priorities. He is also in charge of the Watch if there is no chief or Duty Officer specifically assigned. He does not necessarily make up the menus himself, but determines what menus shall be sent to the bombe control people and the order in which they shall be sent.

¹After May 15, 1943, "Snowdrop", "Hedgehog", and "Lobster" carried "Red" traffic and became important operational messages because the Germans believed "Red" to have been compromised with the fall of Tunis.

Page 43 is missing from the NARA record.

DECLASSIFIED

Authority **NND 963016** **SECRET**
By **wp** NARA Date **6/6/03**

insure that they get up-to-the-minute-information as to cribs. In addition to entering in a register everything that he recognizes as a well established crib, he must also be on the lookout for any new cribs and for reencipherments. I saw the various books in which the cribs are kept, together with most minute, detailed information indicating where they were found, frequency, calls, etc.

The "Number 3 man". His job is to locate the reencipherments by systematic search through the traffic, by a process known as "looking for kisses".

As indicated before, one of the features of practically all the reencipherments is that they carry the same time of origin in the preamble and are approximately of the same length. There are so many messages on each of the operational cryptonets that the only way that reencipherments can be spotted is to compare all the times of origin of all of the messages in the various operational cryptonets with which the Watch deals. To his desk come little squares of paper on each of which is noted the time of origin and a reference number for each message comprising the traffic in each of the operational nets. By sorting the slips and comparing those with the same time of origin this man can often come across cases when two slips indicate that there is a possibility of a reencipherment. Accordingly he marks such slips with a cross: hence the derivation of the term "kisses". Having selected the slips with the crosses he then must decide which are in fact reencipherments or are likely to be, from his background of knowledge of the circuits involved, the frequency with which reencipherments are to be expected, etc. Then if he gets a case which appears to be favorable he must work on it and see what he can do with it. The normal procedure in testing for reencipherments includes deciphering one of the messages as soon as the key has been found, and noting whether its contents are really such as to make it likely that it would be relayed to another cryptonet. The Number 3 man consults very frequently with the IC-OPS and the former's work materially aids in giving the latter a good basis for decision as to what menus to send the bombe first.

The "Number 4 man". He is called the "registrar" and looks out for "cillies". He has a register before him which gives the preambles of all messages in the operational keys. These afford data for the type of computation involved in establishing the presence of "cillies". His work has a direct bearing on the job of the IC-OPS because it affords definite

SECRET

DECLASSIFIED

Authority NND 963016By wp NARA Date 6/6/03

SECRET

information as to what wheel orders to select for trial and their order of priority. If solution does not come out on the limited number of wheel orders tried the inference is that the cribs have "gone down", that is, they have changed. If the "cillie" is a "strong" one they will stand by it and will try a second or possibly a third crib on this same color until they are sure that the crib is not there at all and must try something else. The Number 4 man keeps in close contact with the IC-OPS, for it is possible to make up a menu entirely of "cillies". I was told, for example, that in some cases they could make up a menu upon a half dozen "cillies" alone.

The "Number 5 man". He is called the "odd man" and is available for any of the jobs in the Watch. He may act as an understudy for the IC-OPS, whose job is very difficult and requires concentrated attention. The IC-OPS may not have time to attend to the cribs of all of the operational cryptonets and therefore he may select only two, Red and Lobster, for example, leaving the odd man to take care of the others. The odd man may help with the location of reencipherments, help to sort out the slips and locate "kisses", or try to decide which are good possibilities for reencipherments located by the Number 3 man. When there are a great many slips the Number 3 man may not have enough time to take care of all of them and have to sort out certain ones. In this case the odd man may help out. The latter may also have to help the "registrar" and in some very favorable cases can actually assist in breaking a key by hand if a particularly good ringstellung and wheel order are indicated as a result of his study of "cillies". For example, on the day I visited the Operational Watch (see next section) I heard the registrar say to the odd man, "Have a go at breaking Locust by hand today. It looks good."

On the afternoon of May 18, I had the opportunity of observing operations in the Watch for about two hours, and a few of the highlights will be related.

The Duty Officer on the Watch on this shift was Captain Monroe. He stated that the "Red" key came out very quickly that morning. The proper crib message arrived at 9:00 and by 11:00 they had the key. They were fortunate in that the most probable wheel order assumed by them from basic data turned out to be correct. On the other hand, yesterday's "Red" was quite difficult and only came out today; the reason being that there were two very similar messages both of which appeared to be

SECRET

DECLASSIFIED

Authority NND 963016

By wp NARA Date 6/6/03

SECRET

the proper crib messages and they had to select one of them. Unfortunately, they selected the wrong one. I found, also, that yesterday's "Primrose" key was still unsolved whereas today's "Locust" key, which was a 60 wheel order job, was completed at 10:00. At the moment, they were still working on yesterday's "Locust" key. The crib on the "Locust" key, at the moment, is one of about a hundred letters in length, known as "Fluzmittelmeer".

Last month it was noted that "Foxglove" and "Snowdrop" used exactly the same keys but with different discriminants, and the same phenomena is true with respect to this month's traffic in those two keys. The result of this observation has been that now all keys are tried on all the traffic, since there is no way of telling whether the same keys are used in two or more different cryptonets. This might, of course, be an indication of the beginning of a real disintegration in German cryptography.

It was interesting to be told that on "Lobster", which has a rather wide distribution, solution has been made possible by a crib coming from a certain station in Norway, the message dealing with a very simple stereotypic report of signal strength.

On every cryptonet they maintain a register showing on what basis the key for it was recovered for each day in the month. I thought it would be interesting to copy what that register showed for the "Red" cryptonet for April, 1943. It is as follows:

- April 1: "Chef" crib. This is a well-known, fairly lengthy crib beginning with the words "An Chef...".
- April 2: "Gruenmeldung" crib. This is a stereotypic message describing the previous night's operations.
- April 3: "Sultan's First Meldung". This is the first of a series of operational reports transmitted by the 10th Fliegerkorps and begins "Erste Meldung".
- April 4: "Gruenmeldung" crib, as on April 2.
- April 5: "Zusauf" crib. This is a collection of reconnaissance reports which begins with "Zu...".

SECRET

DECLASSIFIED

Authority NND 963016

By Wp NARA Date 6/6/03

SECRET

- April 6: "Cillies".
- April 7: Signal strength message from Norway. A stereotypic report of signal strength of messages.
- April 8: A "Locust" crib found on "Red" that today consisted of a meteorological message.
- April 9: "Zusauf" crib.
- April 10: "Norse Absichten". Stereotypic report from Norway.
- April 11: "Norse Absichten".
- April 12: "Cillies".
- April 13: "Sultan's First Meldung".
- April 14: "Gruenmeldung" crib.
- April 15: Iraklion "Numbers". This is a three-part message and the third part contains the address and signature which begins "An Funkberatungsstelle Syracuse von Funkmesztrupp Iraklion," followed by numbers.
- April 16: Norse signal strength message.
- April 17: Norse signal strength message.
- April 18: "Gruenmeldung" crib.
- April 19: A "Locust" crib found on "Red".
- April 20: "Sultan's First Meldung".
- April 21: "Sultan's First Meldung".
- April 22: "Sultan's First Meldung".
- April 23: Iraklion "Numbers".
- April 24: "Gruenmeldung" crib.
- April 25: Iraklion "Numbers".

SECRET

DECLASSIFIED

Authority NND 963016

By wp NARA Date 6/6/03

SECRET

April 26: Iraklion "Numbers".

April 27: Signal strength message.

April 28: "Sultan's First Meldung".

April 29: Iraklion "Numbers".

April 30: Muffelbericht. Muffel is the code name for a certain unit. It begins with the word "Gefechtsbericht" and is a report for the previous night's operations for the unit.

All of the cribs for April on "Red" are still valid, which I was told was rather unusual as they change more rapidly than this. There are about 400 messages a day on the "Red" and they yield information of highest importance.

It may also be interesting to list the names applied by Hut 6 to the most important cryptonets now under observation:

A. GAF Cryptonets:—

Red, blue, pink—These are general and apply to all sectors. Blue is a practice key.

Mosquito, beetle, gadfly, ermine, locust, hornet, skunk, wasp, firefly, cockroach, mayfly, lion, squirrel, badger, civet, dingo, mole—These apply to particular regions and are used by particular air force units, mostly "luftflotte" and "fliegerkorps".

Hedgehog—South Russia Army Air Liaison.

Daffodil, clover, gorse, daisy, orchid, foxglove, primrose, snowdrop, lily, tulip, narcissus—These are administrative keys used in particular regions by "luftgaus".

Celery, garlic, leek—GAF weather.

Brown—Radar groups in France.

Mustard—GAF "Y" service.

Rocket—Railways.

Orange, quince—Waffen SS.

SECRET

DECLASSIFIED

Authority NND 963016

SECRET

By wp NARA Date 6/6/03

B. GA Cryptonets"—

Merlin, Falcon, Mallard, Osprey—These are Army general keys.

Greenshank—Central region of Germany.

Vulture, Kite, Rook, Robin—Eastern Front.

Raven, Buzzard—Balkans.

Albatross, Cormorant, Sparrow, Phoenix, Chaffinch, Bullfinch, Goldfinch—Mediterranean.

Blackbird—Holland.

Gannet—Scandinavia.

The actual cryptanalytic processing operations will next be described.

SECRET

DECLASSIFIED

Authority NND 963016

By 4p NARA Date 6/6/03

SECRET

VII. . OPERATIONS UNDER MR. FLETCHER

A. GENERAL

The cryptanalytic processing sections¹ under Mr. Fletcher comprise the following sections:

- (1) Watch Registration.
- (2) Research Registration.
- (3) Registration School.
- (4) Bombe operation, control and testing; "duds" and Railway E or "Rocket" traffic.
- (5) "Decoding" of traffic.
- (6) "Decoding" School.

The foregoing sections will be described in turn. Before doing so it is necessary to explain how the messages are first separated into the operational and non-operational keys, noting that Watch Registration does the sorting and handles the former, while Research Registration handles the latter.

B. WATCH REGISTRATION

a. The Flow of Traffic and the Identification Party

As indicated in the preceding section, the traffic is primarily broken down into two sorts; first, the current or operational messages, the solution of which must be speeded up as much as possible; second, the non-operational or "research" messages, which may be left for the next day or thereafter, whenever the keys can be worked out. The following diagram gives a rough picture of the flow of traffic.

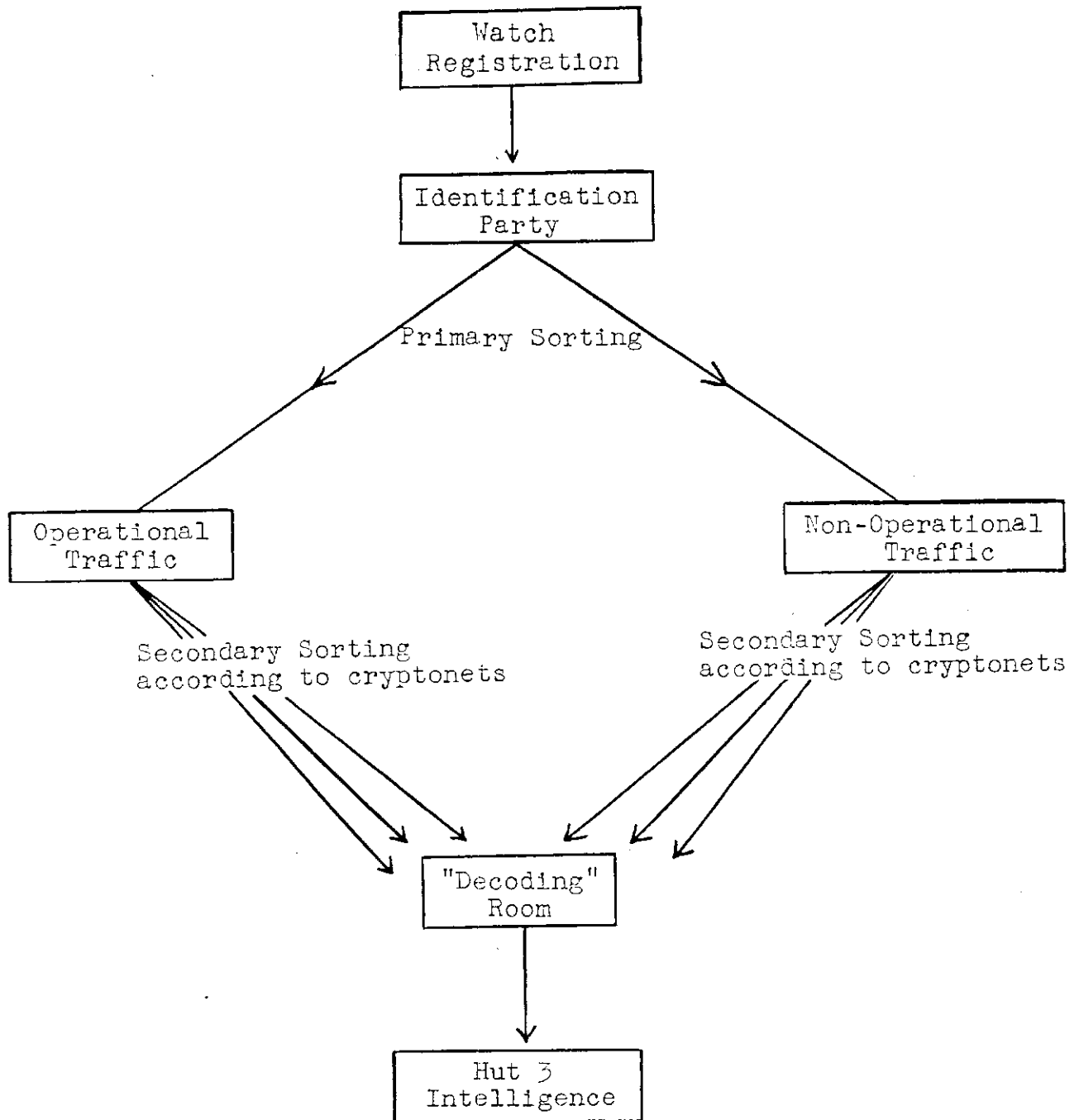
¹These sections, while operating under Mr. Fletcher, really operate for the Watch, which is under Mr. Milner-Barry. This is shown on the diagram accompanying page two by the dotted lines.

SECRET

DECLASSIFIED

Authority NND 963016
By wp NARA Date 6/6/03

SECRET



DECLASSIFIED

SECRET

Authority NND 963016By wp NARA Date 6/6/03

In the Watch Registration basically two things are accomplished. First, they pick out the current or operational traffic, which must be processed as fast as possible, and put the remainder in chronological order by intercept stations. Their second job is to register the preambles of the messages on a special list called a "blist"¹. The process is called "blistening" and it is done by women who are called "blisters".

In the Watch Registration there is a group called the Identification Party, whose function is to indicate on each message the cryptonet to which it belongs, using the "predictions" which have been furnished by Mr. Coleman's section. As stated before, the intercept stations send by teleprinter to BP and in a continuous stream the preambles to the E messages. The women in the Identification Party do the primary sorting. As a result of their labors the traffic is thus quickly sorted into the current or operational and the non-operational or research keys. The former go to Registration Room No. 1 for "blistening" and a further sorting according to cryptonets. As soon as the solution or key has been obtained for each cryptonet, the accumulated traffic in each key is passed to the "Decoding Room".

The research or non-operational traffic goes to "Research Registration" or Register Room No. 2, where "blistening" takes place according to time of origin order. It remains there in a "Research File" until the keys have been solved, whereupon the messages are sent to the "Decoding Room".

In the case of messages which cannot be classified into the cryptonets or into operational and non-operational keys, a separate register is kept. This shows the data in the preamble and a blisting is made according to frequency, and then according to German time of origin.

The operational keys of the GAF and the GA which were in effect at the time of my visit have already been listed in a preceding section.

The Identification Party numbers about 25 women who work in three shifts, eleven on the day shift, ten on the evening shift and four on the night shift.

¹This is another curious name derived by the same whimsical process already alluded to. The first man who got up such a list was named Bannister so that the list was originally called a "Bannister List", then a "B-List" and then finally a "Blist". The nature of this list will be indicated later.

DECLASSIFIED

SECRET

Authority NND 963016By 4p NARA Date 6/6/03

b. Watch Registration Operations

It has been seen how the messages are primarily sorted into operational and non-operational by the Identification Party. The former stay in Watch Registration and undergo a further sorting according to cryptonets.

This second sorting is done by a young woman in Watch Registration who is known as a "discriminatrix". She has before her a chart known as a "Hanki-Panki"¹ on which the discriminants are distributed in the form of a trigraphic chart, the first two letters forming the horizontal and vertical coordinates, the third letter being inserted within the individual cell of the chart, together with an indication of the cryptonet to which the three letter discriminant applies and the frequency. (The information for this chart, perhaps the chart itself, is produced by the Traffic Research Section under Mr. Coleman.) On this chart the discriminants are arranged strictly alphabetically so that if a discriminant KAR is to be sought, one looks for AKR. The discriminatrix looks at the frequency and the discriminant shown on the message and compares them with the frequency and discriminant shown on the chart. If they coincide an indication is made in a column marked "confirmed". When two such checks have been made the discriminant and frequency predicted are considered confirmed.

If, however, the discriminant and frequency are not on the forecast list, she makes an indication in certain columns on the right of the list giving the discriminant, frequency, group count, station of intercept, and register number of the message. Such cases are then referred back to a "super-discriminatrix" in the Traffic Research Section of Mr. Coleman's group. There the case is studied in connection with the other reference data. As a result of special knowledge and experience that section is able to clear up most of the cases giving rise to difficulty or doubt.

The discriminatrix has various sources of reference such as the call-sign books, special charts showing what frequencies in the recent past have been used in what cryptonets, etc. One of such charts is called the GAF FAG, the latter meaning frequency allocation guide. This is useful in the case of air-to-ground communications where the frequencies vary all the time and are tied up with the call signs.

¹So called because the chart was originated by a Mr. Hancock.

SECRET

DECLASSIFIED

Authority NND 963016

By wp NARA Date 6/6/03

SECRET

The messages having been segregated according to cryptonets the next step is "blisting".

The messages on arrival for this operation in Watch Registration are checked off on a list against serial numbers from 1 up, beginning at 0001 o'clock. This list is known as the "Take-off Sheet" and is handled by a young woman jocularly called "the cat". On this sheet she makes a single check in one column next to the serial number. Alongside it she puts "X" if it is an operational message of the current date or "O" if the message is in yesterday's or a preceding day's key. The "Take-off Sheet" is intended merely for keeping track of the messages. On each message she writes an indication of the cryptonet and the messages are then passed to the "blisters" for "blisting". The "cat" and her assistant, who is naturally called "the kitten", must have an excellent memory and must be able to recognize instantly the discriminants and frequencies. A list of the identified discriminants for each date is instantly available for ready reference.

There is, of course, a "blist" for each of the cryptonet keys and this is broken into two parts; first, the data applicable before the key has been obtained and second, for the data after the key has been obtained.

An example of the first type of "blist" with respect to the "Red" cryptonet, showed the following items:

- (1) Number of parts.
- (2) Blist number, serially, beginning with one for the first message in that key.
- (3) Intercept station message number. There are 8 columns for this, applicable to the 8 different intercept stations taking this traffic.
- (4) The number of letters in the text.
- (5) The message indicator.
- (6) Frequency.
- (7) If marked KR (German symbol for "urgent"), in which case a check is placed in this column.

SECRET

DECLASSIFIED

Authority NND 963016

By Wp NARA Date 6/6/03

SECRET

- (8) Time of origin.
- (9) Time of interception.
- (10) Call signs.
- (11) First group of text.
- (12) Second group of text.
- (13) If sent to the "machine room" (a small section in the Watch, where they look for "cillies").¹

After the key has been obtained, the "blist" will show only the following items:

- (1) Message number on the "unbroken blist".
- (2) Intercept station symbol (there are 3 columns for this).
- (3) Number of letters in message.
- (4) Message indicators.
- (5) Frequency.
- (6) Time of origin.
- (7) Time of interception.
- (8) Whether KR or not.
- (9) Call signs.

After the "blist" has been made for each cryptonet it is used as the basis for constructing a special chart which the British call a "Foss Sheet".² This consists of a 676-cell square in which the first and second letters of the message indicator serve as the coordinates, and the third letter is placed within the appropriate cell inside the square, together

¹The name "machine room" is regarded now by the British themselves as a misnomer and the name "Watch" has been applied to the whole group of which this is a section.

²A term derived from the name of the first man that thought of making such an index, Mr. Foss.

SECRET

DECLASSIFIED

Authority NND 963016

By wp NARA Date 6/6/03

SECRET

with the serial number of the message as shown on the "blister".

The "Foss Sheet" has two purposes. The primary one is to afford data for ascertaining the probable "ringstellung" for the cryptonet for that day. The basis for this is the "ringstellung giveaway" phenomena described on page 37-38. The secondary purpose of the "Foss Sheet" is to facilitate the spotting of duplicate messages, a purpose for which it is of course easily employed since it shows the message indicators and serial number of each message in a separate little cell.

On each of the messages the "blisters" write the serial number of the message on the "blister" and, what is very important, the priority for processing it. There are seven priorities, as follows:

- (1) QWD (which is the German procedure sign for highest priority).
- (2) "A-KR"
- (3) "B-KR"
- (4) A
- (5) B
- (6) "C-KR"
- (7) C

These processing priorities are taken from a list which is furnished by the people in Hut 3 and the "blisters" must follow them rigidly. Their guide in so marking the messages is the frequency on which the message was sent; the list furnished by Hut 3 shows this frequency, together with its processing priority.

The "blister" also writes an indication on the message as to which of the three wheel-order periods is applicable.

There is also maintained a simple serial listing of all the messages on each cryptonet, this being desired for speed in ascertaining the number of messages each day on each cryptonet.

SECRET

DECLASSIFIED

SECRET

Authority NND 963016

By wp NARA Date 6/6/03

There is one "blister" for each important and voluminous cryptonet; but as regards the remaining cryptonets one "blister" may be assigned three or more of the less important or less active cryptonets.

Until the key for a cryptonet is obtained, even if operational, the messages applicable to it are kept in a designated tray.

If the intercept station notes a correction to the indicator of a previously intercepted message, the information is telephoned from the intercept station to the Intercept Control Room where the correction is written on a slip of paper which is forwarded immediately to the appropriate "blister" who enters the correction on her "blist".

There are six to seven "blisters" in each of three Watches. They are assisted by a telephonist, who has what is called the "horrors" job, that is, she is the girl who must telephone to various people when there are difficulties in connection with any message. The women who comprise the personnel in the Watch Registration are all of a high-class type. They must be quick, accurate, painstaking and of excellent memory.

Connected with the Watch Registration is the library where the current month's messages are kept in cabinets; last month's messages are kept on open shelves. Applicable "blists" are also kept in two separate sections as above. There is also a special place called "the Horrid Graveyard" where unreadable messages, that is, those which have resisted all efforts to ascertain what is wrong with them, are kept.

The total personnel in Watch Registration is approximately 40 women.

C. RESEARCH REGISTRATION

The operations in and organization of the Research Registration Room follow a pattern similar to that of the Watch Registration Room; only the pace is slower and there is not the urgency of operations as in the latter. The number of workers in both sections is about the same, their training and their duties are similar.

SECRET

DECLASSIFIED

Authority NND 963016

By 4p NARA Date 6/6/03

SECRET

In this section the messages pertaining to the non-operational cryptonets are also registered, "blists" being made as in the case of the messages pertaining to the operational cryptonets. At the time of my visit the latter type comprised about 14, the former about 55 cryptonets. Usually the research or non-operational keys are solved one to three or more days after the day they are in effect.

The "blistings" of the messages is in time of origin order. "Foss Sheets" are made to get "ringstellung" information and to isolate duplicate messages, as in the Watch Registration.

A "traffic summary" is maintained for each cryptonet for each day. This shows the discriminants, whether they are confirmed or not, whether the key was found or not, the number of messages, whether a GA or a GAF key (the two are kept on the left and right hand sides of the sheet, respectively), and so on.

From this traffic summary No. VI Intelligence School makes up daily a typed list of all confirmed discriminants for the various cryptonets.

The messages, after examination and "blistings" bear indications as to cryptonet, date, "blist" number, the wheel-order period (the 3-hour period as regards the 3 shifts of the rotors), whether a duplicate version is available, etc.

A library is maintained, just as in Watch Registration, for the proper filing of messages, applicable "blists", and so on.

The Research Registration also operates in three shifts: a day shift with 11 people, an evening shift with 10, and a night shift with 4. They are all women.

D. THE REGISTRATION ROOM SCHOOL

The primary object of this school is to teach the mechanics of "blistings". The course consists of two weeks and there are two instructors. The personnel selected as students must have a general education and a good memory. They are all women except a few men who are intended for duty in the crib room or special operations. The following is a list of texts, which are all in hand-written form however, and have been prepared by specialists at BP:

SECRET

DECLASSIFIED

Authority NND 963016

By wp NARA Date 6/6/03

SECRET

- (1) "Introduction to Watch". This is a very brief treatise on the functions of the Watch Registration Group.
- (2) "Introduction to W/T". This includes a bit about Morse and non-Morse transmission methods of sending (hand or auto) etc.
- (3) "The Enigma Machine". This deals with the mechanics of the machine enciphering and deciphering messages, the usual types of errors made by cipher operators, the common practices of cipher operators (cillies etc.), the methods of key, etc.
- (4) "How an Enigma Machine message is Made Up and Transmitted". This includes some T/A information regarding preambles and what can be derived from their study.
- (5) "The GAF W/T Communication System". This deals with the origin and basis of the naming of the various keys.
- (6) "Types of Wireless Working".
- (7) "Call Signs." This deals with the cycles and row etc.
- (8) "Discriminants." This includes practice in the identification of messages.
- (9) "Naming of Keys." This is a more detailed explanation of the data in text 5 above.
- (10) "German Army Organization". This is from the point of view of radio communications.
- (11) "The FAG System". This deals with the frequency allocation guide for forward units of the GAF.
- (12) "The Rest of Hut." This deals with the work done in other sections.
- (13) "Reencodements."

About four or five lectures are given by special personnel during the two weeks course on such subjects as cribs, the operations of the bombes, Traffic analysis, etc. After some practice in "blisting" the students are ready for actual work.

I think it would be very useful to have a copy of the foregoing texts.

SECRET

DECLASSIFIED

Authority NND 963016

By Wp NARA Date 6/6/03

SECRET

E. BOMBE OPERATION, CONTROL, AND TESTING;

"DUDS" AND RAILWAY E

a. General

As indicated in the title to this section, this is the group having several important operating functions in connection with bombe operations, their actual control and testing, the processing of "duds", and Railway E or "Rocket" traffic.

The group is composed of subsections corresponding to the duties and operations performed by each. The latter will be described in turn.

b. The Bombes and the Bombe Rooms

On May 20th I was taken into Hut 11A, the building where the BP bombes are housed, and spent about 30 minutes in one of the bombe rooms.

The bombes consist of an assemblage of 36 E's with 3 or more diagonal boards. The E's are of the rotating commutator type and are in reality, merely large, high speed, motor-driven Enigmas. Provided that there are not more than 12 elements in a menu they can run three wheel orders simultaneously on one bombe, but if the menu consists of more than 12 elements, they can run only two wheel orders at a time. It is not often that they have more than 16 elements in a menu.

It takes 35 to 50 minutes to set up the connections dictated by the menu. This includes the time to set the rotors to their initial positions. It takes 10 minutes to change wheel orders. The present rate of rotation is 60 RPM and the speed is limited by the speed of a certain relay, which is at present four milliseconds, although a new relay has been developed with a speed of one-quarter of a millisecond. I was told that with the new type of bombe it may be possible to make a complete run of 17,576 elements in 22/26ths minutes. It was pointed out, however, that because the plugging up of a machine and the time for changing wheel orders requires a minimum of 45 minutes, the rotational speed is of some moment but not of primary importance.

An experimental unit of a three-wheel bombe with a speed of rotation of 3,000 RPM is now on hand. It uses solid brushes whereas all the present bombes use wire brushes.

SECRET

DECLASSIFIED

Authority NND 963016

By wp NARA Date 6/6/03

SECRET

The bombes now in use are of two principal types, one known as the "standard", which produces no printed record and requires the operator to note down on a slip of paper the data for each stop, the other known as the "Jumbo", which automatically searches down the columns of the diagonal board and types out on a record sheet the data relating to the stop, including the steckers found. Of the 72 bombes on hand, 58 are standards, 14 are of the Jumbo type. Another modification which they have introduced into all of the standard machines and in 50% of their Jumbos is the "consecutive stecker knockout" feature referred to in a preceding section. This throws out a lot of cases where the machine will give an incorrect stop.

Mr. Fletcher is the liaison man with the two factories producing the bombes. The latter were recently on a semi-mass production basis and could complete three-wheel bombes at the rate of 12 per month. However, the production of three wheelers stopped in January and all production is now of the four-wheel type. Eight of the latter were to be delivered in June 1943 and 10 per month thereafter. They will not be of the Jumbo type but will have recording mechanisms and will print the "story" for each stop. The new bombes cost approximately £8,000—9,000 each.

It was interesting to learn that the construction of the first bombe, which was begun in December, 1939 was completed in May, 1940, taking about 8 months. The first two bombes were 30-E machines and all of the rest have been 36-E affairs. The original bombe is still in use, but only for training purposes. It was also interesting to learn that the wiring of the rotors as well as the original conception of a bombe came from the Poles in 1939. At that time there were only a few different keys and the "Red" was very widely distributed. It was stated that the situation was too good to last and soon changed.

There are about 11 miles of wire in each bombe, about 1,000,000 soldered contacts, and approximately 500 relays. All of the brushes are of the 16-strand type. There are so many things that might go wrong that it is, in fact, a continuous source of wonder to them that they work as well as they do. They run the bombe 24 hours a day, 7 days a week, and they do not have any time out for preliminary or pre-breakdown inspection. They keep the bombes going until they do break down and then take the machines apart if necessary to repair them or study them until all faulty operation has been eliminated.

SECRET

DECLASSIFIED

SECRET

Authority NND 963016By Wp NARA Date 6/6/03

Of the seven bombes at BP one is used for "ISK" work. In the case of this bombe there is one diagonal board for each set of 4 E's and this diagonal board is somewhat different from that in the other type of bombe as its purpose is to account for movement of the reversing rotor.

The bombes are operated entirely by young women who are members of the WRNS. Each bombe has two Wrens assigned to it; one is called the "operator" and another is called the "tester". When the bombe reaches a "stop" position the operator notes down the data which constitute the "stop" and hands the slip of paper to the tester, who tests primarily to insure that the machine is O.K. If so, the slip is then passed by the tester to the "testing party" in Hut 6 for further examination of the "stop". Just as soon as a valid solution has been attained all bombes on that particular problem are immediately stopped. The menus and wheel orders are prepared in Hut 6 and the data are sent to the bombe controller in Hut 11A.

In the case of the Jumbo type of bombe, where the stecker "story" is printed, the latter is tested for validity beyond the menu.

In the case of the bombes at BP, the bombe controller sends over by messenger the data to be tried out, but in the case of the four "out-stations" at Wavendon (12 bombes), Adstock (5 bombes), Gayhurst (16 bombes), and Stanmore (32 bombes), the controller telephones the menus and wheel orders over direct telephone circuits. I watched the latter operation and it seemed to go nicely. A phonetic alphabet all their own is used.¹ The controller also performs a function known as "numbering up", which simply means that she "numbers" the links on the menus so that the plugging on the bombes is made as easy as possible for the bombe operator. The controller also allots the specific wheel orders and their priorities. They try to avoid operating on the same menu at two out stations, but sometimes this cannot be avoided.

A staff of 25 to 30 mechanics must be maintained for bombe repair and maintenance. They are under Flight Lieutenant Jones, who is one of the top technical men of the British Tabulating Machine Company and had the position of "Works Manager" there. Jones came to BP with the very first bombe. I learned, also, that the first BP bombe was designed by Messrs. Welchman, Turing, and Keene, the latter an engineer of the British Tabulating Machine Company.

¹At the time of my visit the transmission of menus by teleprinter was on an experimental basis and gave promise of success.

SECRET

DECLASSIFIED

Authority NND 963016

By Wp NARA Date 6/6/03

SECRET

The training of the Wrens, who operate the machines, is given in Stanmore, where there are special bombes for the purpose. They are training new operators at the rate of about two dozen a week.

Referring to the training that the Wrens get on bombe operations, I talked with the Wren officer who is in charge of the instruction and learned the following:

Wren petty officers conduct the instruction. They have special qualifications for this work as a result of having been in the actual bombe operations for at least 18 months. Each instructor can take on an average of 15 students per week. There is, of course, some preliminary instruction along security lines. A bit of explanation of what the job is about in general inculcates a feeling of responsibility and importance of the job. The students then are divided into groups of two and the instructor outlines the various details of the operation of the bombe. They receive no training in cryptography or cryptanalysis but get a detailed explanation of what the bombe does. When they have learned that, which takes two days to one week, they go on to plugging and testing jobs. These take another week, after which they learn to do more advanced jobs. They then are put to work in an operational bombe room as understudy for an already well-trained operator, and after about two months' actual work, they take an examination which qualifies them for promotion to the First Grade. This examination is based upon the subjects studied by them during their training and first few weeks actual work. If they pass the examination there is an increase in pay. They then are given more advanced duties such as acting as officer in charge of operation, checking the work of others, and so on. After six to nine months more work, depending upon their ability, they take a second examination for a "Leading Rate". This is very much more advanced and is made up by Flight Lieutenant Jones. If they pass and are considered suitable they take charge of other Wrens and may become a leading Wren. I was told that they must become quite expert to go up to "Petty Officer" but there are no further examinations after the second one.

c. BOMBE CONTROL: The Netz Room

The name of this room dates back about two and one-half years and I failed to learn its origin. What it really does

SECRET

DECLASSIFIED

Authority NND 963016By Wp NARA Date 6/6/03

SECRET

is to test out the successive bombe "stops" which are sent from the various bombe rooms in order to ascertain when a valid solution has been reached.

Its personnel consists of a chief, who is in charge of menus, and two or more assistants, who are in charge of "wheel orders" and the testing of "stops".

The Netz Room receives the menus as regards operational keys from the Operational Watch, together with data as to how many bombes are to be put on each menu and other information relating to processing priorities. It is the policy to follow these priorities quite rigidly, regardless of whether or not an existing wheel-order set-up on a bombe must be changed. The Netz Room in turn, transmits this information relating to bombe operations to the bombe rooms in Hut 11A or at the various out-stations.

The Netz Room receives back from the bombe rooms the good "stops", or possible solutions, examines them, determines whether they will solve the key and completes the breaking of the key after the initial step has been provided by the bombes.

They keep an accurate account of the progress of each job by means of two logs called "Bombenlage". This is a coined word meaning the "bombe situation". One of these logs is for the 32 bombes at Stanmore, the other is for all the bombes at the remaining out-stations. These logs show the following data:

- (1) Time menu received.
- (2) Time sent to the bombe room.
- (3) Name of the job, "Red", "Primrose", "Locust", etc.
- (4) Job number assigned. They begin with 1 and go up to 1,000 and begin again, but they have 26 such series, each preceded by a letter of the alphabet.
- (5) Name of the bombe assigned (every bombe has a name, all the bombes at each station having names which are associated in some fashion; for example, the bombes at Adstock are named after famous physicists.
- (6) Date of job.

SECRET

DECLASSIFIED

Authority NND 963016

SECRET

By wp NARA Date 6/6/03

- (7) Menu number.
- (8) Number of times the menu goes on the bombe. (This depends on the length of the menu, if of 12 elements, the menu will go three times, that is, three wheel orders can be tried on that bombe. If the menu is greater than 12 it can only go on two, that is, only two wheel-orders can be put on it simultaneously.
- (9) Controller's initials.
- (10) Time that the menu is stripped, that is, after the completion of the job, the time the plugging connections were taken down.
- (11) Remarks. This may consist of various notations such as whether consecutive stecker knockout was applied, whether the solution was reached or not, and so forth.
- (12) Date the menu was stripped.
- (13) Total number of hours the menu was run.
- (14) Initials of the controller who authorized stripping the bombe connections.

Another record is maintained called the Job Number Book. It contains seven elements as follows:

- (1) Job number.
- (2) Title, that is whether "Red", "Primrose", "Locust", etc.
- (3) Time menu was received.
- (4) Time menu was put on the bombes.
- (5) Time and date menu was taken off the bombe.
- (6) Name of the bombe on which solution was reached.
- (7) Particulars of the correct stop, that is, the position of the wheels, the wheel order, the "input letter of the menu and so on.

Another record is maintained of what they call "Jobs Up and Jobs Missed". This is a record maintained for the purpose of keeping track of bombe failures, that is, where solution

SECRET

DECLASSIFIED

Authority NND 963016

By Wp NARA Date 6/6/03

SECRET

should have come up but did not because of faulty operation of the bombe itself. This record constitutes a factual basis for improving the bombes or the technique in their operation. The record I saw showed that from May 1 to May 20 there were six cases of bombe failure, when solution should have been reached but was not.

The way in which they determine when a bombe failure has occurred is, of course, dependent upon how they got the solution for the key that the bombe failed on. This solution might have been reached by a re-encipherment, by another crib, by cillies, and so forth.

I examined the data of Jobs Up and Jobs Missed for all stations for the period January to April. It showed the following:

Month	Jobs Up	Jobs Missed	% of Efficiency
January	374	14	96.3
February	304	7	97.7
March	344	4	93.7
April	390	17	95.6

Naturally, such a record does not take into account the jobs that are missed the cause of which has not been ascertained.

Another record maintained is called the "Controller's Log Book", which is a two-part affair, one for the odd days in the month and one of the even days. The purpose of this two-part arrangement is so that a study can be made of the previous day's log. The data in this log deal mostly with machines coming in and out of action, the time of the event, what errors were encountered, what rearrangements had to be made, changes in personnel and so forth.

On a wall in front of her, the controller has a large map showing the names and locations of all the 72 bombes and their condition.

When a bombe room reports faulty operation of one of their machines it is up to the control room to select another bombe, if available, and continue the job.

DECLASSIFIED

Authority NND 963016

By Wp NARA Date 6/6/03

SECRET

The Duty Officer of the Operational Watch (under Mr. Milner-Barry) has the final word on and responsibility for bombe control and processing operations.

When the solution has finally been reached, data as to the proper wheel order and the setting of the "Ringstellung", the various "Steckers", etc., are sent to what they call the "decoding room", where traffic is processed or decrypted by means of the solved keys.

d. "Duds" and Railway E Traffic

The Netz Room also works upon "dud" messages and processes the German Railway E ("Rocket") traffic.

With respect to the former, there are in the Netz Room two people who try all reasonable assumptions for garbles in indicators and discriminants in the case of messages which fail to yield to decipherment by means of the key they bear on their face. If after trial these workers cannot ascertain the cause of the difficulty they pass the "duds" to the log readers in Major Lewis' section, in the expectation that there will be found some indications in the receipts or in service messages which may throw some light on the matter. If the log readers find such data the "duds" are returned to the Netz Room and the operators there try once more to straighten out the trouble. If successful, they then pass the messages on to the "Decoding Room" for further processing, just as normal messages are passed.

The people who work on "duds" in this room are selected from among those most skilled in the testing of normal messages, since a good background of experience with the latter type is essential for success with the former.

SECRET

DECLASSIFIED

Authority NND 963016

By 4p NARA Date 6/6/03

SECRET

With regard to the processing of "Rocket" traffic, which consists of E messages of the German Railways, personnel of the Netz Room are responsible for hand-solution of the keys applicable thereto.

The Railway Enigma machine is a relatively simple affair. It has only three rotors, which have but a single turnover point; the reversing rotor is also rotatable just as the other rotors are; there is no plugboard.

The keys are solved on the basis of cribs and the use of special charts which eliminate the effect of the fast-moving rotor.

The British regard the solution of "Rocket" traffic so simple as to make the use of bombes therefor unnecessary. However, occasionally in difficult cases, a single bombe may be employed to facilitate solution.

The intelligence obtained from "Rocket" traffic is of first-grade importance since it gives long-term information as to production and movements of supplies.

F. THE "DECODING" OF TRAFFIC

a. The "Decoding Room"

The messages come to this room for decipherment after the keys have been found. Its equipment consists of a battery of 14 Typex machines which have been converted into automatic Enigmas. There are approximately a dozen women on each shift, the two extra machines on hand being available in case of a breakdown of a machine.

A large number of plugboards for Steckerung set-ups are provided and these Stecker boards are left set up for 48 hours after they go out of effect, so as to be able to process late messages.

The girls who operate these machines get two to four weeks' special training in their operation, after which they are capable of not only deciphering messages free from serious garbles, but can also straighten out the most common types of errors encountered. They paste up the decipherment slip on the

SECRET

DECLASSIFIED

SECRET

Authority NND 963016

By 40p NARA Date 6/6/03

back of the message itself, and they also write down on the message the final setting of the rotors at the end of the decipherment.

Approximately one-third of all the messages processed come right out without any difficulty, two-thirds of them present some trouble. I might add that the printed slips which come out of the Typex Machines are extremely poor and hard to read. Many of the letters are printed off line, the characters themselves are dim, and often are not legible. This is the result, of course, of a poor machine to begin with.

The deciphered texts are then passed to a room known as the "Cubicle", "Cottage", or "Goldfish Bowl", where a record is kept in the form of a card index showing the cryptonet, the frequencies involved, the date, the time the decipherment of each message was started, the serial number corresponding to the "blis" number of the message, and so on.

Often messages which are badly garbled are returned from Hut 3 for correction by comparison with a possible duplicate, and a record is kept of these cases. This shows the cryptonet, the date, the "blis" number, the time of arrival for correction, the priority assigned to work by Hut 3, the time the correction went out and remarks such as, "There are no duplicates", "The message was very corrupt," etc.

More detailed records are kept of the work in and work out, according to various headings, all for the purpose of keeping track of the traffic, expediting its transit, noting where delays occur, etc. Great pains are taken to eliminate all delays and bottle-necks.

As noted above, the decodes pass into the "Cubicle", "Cottage" or "Goldfish Bowl", but in so doing, they pass across a desk occupied by a chap who is called the "E/P-er", who is in the Watch. He is the one who makes entries into the crib books "En Passant". It is his job to note everything old and anything new in the cribs. Although this delays the transit of the decipherments a few seconds, it is, of course, a very necessary delay.

Messages which cannot be broken down and become "duds" pass through a separate window from the deciphering room into another room where they are handled so as to bring up the proper

SECRET

DECLASSIFIED

SECRET

Authority NND 963016By Wp NARA Date 6/6/03

correction. If a "dud" is only a part of a multiple-part message, even if the other parts have been deciphered they are held there with the "dud" part. If correction data come in, the "dud" is corrected and passed to the "E/P-er". If, however, no correction is forthcoming, all of the good parts are passed to Hut 3 and note is made of the presence of a "dud" as one of the parts. Hut 3 may then come back with some suggestion for a possible beginning for the defective part.

Here again registers are kept of the serial numbers of the "dud" messages, whether finally passed to the "E/P-er", whether correction was impossible, etc.

The messages processed in the "Decoding Room" are sent by conveyor belts (soon to be replaced by pneumatic tubes) to Hut 3.

b. Training Course For Typex Operators
of the Deciphering Room

A school is maintained for the training of young women who go into the Deciphering Room. They are selected primarily as typists and, after clearance and preliminary security indoctrination, they receive some training in the basic principles of the Typex machine as converted for E purposes. No specific types of problems are selected but they work largely on back traffic. At the end of two weeks' training, they begin to be useful and can be employed on regular shifts if there is a rush on, but it is preferable to keep them in training for a total of one month. These girls do not know any German to begin with, but they pick it up quickly and learn to recognize when plain text German is coming out and when it is not. The school is equipped with six Typex machines.

SECRET

DECLASSIFIED

Authority NND 963016
By wp NARA Date 6/6/03 **SECRET**

VIII. "INTELLIGENCING" OF E TRAFFIC

A. GENERAL

Although the general subject of intelligence operations do not come within the scope of my own duties in the Signal Security Agency, since the "intelligencing" of E traffic is a vital part of operations at BP I deemed it advisable to look into this phase while making a tour through the whole E operation there.

The intelligence operations based upon the solved E traffic are conducted in Hut 3 under Wing Commander Jones, who, in civil life, is a high executive with a textile firm in Manchester. Before coming to BP he spent two years at the Air Ministry in London, handling the information sent from BP, and therefore had a good idea, when he came to duty as head of Hut 3, of the requirements of the Air Ministry in this field, how the material is handled and what is done with it there, where it is forwarded, and so on. He gives one a decided impression of great ability, force, and decisive power.

Before beginning a tour of the activities under him, Wing Commander Jones spent some time with me in his private office, giving a verbal description of Hut 3 organization and the functions of his various assistants and their respective organizations. This section summarizes the talk we had.

Hut 3 now receives daily about 1000 processed E messages from the deciphering room of Hut 6. They comprise only the following categories of traffic:¹

- (1) E traffic, including GAF, GA, Submarine, and Naval.
- (2) Geheimschreiber traffic (the German enciphered tele-type traffic, which they regard as even more secret than E).

¹The E traffic on "Orange" and "Quince" cryptonets, which deal with communications of the Waffen SS go to No. IV Intelligence School for study alongside the Double Playfair "Domino" traffic of the German Gestapo. The E traffic of ISK goes to the section under Mr. Twinn. These types will be explained in another report.

SECRET

DECLASSIFIED

SECRET

Authority NWD 963016

By Wp NARA Date 6/6/03

- (3) Italian Naval Hagelin traffic.
- (4) Enciphered code traffic of non-E German naval and submarine communications.
- (5) The Double Playfair traffic used as a back-up for the E machine when the latter is inoperative for any reason.

The messages are registered individually and are at once sorted into two principal classes before being distributed within Hut 3. These classes are: (1) urgent operational material, which goes to the "Central" or "Operational Watch Room"; (2) less important or less urgent material, which goes to the "Back Watch Room".

The messages of both categories are read immediately upon receipt by the No. 1 man on the Operational Watch, who is usually the most experienced person. He gets a sense of the urgency of the contents and sorts the messages into four groups as follows:

- (1) Material of an immediate operational character requiring quick action. These are certain to be sent by "signal" to commanders abroad. They are also teleprinted to the Ministries in London.
- (2) Material of importance but not requiring instantaneous treatment. These are to be teleprinted to the Ministries and probably to be sent abroad by signal. This category constitutes 90% of the material coming to Hut 3.
- (3) Material which is of definite value but need not be teleprinted and can be sent via courier to the Ministries in typewritten report form, this involving a delay of 1 to 5 days. Such messages are primarily of interest in connection with German production, movements of small units, etc., and are generally dealt with by the Back Watch.
- (4) Material of no importance (called "Quatsch"), which may not leave Hut 3 at all.

The messages of the first two classes are at once worked on by the "Central" or "Operational Watch"; those of the last two classes are dealt with by the "Back Watch".

DECLASSIFIED

Authority NND 963016

SECRET

By Wp NARA Date 6/6/03

The work of the Operational Watch is continuous throughout the 24 hours every day, that of the Back Watch is on a 16-hour basis. The Watches are as follows:

	Operational	Back
9 a.m. to 4 p.m.	1 watch	1 watch
4 p.m. to midnight	2 watches	1 watch
Midnight to 9 a.m.	1 watch	none

The work of the Back Watch is quite similar to that of the Operational but since the processed material is seldom of an urgent character it requires a bit different handling and the pace of operations is much more leisurely. The work of the Operational Watch will be described first and in detail.

The Operational Watch consists usually of a Duty Officer with a translation party of eight members, each of whom is an expert in translation and emendation. First, the translator must mark off the text into proper word lengths, since the texts coming from the deciphering room are not so divided up but are merely in 5-letter groups, the space being automatically inserted by the Typex machine. He then makes such corrections as are necessitated by reason of faulty interception. If badly garbled he may return the message to the deciphering room, attaching a special chit to it (see sample, next section). The final emended translation is written on a chit which the translator passes immediately to the No. 1 man or the Duty Officer in charge of the Watch (see sample form, next section). The latter checks the translation against the original German, and examines and approves any notes or comments which the translator may have deemed advisable to make on the message. In connection with this matter of making notes and comments, it was indicated that the translators are encouraged to do simple "intelligencing" on the messages they translate, such as conferring by phone with other people in Hut 3, with people in Hut 6, or with people in the Air Section, in order to clarify doubtful points, check addresses and signatures, or to be able to indicate whether or not the messages contain important new information.

This duty of translating and emending requires the highest skill and an excellent knowledge of German. (Later I saw quite a few of the German texts, pasted on the back of the intercepts just as the slips come from the Typex Deciphering Room, and I was impressed with the difficulty of the job.) In the first

¹The letters CH in German E messages are almost always replaced by the single letter Q, so that a word such as "bericht" is spelled "beriqt".

DECLASSIFIED

Authority NND 963016 **SECRET**

By Wp NARA Date 6/6/03

place, the printing on the slips is very poor, irregular, and hard to read. This is, of course, the result of the poor working of the Typex machine itself but much more important sources of difficulty are (1) the corruptions in the texts themselves, due to intercept errors, (2) the high degree of abbreviation used by the Germans, (3) the lack of punctuation, and, in general, (4) the complexity of the military or technical language itself.

With respect to the training of the people employed in the Watch as translators and emenders, Wing Commander Jones indicated that it takes about three months for a person skilled in German to be any good at all, six months to be useful, and twelve months before he is really capable of doing first-class work. These people must, to begin with, be of the highest grade intellect besides having an excellent knowledge of German. Those dealing with Naval Italian Hagelin must of course be equally good in Italian.

The final emended translations pass to a team of "advisers", the team consisting of six officers, two from each of the three services.¹ The advisers are in the same room as the translators and there are three such teams for 24-hour service. The functions of the advisers are two in number. First, they check and annotate the translations for the Ministries, adding such notes and comments as may be of assistance in understanding the import of the messages and doing additional "intelligencing" on it, after conferring with the translator or with other advisers on the Watch. The second and more important function is to draft "signals" or messages based upon the translations to operational commands abroad.

In respect to the first function, Wing Commander Jones indicated that the notes and comments which are added are never in the form of deductions or inferences made by the advisers but merely factual data known to the advisers from previous messages or from other intelligence sources. It is distinctly not their function to "evaluate" the messages or to make "appreciations", as the British term what we call "evaluations". As regards the drafting of the signals, the advisers, who must be excellent German scholars, are required to read

¹The representatives of the Army and the Air Force are called "advisers"; the representative of the Navy is called the "Naval Duty Officer". However, they are all usually referred to as "advisers".

DECLASSIFIED

Authority NND 963016

SECRET

By wp NARA Date 6/6/03

the original German text alongside the translation made by the translators of the Watch, for a signal itself consists of a paraphrase of the translated text, never the literal text itself. Minor details of no advantage to overseas commanders are omitted. Having drafted the signal, the advisers must decide who should receive it. This, Wing Commander Jones told me, was an art and not a science, since there is no book of rules to be followed. For example, the Mediterranean operational signals of this sort were sent to twelve stations and each one had a different function to perform. They never send these signals except to those commands who can use them; that is, they are not sent purely as a matter of supplying information. AFHQ, however, gets everything that is sent to any one of the other eleven stations and in addition it gets long-term intelligence which the forward stations do not get from Hut 3. Wing Commander Jones indicated the distribution of the material as of that date and named the following commands:

- (1) AFHQ, Algiers.
- (2) The 8th (British) Army.
- (3) The 1st (U.S.) Army.
- (4) The U.S. Army Air Forces under General Spaatz.
- (5) The 18th Command Group under General Alexander.
- (6) The Command at Malta.
- (7) The Command at Cairo (HQ of Middle East).
- (8) The Command at Alexandria (C & C Levant).
- (9) The Naval Cooperation Group in the Mediterranean.
- (10) The forward wing of the Naval Cooperation Group at Benghazi.
- (11) The Captain of the Submarine Base at Beirut.
- (12) The Command at Gibraltar (only for some of the traffic).

Having drafted the signal (see sample form, next section), the advisers assess the priority for its transmission, indicating urgency by the number of "zeds" as follows:¹

"Z" = important
"ZZ" = immediate
"ZZZ" = urgent or emergency
"ZZZZ" = emergency plus
"ZZZZZ" = highest emergency or urgency

In the Tunisian Campaign a "5-Zed" message, during active operations, was sent out on the average only once about every two days and usually reached the command concerned within an hour. The messages are, of course, cryptographed either by Typex or by 1-time pad systems with a good basic code.

¹The form shows only 4-Zed priority but when a higher priority is needed they add another Zed by hand.

DECLASSIFIED

Authority NND 963016 **SECRET**
By wp NARA Date 6/6/03

Sometimes a long message is broken up into several parts and the essence or most important item is sent as a "5-Zed" message. This may be followed by one "4-Zed" and two or three "3-Zed" messages covering the minor details.

Wing Commander Jones emphasized that the fundamental principle upon which his organization guided itself was absolute accuracy. They never let it be a case of "this will do" and they never leave any margin for guesswork on the part of the recipient of a signal. If the text of a German message is not 100% clear in and of itself they never attempt to supply clarification or interpretation. In every case they indicate the degree of reliability of the text by the following symbols:

A% = highest, or 100% accurate.
B% = anything better than 75% accurate.
C% = better than 65% accurate.
D% = about 50% accurate.

They do not, however, use this percentage system in signals to commands abroad but only in marking messages going to the Ministries by teleprint. In the case of messages going to the commands abroad, they use the expression "very reliable" as the equivalent of A%; "strong indications" as the equivalent of B%; "slight indications" as the equivalent of C%; and "fair indications" as the equivalent of texts some where between B and C%. They never send D% material abroad.

In the case of messages which have been translated but are lacking in address or signature, Hut 3 may apply to the T/A people for information but T/A evidence is never allowed to be used as absolutely certain.

A cardinal principle observed as regards all the material sent out from Hut 3 is that they never insert any wording in the signals or add any external indication whatsoever which might make it obvious that the information comes from a radio intercept; in fact, they always delete everything that would make this fact evident. Accordingly, the application of "camouflage" is an important measure. The camouflage which Hut 3 puts upon the texts is bizarre, sometimes to the point of being fantastic, but I was told that it is apparently effective. In the first place, the messages bear the curious and mysterious reference symbols "CX/MSS" followed by a number. The "CX" is understood to refer to "secret service"—by inference, the

DECLASSIFIED

Authority NND 963016

SECRET

By Wp NARA Date 6/6/03

work of "agents". They never show quite so openly as do our "bulletin" messages the address, signature, etc., but every attempt is made to make it appear that the information was obtained by secret agents. They use such circumlocations as: "The following was obtained by source who copied it from flimsies in a file at _____"; "Following reconstructed from fragments found in a wastebasket found at _____"; Part of a document issued at (time) at (place)"; "Compiled from a record seen by source on (date) at headquarters"; etc. When a corrupt portion cannot be straightened out they take advantage of the situation and put in an expression such as "document smudged here", or "report was torn badly", or "ink spot here", etc. Just what sort of a disguise is to be adopted in a specific message or place in the message is the responsibility of the No. 1 man on the Watch. It is left to his judgment as to what messages are to be treated in one way or the other, but a guiding rule is that one third of all the messages must be subjected to such camouflage treatment, and in the other two-thirds it is his responsibility to see that no wording is left in which would obviously or by inference make it clear that the information is based upon an intercepted and solved enemy message.

As already noted above, the emended translation and, if made, the signal based upon it are then passed to the Duty Officer, who again checks everything and is responsible for the final German as well as the English translation and the signal (if prepared). The Duty Officer passes the English text and the signal to the Signals Section for forwarding.

There are now in Hut 3 a total of five men capable of functioning effectively as Duty Officers. They are all commissioned officers except one (a Mr. Marchant). Usually there is only one on duty per shift, but in times of stress there may be two. The Duty Officer is responsible directly to Wing Commander Jones and acts as his deputy in case of his absence. This may occasionally mean dealing directly with Mr. Travis or with Brigadier Menzies in an emergency. The job of the Duty Officer is a very difficult one because not only do they have to do a full 8-hour trick in active operations but also they must do a very considerable amount of studying on the side, in order to keep up with events. When they return from leave, for example, it is necessary that they spend a full week or more in "reading up" so as to get back into the picture of what is current, what changes have taken place in the military situation, what movements of German units have occurred, etc.

SECRET

DECLASSIFIED

reproduced in full and in part

Authority NND 963016

By wp NARA Date 6/6/03

SECRET

Certain messages not processed by Hut 6 also come to Hut 3 for action. For example, if a signal based upon a message solved by the Air Section, or by the ISOS-ISK party, or by No. IV Intelligence School must be sent to an overseas command, it is Hut 3's responsibility to check it and forward it, although the "intelligencing" of the messages on which the signal is based is done by other than Hut 3 people. Thus, for example, German submarine or naval E material is handled directly by the Naval Section under Mr. Birch, who is responsible for reporting directly to the Admiralty and for actually drafting the signal to be sent to an overseas commander but the signal itself must pass through Hut 3 for checking and review, since Hut 3 has final responsibility in the matter of all intelligence signals forwarded from BP. In case the military or the air adviser deems certain naval messages of interest to his own "clientele" he causes such messages to be sent to them; similarly, the naval adviser can send to the Admiralty or to Naval Commands any air or military traffic he thinks of interest to them.

Thus Hut 3 acts as a clearing house for material going to the War Office, the Admiralty, the Air Ministry, and to overseas commands. Hut 3 sees all of the material from all the sections and decides for itself what should go out in each case. Sometimes Hut 3 passes material to the Air Section under Mr. Cooper but this is only by special arrangement and is not a regular service.

It has been noted that as regards the signals to be sent to commands abroad (based upon deciphered or decoded material), no matter what its source at BP, Hut 3 is the final authority and is responsible for transmitting them. However, when messages of operational character of interest to Home Forces are encountered, it is a responsibility not of Hut 3 but of the Ministries to disseminate them to the Home Forces units concerned.

There are certain classes of E traffic which do not flow through either the Operational Watch or the Back Watch, but go directly to a special section of Hut 3 known as the General or Interservice Intelligence Section. Just what this traffic is will be told when describing that section.

Referring to the work of the Back Watch, the operations there are in general similar to those in the Operational Watch except that there is seldom occasion to prepare or send a

SECRET

DECLASSIFIED

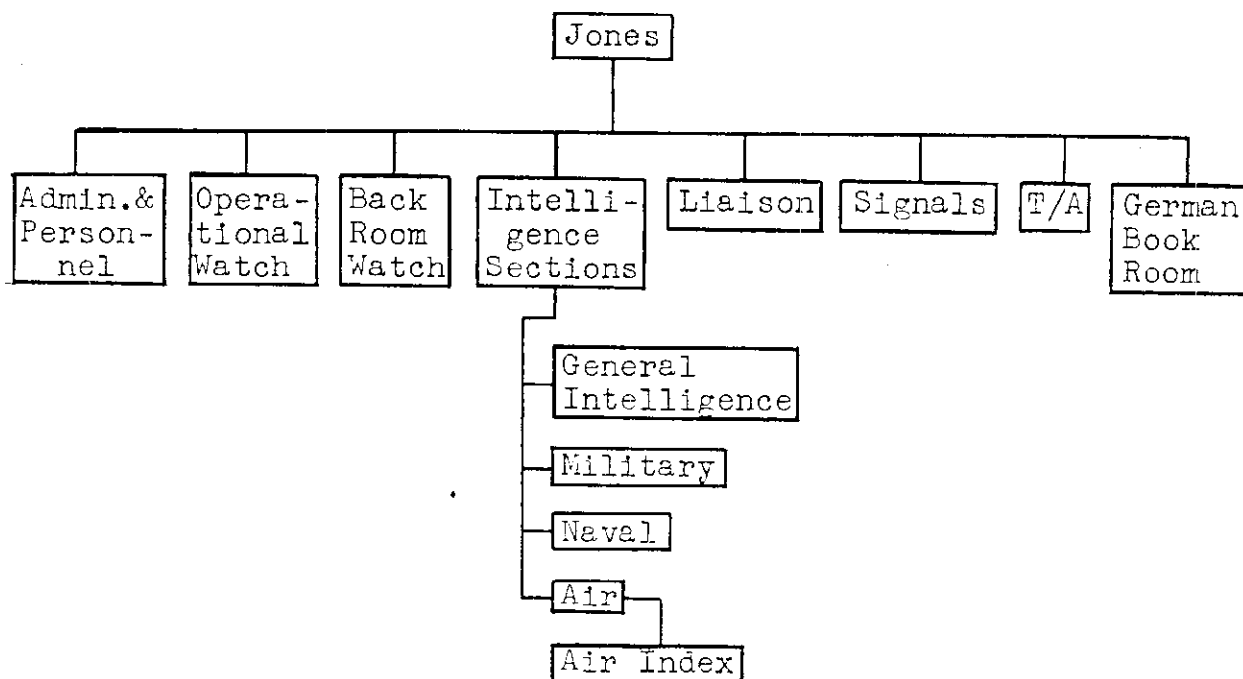
Authority NND 963016

SECRET

By Wp NARA Date 6/6/03

"signal" to overseas commands and therefore no advisers sit with that Watch as with the Operational Watch. One of the chief concerns of the Back Watch is E traffic on the "Rocket" cryptonet, which deals with German railway operations.

The operations in Hut 3 require the services of a staff of 328 people¹, organized as shown in the following diagram:



The functions of the Administration and Personnel Section are of the usual sort implied by the name. The functions of the Operational Watch and the Back Watch have already been described but I visited them and a few notes on what I saw will be given later. Regarding the other sections Wing Commander Jones indicated their functions in a general way which I summarize below.

¹This figure is of 17 May 1943 and does not include the T/A personnel of Major Gadd's section, who belong to No. IV Intelligence School.

DECLASSIFIED

SECRET

Authority NND 963016

By wp NARA Date 6/6/03

The intelligence sections have the following chief functions:

- (1) Through their respective advisers on the Operational Watch they are responsible for disseminating information to their respective Ministries and to overseas commands. In this respect the important principle is followed that the material is never handed out merely as a matter of supplying information for its own interest but is furnished only to those who actually have need of it for the proper conduct of their duties. The advisers see everything that comes to or through Hut 3 and they decide what shall be reported to their Ministries or sent abroad, except in a very limited number of special cases where a decision by higher authority (Commander Travis or Brigadier Menzies) is indicated.
- (2) Maintain liaison with their respective Ministries in order to serve the latter better, by a full understanding of what they require.
- (3) Serve as a channel for information from other sources such as that received or elaborated by the Ministries and deemed useful in BP operations.
- (4) Maintain files, indexes, charts, maps, etc., to constitute a general pool of information for other sections of Hut 3, for Hut 6, or for other groups at BP.
- (5) Serve as a channel for feeding information back to Hut 6 and to other groups at BP.
- (6) Review all the reports, teleprints, and signals sent out from Hut 3, to check them once again and insure that no conflicting intelligence is disseminated.

Each of the three services has its own intelligence section and the advisers on the Operational Watch are the representatives of these sections. Just what they have and do will be discussed under separate headings but at this point it may be indicated that the advisers, in the capacity noted above, constitute the means whereby the Ministries feed back information to the Watch by sending to the chiefs of the respective intelligence sections

DECLASSIFIED

Authority NND 963016

By Wp NARA Date 6/6/03

SECRET

information or intelligence received or elaborated at the Ministries. Naturally, the latter type of information or intelligence is never later embodied in any signals sent to overseas commanders or in any teleprint reports from Hut 3 to the Ministries.

The three service sections mentioned above deal with all current problems of their respective services but they cannot cope with long term intelligence research, or with special problems of interest to all of Hut 3. As a consequence there is a fourth section called the "General Intelligence Section" or, sometimes, the "Interservice Intelligence Section", organized to undertake long-term intelligencing and studies of specific subjects, such as, for example, the interpretation of cover names for persons, thrust lines, target areas, air fields, anti-submarine areas, and technical equipment. It also studies German abbreviations. The General Intelligence Section passes the results of its studies to the three service intelligence sections and to the Watch Rooms, so that items such as the foregoing will be intelligible to the translators and emenders. They also prepare "appreciations" or special reports on subjects of general importance.

That section in Hut 3 known as Hut 3 Liaison, or 3-L, has as its function the supplying of information to the Intercept Control people for guidance in coverage from the intelligence standpoint.

In the German Book Room every message processed through Hut 3 is typed in the original German and copies are sent back to the sections interested, such as the T/A, the cryptanalytic etc.

The Signals Section is responsible for all telegraphic communication between Hut 3 and the Ministries and commands overseas.

Finally, the function of the T/A Section is to study all problems in the T/A field from the point of view of Hut 3 operations. The studies are made by a section of No. VI Intelligence School under Major Gadd, which will also be described later.

In closing his discussion Wing Commander Jones emphasized that the people in Hut 3 do not make "appreciations"; that is,

DECLASSIFIED

SECRET

Authority NWD 963016By Wp NARA Date 6/6/03

what we call "evaluations". Only factual comments, as noted above, are permitted to be made on signals sent abroad. If any deductions are made by Hut 3 people, these deductions are sent as a separate series of documents to the Ministries and if the latter wish to forward them to commands abroad this must be done through Hut 3. Occasionally if a deduction seems very worthwhile to include in a signal this is never done without reference to the Ministry concerned, in which case the statement is made "comment by Air Ministry" or "comment by Admiralty", or "comment by War Office".

A few words concerning the general nature of the intelligence contained in the E traffic may not be amiss at this point. In discussing this matter with Wing Commander Jones and others at BP I learned that about 95% of the material is operational in character, the remaining 5% yields "long-term" intelligence. In one of the telegraphic reports our mission made there is given a summary of the contents of about 100 messages processed by 4 working shifts of 8 hours each around 7 May 1943, these messages having been reported by teletype to the Ministries and for the most part sent as "signals" to overseas commands. For the sake of completeness the summarized contents of some of the messages are repeated below:

- 6 reports of immediate combat intentions.
- 12 reports on air and ground combat.
- 4 reports on airfield conditions.
- 4 strength returns, including one giving all details for "Battle Group Messina".
- 6 specific operational orders.
- 2 submarine reports (sighting of convoys, attacks by planes).
- 4 ship reports.
- 3 reports on reasons why certain movements could not be executed.
- 3 reports of aircraft serviceability.
- 1 report on gasoline consumed and on hand.
- 6 sighting reports by aircraft.
- 1 report giving names of overdue aircraft.
- 1 battle order report for units in eastern Mediterranean.
- 3 orders relating to urgent measures to concentrate aircraft on Mediterranean Islands.
- 5 personnel orders and reports.
- 1 inquiry as to possibility of executing a certain operation
- 1 report giving recognition signals for next day.
- 1 explanatory message about Croatia.

DECLASSIFIED

Authority NND 963016

SECRET

By Wp NARA Date 6/6/03

Wing Commander Jones stated that the arrangements for disseminating the intelligence, were quite good. Although the Naval and submarine E operations are under Mr. Birch and not under Mr. Welchman, its product does come to Hut 3 to become a part of the general pool of intelligence that is examined by the service advisers. If the army or air adviser deems certain naval material from Mr. Birch's section to be of interest to their ministries or service commanders abroad they can direct that material to be sent by teletype or by signal. The same is true as regards the forwarding, by the naval adviser to the Admiralty or to warships, of intelligence coming from Hut 6 operations under Mr. Welchman. The important point is that there is a very complete interchange of intelligence among all people who need it, and appropriate security arrangements exist to protect the source of the information so that it will not dry up. In addition, and to insure that no service fails to get everything it should get there is at BP a unit known as the "Intelligence Exchange". It receives a copy of every bit of information and intelligence that is produced at BP, and to this "Exchange" are assigned people from the various services and agencies of BP whose job it is to examine this material to insure that if there is anything there of interest which has not been routed to his group it will be sent, or to make a protest if it is withheld from the group he represents. (The "Intelligence Exchange" will be covered in a separate report.)

When I expressed some skepticism regarding the alleged efficacy of the "smudge procedure", etc., as a cover or camouflage for security purposes, Wing Commander Jones told me that while it might seem ridiculous or fantastic the camouflage procedure really works so far as concerns not only the people who are curious enough to glance over the shoulder of a man to take a peek at the papers on the desk but also the clerks who must be entrusted with the handling of the papers, the teletype machines, and so on. He himself, for example, had been handling this material in the Air Ministry for two years and never during all that time was he really certain what its source was. He furthermore stated that a typist in his own office who had been handling the material for over six months recently said to his private secretary, "That man Source must be the most marvelous man in the world!" Jones was convinced that she was quite serious in her belief, adding that it was really amazing what the average service officer would believe in regard to "secret service" activities. So far as most of

SECRET

DECLASSIFIED

SECRET

Authority NND 963016By wp NARA Date 6/6/03

the people in the Ministries are concerned he said that the camouflage Hut 3 put on the messages was taken as fact, not fiction, although there are, of course, a few higher-up people there who know the truth.

Finally, as to the security arrangements in forwarding the material to overseas commands Wing Commander Jones gave a rather important bit of information in connection with what is called the "SCU" or "Secret Communications Unit". It appears that the normal channels of communication between Hut 3 and overseas commands use special radio links operated by GC & CS people themselves, not the ordinary War Office, Army, Navy, or Air Force radio systems. For this purpose there is a special radio station at Windy Ridge (near London), but the transmissions are keyed at BP and the incoming signals are "piped" to BP. Attached to the staff of each overseas command to which the "signals" from Hut 3 are sent (see list on page 74) is an officer who is not a member of the staff but acts as the representative of GC & CS or rather Brigadier Menzies. This officer has a staff of his own, equipped with the necessary cryptographic paraphernalia (Typex machines, codes, 1-time pads) for handling messages from and to BP; only this officer or his special staff can handle the messages and it is his responsibility to see that the messages go directly and only to the commander himself or his authorized agent. The SCU officer has direct access to the commander and acts as his adviser in connection with the policies governing the handling and usage of the MSS messages, and also as a sort of watch dog for Brigadier Menzies in regard to security and violations thereof. It is his duty to insure, for example, that operational action is never obviously taken solely on the basis of information contained in "signals" from BP. In order to provide an adequate camouflage he must insist that local or long-distance reconnaissance operations be made evident to the enemy so as to make it appear that the action taken was based upon this latter source and not upon the MSS source. In short, the SCU system and its representatives completely by-pass the normal military, naval, or air force channels and are responsible only to Brigadier Menzies, for whom these representatives act as monitors with great prestige and authority to back them up.

In the following sections I will take up the work of each of the principal working groups mentioned above.

SECRET

DECLASSIFIED

Authority NND 963016

By Wp NARA Date 6/6/03

SECRET

B. THE OPERATIONAL WATCH

On the morning of May 26, I visited the Operational Watch Room in Hut 3 to observe the operations therein.

As noted from the preliminary outline in the conversation with Wing Commander Jones, the No. 1 man on the Watch sorts the messages coming from Hut 6 into four piles according to the degrees of urgency or importance of the messages. There are not many on the No. 1 pile; at most three or four at a time. The translators and emenders take the messages from the piles, naturally clearing the messages from the No. 1 pile first and when those messages have been finished then they begin on the No. 2 pile, etc. Translation is made as rapidly as possible but accuracy comes first and speed second. The translations are written by hand on forms as per sample attached hereto. In case the message is badly garbled the translator may return it to the "Decoding Room" using the sample chit shown below.¹ (It has a gummed back, which is used to attach it firmly to the message.)

D.R.

(1)

RETURN TO (2)

WATCH:— A. B. C. D. E. F. G. (3)

PRIORITY. Z. ZZ. ZZZ. (4)

¹Notes:

- (1) "D.R." means "Decoding Room".
- (2) The name of person to be returned to.
- (3) There are usually 3 Operational Watches, A, B, and C; 2 Back Watches, D and E. But in times of very active operations there may be additional watches.
- (4) The priority or urgency of the corrective action.

SECRET

DECLASSIFIED

SECRET

Authority NND 963016By wp NARA Date 6/6/03P. 39.
(1)

Geog. Heading.....(2).....CX/MSS/.....(3).....T.....(4).....

Sub-Heading.....(5).....

(6)

(7)
(P.T.O. if necessary)

Routing	G.T.O. and Date	Freq.	Colour and Number
(8)	(9)	(10)	(11)
Originator	No. 1	D.O.	T/P Supervisor
(12)	(13)	(14)	(18)
N.D.O.	M.A.	A.A.	
(15)	(16)	(17)	

Same of form used for writing down the translations.

DECLASSIFIED

Authority NND 963016

SECRET

By 40p NARA Date 6/6/03

Notes:

- (1) This is the BP "form" number.
- (2) A general indication of the area involved, such as "German", "Western Europe", "Eastern Europe", "Northern Europe", "Mediterranean", etc. In the case of the Balkans area the name of the country is given.
- (3) "CX" stands for "Secret Service"; "MSS", for "Most Secret Sources". The space is filled in with the serial number of the 8-hour period involved. At the time of my visit this was the 2,628th period.
- (4) "T" means "teleprinted". If teleprinted to Ministries the sheet receives a serial number, the series beginning with 1 for each 8-hour period. Thus "CX/MSS 2628 T 52" would designate the 52d teleprinted reported message in the 2628th 8-hour period. If not to be teleprinted the "T" is crossed out and an "R" inserted, meaning "Report".
- (5) In this space "Army", "Navy", or "Air" is written depending upon which service is primarily interested.
- (6) In this space is handwritten the emended translation.
- (7) "P.T.O." means "Please turn over". If the translation is long or if there are many "notes" by the translator the back of the sheet is used.
- (8) In this space is written the Ministry to which sent.
- (9) G.T.O. is German Time of Origin.
- (10) The frequency on which the message was sent.
- (11) "Colour" is what we call "cryptonet". The number is a serial number assigned the message during its processing in Hut 6.
- (12) The translator's initials.
- (13) The initials of the "No. 1 Man" on the Operational Watch.
- (14) The initials of the "Duty Officer" of the shift of the Operational Watch during which the translation was made.
- (15) The initials of the Naval Duty Officer (= "Naval Adviser").
- (16) The initials of the military adviser.
- (17) The initials of the air adviser.
- (18) The space is used by the time-stamp and initials of the supervisor in the Signals Section if the message is teleprinted or sent by Signal to an overseas command.

DECLASSIFIED

Authority NND 963016

SECRET

By Wp NARA Date 6/6/03

Having checked the translation, the translator marks it either "R" for report or "T" for teleprint, pins it to the original German message, and passes the messages to the No. 1 man on the team of advisers. (The No. 1 adviser on the day I visited the Watch was the RAF officer.) If the message does not concern him he passes it to the military or naval adviser, whichever he deems the message to be of most interest to.

A record book is maintained of the hour when solution has been reached and of the keys applicable to the various cryptonets. This information comes from Hut 6 by telephone and is intended merely for the convenience of the Watch since it gives them a picture of the current situation regarding the keys. A very brief record is kept of the contents of messages which have already been teleprinted to the Ministries that day, so as to insure the detection of duplicates, for ease in reference, etc.

The advisers may send back to the emenders any message which they believe requires more clarification, or a correction. If a note is necessary or deemed advisable by way of explanation it is added when teleprinting the text to the Ministries but these notes are strictly factual. No deductions or inferences whatsoever are permitted on the part of the advisers.

The camouflage which is applied to the messages in order to hide the source is applied by the No. 1 man on the Watch and not by the advisers, whose only concern is the intelligence content. It is the advisers, however, who draft the operational signals when necessary. For this they use a form as per sample attached. If no signal is necessary the emended text passes to the Duty Officer, who forwards the message to the Signals Sections of Hut 3. The Duty Officer, before forwarding it, looks at the text, placing himself in the position of the recipient. He is the final arbiter as to the sense of the message, its clarity, etc. If the message is complicated and of vital importance he checks it against the original German text. If the message is of such character as to be deemed of interest to Brigadier Menzies, a "headline" or very succinct summary of its contents is prepared and forwarded immediately by teleprinter. If of sufficient importance it may be flashed to the Prime Minister by Brigadier Menzies.

Messages of no intelligence value but of such character as to be of deep interest to commands abroad and likely to

SECRET

DECLASSIFIED

Reproduction of the original document

Authority NND 963016

SECRET

By Wp NARA Date 6/6/03REF.....
(1)Z / ZZ / ZZZ / ZZZZ
(2)

((ML... (3) (UG... (4) (WD... (5) FI) (6)

MA... (7) TZ... (8) DE... (9)

CO... (10) AL... (11) NC... (12) NCA... (13) SM... (14)))

N.B. All deletions MUST be made by an oblique stroke, thus ~~###~~ ~~###~~
(15)

(16)

Have you checked PRIORITY and ROUTEING?

Originator (17)	D.O. (18)	Seen by		
		N.D.O. (19)	M.A. (20)	A.A. (21)

DECLASSIFIED

SECRET

Reproduced at the National Archives

Authority NND 963016

By Wp NARA Date 6/6/03

Notes:

(1) Reference No. of signal. This corresponds with the "CX/MSS and T" number on the translation. See notes (3) and (4) on preceding form.

(2) The urgency or priority is indicated by passing strokes through the other classes. See note (15).

(3) "ML" is symbol for "AFHQ, Algiers". In the space is written the serial number of the signal in the series to Algiers. At the time of my visit the number was in the neighborhood of 2730, that is, 2730 signals of this sort has been sent to that command.

(4) "UG" is the symbol for General Alexander's HQ at Constantine. The serial number of the signal for that command would be written in the space.

(5) "WD" = Western Desert Army

(6) "FI" = First (U.S.) Army

(7) "MA" = Malta

(8) "TZ" = Gen. Spaatz's Air Force HQ

(9) "DB" = Gibraltar

(10) "CO" = Cairo

(11) "AL" = Alexandria

(12) "NC" = Naval Cooperation Wing (Group 201)

(13) "NCA" = Advanced Naval Cooperation Wing

(14) "SM" = Captain of Submarines

(15) Unless deleted by strokes the signal will be sent to each headquarters noted.

(16) The text of the signal in handwriting of adviser.

(17)-(21) Initials of officers concerned, as in preceding form.

DECLASSIFIED

Authority NND 963016

SECRET

By wp NARA Date 6/6/03

form the basis of "talk" are withheld. Such a case is exemplified by a message concerning Rommel's illness. In this case the translation was sent to the African Forces and word of it leaked out, with the result that gossip was widespread and caused mild panic at BP. The practice of withholding messages of this character has been in effect about eighteen months. A typed copy of such messages goes only to Brigadier Menzies and the chiefs of the three Ministries. No distribution is made within BP and the message is kept in a separate safe.

I talked at some length with Major Douglas, who was the Duty Officer at the time of my visit. For seven years prior to 1939 he had been in charge of the branch agency in Berlin of a British insurance firm and of course knew German thoroughly. He told me that the personnel of the Watch was a mixture of schoolmasters, professors, dons, business men, journalists, etc., but he emphasized that the translators and emenders had to be more or less walking encyclopedias. Douglas has been on the job here for three and a half years having come on before any E was broken. There were then only about eight people in Hut 3. Although breaks into keys had been made more or less sporadically ever since 1939, the first time anything was broken currently was during the Battle of France. Soon thereafter, when the Germans were preparing to invade England, a very full picture of the invasion operations were obtained from the E operations. This resulted in the RAF being able to bomb all the invasion barges at Antwerp, Rotterdam, and Dunkirk to bits, probably saving England from this great danger.

C. THE INTELLIGENCE SECTIONS

a. Military Section

This section is under Major Leatham and it is his function to supervise and coordinate the work of the military advisers and to provide background information for them as well as for Hut 3 in general. In this section are prepared and kept all sorts of maps, charts, indexes and files, the whole going to form a central pool of intelligence of a military nature relating to the German Army, so that if called upon by the War Office or by any of the groups at BP the section can produce at once or in a very short time the answers to questions of an intelligence nature that can be answered from detailed study of the

DECLASSIFIED

Authority NND 963016

By 46p NARA Date 6/6/03

SECRET

messages passing through Hut 3. The work done in this section parallels that done under Lieutenant Bright in the Naval Intelligence Section and under Squadron Leader Rose in the Air Intelligence Section. Major Leatham also covers intelligence on anti-aircraft.

With reference to his function of supervising and coordinating the work of the military advisers, the chief of the section also serves as liaison between Hut 3 and the War Office. In fact, he is a member of the military staff of the War Office and as such he generally looks out for the DMI's interest on every side of the activities at BP. He does this in a variety of ways. He knows what the staff requirements are in the way of intelligence and he represents the Military Intelligence staff in the important matter of fixing priorities in intercept coverage, processing, and treatment of E material in both Hut 6 and Hut 3 from the military point of view. He presents to Wing Commander Oeser (Liaison Section) the staff's views in these respects and Oeser must coordinate the military requirements with those from Naval Intelligence and RAF Intelligence staff's points of view. Major Leatham provides Wing Commander Oeser with a weekly directive in this regard.

Through Wing Commander Jones he directs and coordinates the work of the military advisers and he maintains telephone liaison with the War Office regarding signals to be sent to overseas commands. Because of his extensive sources of information in Hut 3, Major Leatham is to a considerable degree independent of War Office or Military Intelligence staff sources of information in London. Although the decision in specific instances as to what is to be sent out to overseas is made under Major Leatham's direction, the War Office fixes the general policy governing the dissemination.

Whenever notes or comments of a strategic nature are made on signals going out to overseas commands it is understood that they were made on behalf of MI-14 (which is responsible for intelligence on Germany proper and the German Army) and not on Major Leatham's own initiative. The advisers, of course, write the comments in Hut 3, but they phone to London for concurrence. Major Leatham goes to London once a week for liaison with the War Office Staff and brings back with him, or arranges to be sent to him, such information as is collected or elaborated in London and which may be of use to him at BP. Thus there is a two-way liaison with the War Office. Major Leatham prepares

DECLASSIFIED

Authority NND 963016

SECRET

By wp NARA Date 6/6/03

digests or summaries of information and comments based on War Office papers and summaries, or prepares notes as a result of telephonic information from and visits to London.

It is also his duty to clear up doubtful points for the War Office as to the results of the analysis of messages processed at BP. The military advisers submit doubtful points to him for clarification in which case he may have to confer with his people in the War Office.

In order to provide all of the background information and intelligence, Major Leatham maintains an extensive set of files, indexes, charts, and maps. He correlates information with reference to supplies so that duplication of information is avoided. For example, when a military adviser gets a message about fuel he can look through the files to see if the particular items in that message have already been sent out in another report or signal. He also has a representative in the "Intelligence Exchange", who reads not only all of the Hut 3 material but also non-Hut 3 material so that information from all other branches of BP can be used to advantage by the Military Section.

The Military Intelligence "Index" is in charge of Captain Lyon, who is a specialist on German Army Order of Battle. Some of the indexes which he maintains are as follows:

- (1) Personalities—of German and Italian or foreign armies in general.
- (2) Small units of the German Army—from regiment down—and for all units of the Italian army.
- (3) Large units of the German Army.
- (4) Equipment—including guns, tanks, vehicles, etc.
- (5) Supplies—fuel, ammunition, etc.
- (6) Departments of the OKW and OKH.
- (7) Cover names.
- (8) British and American units.
- (9) Geographical.
- (10) General.

SECRET

DECLASSIFIED

Authority NND 963016

SECRET

By 40p NARA Date 6/6/03

There is also a "railroad index", which deals with the movements of supply trains and the cover names for such movements. In addition there is an index of shipping, of ports, and of the movements of vessels, together with their cargoes.

A large array of battle order maps is maintained here. These are issued frequently to those on authorized distribution lists.

The staff of the Military Intelligence Section comprises the following:

- 1 Chief
- 3 Intelligence Officers
- 1 Assistant Chief
- 10 Military advisers
- 10 Indexing, charting, and file clerks
- 1 Secretary
- 1 Assistant secretary

One officer (in rotation) serves as representative in the Intelligence Exchange. The three intelligence officers listed above are specialists in (1) Battle Order, (2) Flak, and (3) Supply, respectively.

b. Naval Section

What has been said about the duties and responsibilities of the Military Section applies in general also to the Naval Section under Lieutenant Bright, so that it is not necessary to go further into them here. But there are certain remarks which apply specifically to the Naval Section alone and these will be noted below.

It has been observed that E operations on German Naval and submarine traffic constitute a group of operations rather distinctly separated from those on GA and GAF. The naval and submarine E work is conducted in "Block A" under Mr. Birch and the material is processed separately up to the point where the final messages are ready to be reported to the Admiralty or to go by "signal" to naval commands. It then goes to Hut 3, where it becomes part of the general pool of intelligence coming under the purview of the advisers in Hut 3.

The primary function of the Naval Section of Hut 3 is, therefore, to maintain liaison between the operations under Mr. Birch and those under Wing Commander Jones.

DECLASSIFIED

Authority NND 963016

SECRET

By 490 NARA Date 6/6/03

The output of the traffic in Italian Naval Hagelin and German naval or submarine E, as far as it concerns the Middle East and the Mediterranean area, is routed through Hut 3. This output consists of "zed" traffic. ZTPI is Italian Naval Hagelin, ZTPG is German naval general, ZTPGM is German naval E, ZTPGU is German submarine E, ZTPS is a Spanish naval machine cipher (but I did not learn what it is), STPG is a German naval hand-operated cipher. All translated and emended messages processed in Block A which have any naval angle at all pass to the Naval Duty Officer in Hut 3. The Naval Section serves him in his capacity as the adviser on the Operational Watch of Hut 3. (The Naval Duty Officer drafts whatever signals may be necessary and passes them to the Duty Officer of the Watch for approval; thence they go to the signals section of Hut 3 for enciphering and forwarding just as do the signals prepared by the military and the air advisers.)

With regard to the ZTPI traffic, I was told that the keys change monthly but that they are able to get into the traffic on the very first day. Later, when I had a conference with Professor Vincent, the latter explained to me the basis for this quick solution, which arises from faulty usage of the Hagelin machine by the Italians.

The ZTPGU operates by means of a daily key and is of importance only in the Mediterranean.

ZTPGU also operates on a daily key and I was told that Block A has to break into it only spasmodically. However, usually not more than a week passes by without a break into it.

In the Naval Section the services rendered are purely editorial and advisory as regards Middle East problems. Service for the Atlantic is direct from Block A to the Admiralty.

The Naval Section serves as an information center for the naval duty officer. For this purpose there is maintained a very comprehensive card index so that anything relating to any ship, port, mine field, etc., can readily be supplied. A comprehensive index of personal names is maintained, especially as regards the personnel aboard submarines. The latter is important because messages for submarines are addressed personally to the commander by name. The complete file of cards totaled well over 200,000.

DECLASSIFIED

Authority NND 963016

By Wp NARA Date 6/6/03

SECRET

One interesting point I picked up was that despite the ease in reading Italian Naval Hagelin traffic, the British have not been able to read Italian Naval E traffic. In general, however, Italian Naval cryptography is good. In talking later with Professor Vincent he referred me to a quite extensive manual on security, prepared by the Italian Navy, and declared it excellent. On my return I found we already had a copy of this treatise and agreed with Vincent.

Another interesting point I learned was that BP has had one or two "scares" in recent months, when leakage of information regarding E operations seemed clear. During the Tunisian Campaign, when Admiral Cunningham had smashed up two convoys pretty badly, there were indications in German E messages that the Germans were getting suspicious about the security of the E machine. But after investigation the Germans apparently came to the conclusion that British spies were at work. In this connection it is important to note that the British adhere very firmly to the security principle that direct action must never be taken on information coming from the E or other operations at BP. For example, they make it a fixed rule never to bomb a ship or a convoy without sending out a reconnaissance plane or two and making their presence quite obvious. This is to protect the source of their information, of course, and so far the practice has been effective apparently.

c. Air Section

The functions of the Air Section, under Squadron Leader Rose, are in general, similar to those of the Military and Naval Sections. It keeps GAF Battle Order maps up to date, indexes all air intelligence and such military, naval, political, commercial, and "abwehr" intelligence as may be of use from the standpoint of those primarily concerned with air operations.

Its personnel is as follows:

- 1 Chief
- 11 Advisers
- 2 Intelligence Officers for short term research
- 2 WAAF Intelligence Officers for long term research
- 1 Chief of "Index"
- 25 Index clerks

A few of the highlights regarding this section follow.

SECRET

DECLASSIFIED

Authority NND 963016

SECRET

By wp NARA Date 6/6/03

At the outbreak of war the GAF completely changed all its designations of units and previous British information regarding GAF Battle Order which had been gathered with a good deal of labor became worthless. Consequently, the Air Section had to rebuild practically the whole of its information regarding the organization of the GAF. Now they have a better picture of the GAF probably than the GAF has itself.

The "index" maintained in the Air Section is so extensive that the indexing has been in fact organized as a separate section under a Miss Webb. The 25 girls who work for her are all of excellent education and most of them have university degrees.

The personalities index, for example, comprises over 15,000 names, including data on all the high commanders, of course, but going down as far as NCO's. The card applicable to a particular man will give practically the data of his whole career, including promotions, leaves, illnesses, trips, etc. In fact, in order to get the information which is on file in the Air Section one would probably go to a half a dozen different offices in Berlin. This large file of data regarding personalities is very useful in tracing the movements of GAF units. The complete structure of the GAF and especially of its signals organization is known in the most minute detail. An important source of early intelligence regarding a future move of a GAF unit is found in the movements of these signals organizations because their movement is the first indication of larger movements. The composition of each Fliegerkorps is variable and it is important to know the composition of each one. The movements of the Fliegerkorps of course tell in advance about the movements of German Army and its intentions. The most versatile of the Fliegerkorps is the Fliegerkorps VIII on the Russian Front. Incidentally I was told that the British gave the Russians very important information coming from E traffic about the Voronez attack last year but it appears that the Russians just would not credit the information.

The Air Section finds it important to watch the training activities of various GAF units. Information regarding the training of pilots, for example, to see if the period of training is cut short indicates that there is a shortage in the number of pilots capable of active operation.

SECRET

DECLASSIFIED

Authority NND 963016

By wp NARA Date 6/6/03

SECRET

Here follows the list of the various types of indexes maintained:

- (1) Personalities.
- (2) GAF units.
- (3) Air fields and the units which are located there. This index is subdivided geographically.
- (4) Cover names.
- (5) Supplies—divided into two parts, namely, supply units and returns on supplies.
- (6) Signal units.
- (7) Construction units.
- (8) Repair units.

The two WAAF Intelligence Officers specialize in long term intelligence studies of special proformas, of which the GAF uses at least 28. By a careful analysis of messages following proforma lines the Air Section is able to build up the nature of the proformas and determine the items dealt with under each heading. Thus they get extremely important data on aircraft production, servicability, losses, etc.

As in the other sections, detailed Battle Order maps are kept current.

d. The General Intelligence Section

This section known as 3-G has as its mission the derivation of special information covering such subjects of interest to the whole of Hut 3, to Hut 6, or to other sections of BP. The section is under Mr. Lucas, one of the "old timers" of GC & CS, with whom I had a conference.

One of the most important subjects studied in this section is that of the interpretation of "decoding" of code or cover names. He stated that apparently the Germans cannot conceive that their high-grade ciphers are being read and since they

SECRET

DECLASSIFIED

Authority NND 963016 **SECRET**
By Wp NARA Date 6/6/03

detect certain evidences of leakage, the only thing they can assume is that there are spies and agents on their own staff. In order to thwart such leakage they have been going in more and more for the use of cover names. The German Army, for example, drew up a list of over 1000 names of birds, plants, minerals, etc., all randomized and numbered. Distribution of names is made by sub-allotment from Army down through corps and divisions. The names are then applied to units, ships, times of day, operations, etc., and the list is changed very often. The GAF on the other hand allows each command to use its own initiative in composing cover names. The primary functions of his section is to identify individual cover names and then blocks of cover names. The individual identifications are made by deduction from references in messages and cross references between the real name and the cover name. The information is drawn up on card index forms and given reliability ratings:

A = 100% reliability.
B = 75% reliability.
C = 50% reliability.
D = 25% reliability.

There is an exchange with the Middle East commands with regard to the identifications reached by a study of messages in the forward areas.

I saw a list of cover names for types of ammunition. It consisted of nine pages of about twenty-five lines each, in other words, about 250 cover names alone for types of ammunition. There were also lists of cover names for points of the compass and for even the individual digits. Here is an example of the German idea of camouflaging the text of a message by means of cover words: (This is, of course, a translation) "Five turkey hens and a blue whale from evening meal repeat from evening meal baker shop exchange to little squirrel bear's hide evening meal from little glow worm to Irmgard." A translation of this message is: "5 JU 52's and 1 ME 323 from 0040 to 2150 from Trapani to Air Field E 14." (Air Field E 14 must then be identified, as it is a code equivalent also.)

Another function of the General Intelligence Section is to assist in the interpretation of proforma messages. These are messages in which weekly or monthly returns on supplies are made by merely giving the paragraph numbers and then the

SECRET

DECLASSIFIED

Authority NND 963016

By wp NARA Date 6/6/03

SECRET

statistical data applicable to each of them. By a careful study of the contents of such messages the General Intelligence Section is able to arrive at what the returns are about. For example, in one recent type of proforma, Section I was found to relate to data on fuel supplies, Section II to rations, Section III to ammunition, etc. There are many such types of proformas and two units might get up one of their own by agreement between Quartermasters. All of them are deemed worth study, and often a proforma can be "decoded" from only half a dozen reports based upon them.

The General Intelligence Section has a number of subsections. One, under Mr. Trevor-Jones, deals with abbreviations and technical terms only. It lays down standard or agreed-upon translations of abbreviations and feeds the results to the various index rooms and to the Watch. It studies captured documents from this point of view.

Another section, under Captain Holroyd, deals only with the equating of German field post offices and field post numbers. These are studied very carefully because they assist in identifying units mentioned in messages, in captured documents, and in interrogation of prisoners. Because there was much need for this information at the Ministries as well as at BP the job was undertaken by Captain Holroyd in order to equate the field post offices with the field post numbers—the assignments are all random. Captain Holroyd works in close collaboration with the "Battle Order Group", a combined show in London.

Another section, under Mr. Pickering, studies the messages of the "Mustard" cryptonet, which messages report the results of German "Y" work. (By a study of these messages the British are able to get accurate information on Order of Battle of the Russian army and air force.)

Another section, under Professor Norman, (Germanic Philology at Cambridge), deals with the technical side of intercept in air warfare.

Another section, under Mr. Saltmarsh, (another "old timer" of GC & CS), deals with the geographical side such as German map references, codes, thrust lines, and targets, etc. He also prepares information regarding similar subjects for the Naval Party especially as regards areas in the Mediterranean.

SECRET

DECLASSIFIED

Authority NND 963016

By wp NARA Date 6/6/03

SECRET

One interesting thing I learned about his work is as follows: it seems that the GAF undertakes anti-submarine patrols in the Mediterranean and the German naval command sends messages to the GAF telling them where no such patrol should be sent. This gives direct information as to where a German submarine is, for the purpose of notifying the GAF not to send an anti-submarine party there is, of course, to prevent the possibility of their bombing one of their own submarines.

The General Intelligence Section gets out occasional reports¹ called "Salus". These are "appreciations" on subjects of special interest to his own section. For example, I saw two Salu reports, one entitled "German Intentions in the South Caucasus", the other entitled "Possible appearance of another Fliegerkorps in France."

I spent some time with Mr. Pickering, since I was interested in the information which they were able to obtain from their reading of German "Mustard" cryptonet messages dealing with "Y" work. There are two or three sources of this material since German "Y" work was done in Tunisia, in Rome, and on the Eastern Front. With regard to the German "Y" work in Tunisia, the headquarters of the service are at Rome and are designated as WA7. They had one fixed intercept station (in Sicily ?) working on fairly high-grade American and British cryptanalytic systems. They also had a forward echelon on Tunisian soil covering plain language and low-grade systems. This company, known as NFAK 621, though a long-range signal reconnaissance company, always worked close to the front. It seems that the Germans listened to a lot of plain language and got a great deal out of it. As to what the Germans were able to get out of British and American front-line codes, it appeared that the Germans had considerable success with them but BP was not yet in a position to state definitely what codes were involved and were making inquiries from African Headquarters. It was definitely established, however, that the main leakage was from the air-liaison-officer nets which accompany each army and division. Many of these used code carelessly. On two occasions the call signs for the next three days for a certain group of units were given away. It also appears that the Germans have a very efficient D/F and that they get good Order of Battle information by locating

¹So called because they are prepared by Messrs. SALTmarsh and LUCas.

SECRET

DECLASSIFIED

Authority NND 963016

By Wp NARA Date 6/6/03

SECRET

stations. Our cover names and grid references were apparently easily understood. In particular, the "Y" company in Sicily was able to translate grid references immediately into plain language bearings.

As to what the headquarters of "Y" service at Rome were able to get, Mr. Pickering found it impossible to say because no detailed results were at hand by the time the Tunisian campaign had been completed. There was, however, no evidence to indicate that the Germans were able to read the high-grade systems, although Mr. Pickering admitted there was a possibility that the "Y" headquarters at Rome would not use radio for reporting such results but might send them on to Berlin or to the German GHQ by courier plane. There was nothing of cryptanalytic importance found on E circuits going back to Berlin, but Pickering said that they knew that the principal cryptanalysts and experts were in Berlin. The main German Army "Y" and cryptographic center at Berlin is known as "Inspectorate 7"; the main Navy "Y" and cryptographic center there is known as the "B" office of the Supreme Command of the Navy; the main German Air Force "Y" and cryptographic center is known as the "Crypto Office, C-in-C, GAF". These services are not unified. There is still another "Y" center in Berlin which apparently works on diplomatic. The foregoing names are based on information contained in reports passing from Athens to Berlin via the Geheimschreiber. At the present time, the traffic is not very interesting. They found in the old days that the Germans used to read the Syko currently but are not doing so now. There was then a GAF "Y" station off the coast of Denmark that used to work on the Syko traffic of the North Atlantic and coastal waters; this station then moved south to work on Mediterranean traffic.

Mr. Pickering stated that one of the men in the German "Y" unit in Tunisia was taken prisoner by the British and he was able to explain sufficient of the working of this group to "make our signals people sit up". The 9th Company of each GAF signal regiment does "Y" work, including D/F. They pick up sighting reports in self-evident code or emergency signals; they count aircraft landings and take-offs, ferrying flights, transport flights and operational flights from Malta, etc. They also listen very carefully for radiophone conversations from which they get a fair idea of the location of the principal British and American stations. However, in a good many cases they get erroneous information. In the case of the South Africans,

SECRET

DECLASSIFIED

Authority NND 963016
By wp NARA Date 6/6/03

SECRET

because of their peculiar dialect, their units can always be spotted easily.

Mr. Pickering said that he had seen at no time any evidence that the Germans had been able to get anything out of our Converter M-209 traffic. He also told me (what I already knew) that there were cryptanalytic exchanges between the Germans and Japanese at Helsinki. He had no data with reference to the relations between the Germans and Japanese in Berlin. He told me there was some evidences of cooperation between the Germans and Italians. Although there was no information regarding the Italian "Y" service in terms of offices or units, but GC & CS had evidence that the Italians were able to pass information concerning ship movements to the Germans and that the Italians had intercept detachments in Tunisia. There were no examples of their work but they do know that the NA 7 in Rome was at one time much concerned about the possibility of the Italian forward "Y" Party in Tunisia being captured.

I looked very briefly at three reports which Mr. Pickering had before him. One was a report entitled "The German Y Service on the Eastern Front from October 1942 to March 1943". Another was entitled "A Report on the German Y Service in Tunis", and a third was entitled "Axis Watch on Signals of Allied Air Force in Tunis".

I next visited Professor Norman who has the technical subsection dealing with night fighters and radar.¹ His principal work is to get all the information he can from a study of F messages relating to the German radar system and how it is used to control their night fighters in their operations against British night bombers. I saw in Professor Norman's section a very large map on which had been charted the locations of German radar stations as determined from an intelligence analysis of the E traffic, largely on the "Cockroach" and "Brown" cryptonets. It was a marvel of precision and accuracy. From the very elaborate picture that has been built up the British night bombing operations can now be carefully directed with regard to the course to be flown in order to cross certain boundaries in such a manner to cause the greatest confusion and

¹In my first few minutes with Professor Norman I was a bit confused by his use of the term "RDF". When it dawned upon me that he meant "radar" I told him what our term was and it seemed to him an apt one. He had never heard it!

SECRET

DECLASSIFIED

Authority NND 963016

By W/p NARA Date 6/6/03

SECRET

disorder in the German night-fighter organization, since the German night-fighters are not permitted to cross these boundaries. In addition to locating accurately the radar stations they also give the frequencies used, the particular type of signal, and the call. More information concerning this subject will be found in my report on the work done at Cheadle in connection with the so-called "Little Screws".

The information which Professor Norman uses as a basis for his work comes largely out of "Cockroach" traffic. Messages on the different cryptonets come to him for translation and emendation and he reports to the Air Ministry what he thinks will be of interest. Most of the time, however, he produces special notes and summaries, although occasionally if a message of importance turns up its contents will be telephoned or teleprinted to the Air Ministry.

Radar zones in addition to those in Northern France and the Low Countries have also been set up in Roumania to protect the oil fields. There were similar zones in Tunisia, Sardinia, and Sicily.

Professor Norman said that in his opinion the German radar was not as good as our own, but that they had a marvelous ground organization for directing the movements of the night fighters.

D. THE LIAISON SECTION

The Liaison Section comprises Wing Commander Oeser (OIC), a Captain Crawford, and three women. Captain Crawford in civil life is a professor of biology at one of the leading universities. W/C Oeser's background is very interesting. He is a Ph.D. in mathematics and physics, having taken two degrees in Germany. A problem in astrophysics brought up questions of color vision, whereupon he turned to experimental psychology. This carried him to the United States, where he had a fellowship at Yale and conducted an important field investigation for the Institute of Human Relations. He returned to England as soon as war began for he had been in the RAF Reserve and had had three years flying experience. However, he was assigned to duty at BP immediately upon his return. Hut 3 was then under a Captain Humphreys and W/C Oeser qualified as one of the Duty

SECRET

DECLASSIFIED

SECRET

Authority NND 963016By 46p NARA Date 6/6/03

Officers in Hut 3. Soon he became the head of the Air Section of Hut 3. He found that the E had just been broken and was the only one that had been solved. This was in November 1939. From the middle of May 1940 they started solving the "Red" key fairly regularly. During the Norway campaign they broke another key and now 70 or more are being handled. He was the one who brought in and trained the advisers in the Operational Watch.

W/C Oeser stated that naturally it was physically impossible to intercept all E traffic and also to break the whole lot every day and that somebody must set up intercept as well as processing priorities. Hut 6 asks what cryptonets the intelligence people want intercepted, which of them they want broken, and the relative priorities which should be followed in breaking them. In Hut 3 itself translation priorities must be set up in the processing of the deciphered texts. W/C Oeser started a few notes when he first came on the job and from this small beginning the Liaison Section developed. It is now his responsibility to study the traffic from the intelligence view point and to set up (1) intercept priorities for the intercept control people, in Mr. Coleman's section of Hut 6, (2) solution priorities for Mr. Fletcher's operating group under the Operational Watch in Hut 6, and (3) processing or translating priorities for the various intelligence Watches in Hut 3.

The Liaison Section has several additional functions: it provides liaison between the various other sections of Hut 3 with other groups at BP; it has charge of regulating the flow of material within Hut 3 so as to insure that intelligence gets to the Ministries and overseas commands in proper priority and within the shortest possible time; and it receives and distributes all processed material other than E material coming to Hut 3.

In talking with Wing Commander Jones I learned that there had been a certain amount of misunderstandings between Hut 3 and Hut 6 people before the Liaison Section was established and that since then the relations between them had greatly improved.

The primary function of the Liaison Section, viz., that in connection with the establishment of processing and intercept priorities, was naturally of greatest interest to me. It has been reduced to a statistical basis so as to eliminate so far as possible all guesswork..

SECRET

DECLASSIFIED

Reproduced at the National Archives

Authority NND 963016 **SECRET**
By 46p NARA Date 6/6/03

What the people in this section do is to assess the intelligence value of the messages of each cryptonet and this they do by several methods. One of the best of them involves an intelligence evaluation schedule, and will now be described. After the messages have been processed, they are sorted according to cryptonets and then separated into four classes: first-rate material is given a value of 10 points; second-rate material, a value of 3 points; third-rate material, a value of 1 point; and fourth-rate material (the so-called "quatsch"), a value of 0. These four classes correspond, of course, to the four classes into which the messages are sorted, as noted in one of the preceding sections. Material of the first class corresponds to that on which operational signals have been sent to overseas commands; material of the second class is also very important but not of immediate operational nature; material of the third class contains useful intelligence but not of great importance nor operational in character. Then the number of messages in each class is taken into consideration, the point value being multiplied by the number of messages in each class, thus weighting the classes. The product is known as D_1 , or "intelligence density". For example, if there were in a given cryptonet 3 messages of the first class, 10 messages of the second class, 50 messages of the third class, and 2 of the fourth class, the total weighted point value of the 65 messages is 110 points. This total divided by 65 gives a D_1 or an "intelligence density" of 1.69, which can be compared with the D_1 values for other cryptonets. A value of 1.0 is considered worthwhile intercepting but is of no special urgency.

The D_1 factor gives a guide as to cryptonets whose messages should be processed most expeditiously throughout all the operations in Hut 6 and Hut 3. It also yields a basis for roughly determining the value of the messages of the cryptonet for comparison with other cryptonets as sources of intelligence.

The D_1 factor is, however, only one of two factors taken into consideration in accurately assessing the intelligence value of a cryptonet. The other factor is volume, or V_1 , and records of volume give a good idea as to what cryptonets are consistently high yielders of intelligence. Consequently, by taking into consideration by-factors, D_1 and V_1 , one can get fairly good bases for determining not only what cryptonets are most valuable but also some guide for the relative priorities which should be followed in processing their respective messages. Graphs are therefore drawn, in which both factors enter.

SECRET

DECLASSIFIED

Authority NND 963016

SECRET

By Wp NARA Date 6/6/03

The "intelligence density" or D_1 is plotted against the volume or V_1 , for a number of cryptonets and these graphs are maintained current by monthly studies. In these graphs V_1 , in hundreds of messages, serves as the Y coordinate and D_1 forms the X coordinate. The points are plotted for a week, for example, and then a "center of gravity" of the loci of the V_1/D_1 points for the seven days traffic of each cryptonet is calculated. This merely means that a central point on the graph about which the various loci (determined as specified above) cluster will give a good measure of the V_1/D_1 value for each cryptonet. When the "Red" cryptonet is charted in this way it gives a consistently high value, that is, the center of gravity for this cryptonet is higher than that for any other cryptonet on the chart. Naturally, "Red" messages are collected and processed with greatest priority.

Daily analysis of this type has been found to be too variable and at the present time the calculations are made on the basis of weekly traffic counts and intelligence evaluations. Of course continuity of studies over a number of weeks is vital.

Other sorts of graphs are made also. Graphs of total intelligence produced and also of intelligence of specific kinds or from specific areas are made. For example, there was one graph on which were plotted the values for cryptonets yielding intelligence concerning North Africa. It disclosed the interesting fact that the "Red" cryptonet, which is the general GAF key and is used over a very extensive area of which North Africa is only a relatively small part, nevertheless consistently yielded more intelligence regarding that area than did other cryptonets used exclusively in North Africa.

In my talks with various people in Hut 3 I was somewhat astonished to learn that they regard the importance of E traffic to be on the wane and that what they call the "fishes" traffic¹, is becoming more and more important to them as a source of long-term strategic intelligence. This is probably not in any way connected with a suspicion or inkling on the part of the Germans that their E traffic is being read; it may be merely the result of the greater speed and facility of intercommunication, by means of enciphered teleprinter signals, among the principal

¹This comprises the traffic known as "Tunny", "Sturgeon", etc., which will be discussed in a subsequent report.

SECRET

DECLASSIFIED

Authority NND 963016

SECRET

By Wp NARA Date 6/6/03

headquarters of the high command. It is, of course, beyond question that the enciphered teleprinter service is very much faster than the E service, which uses only a light-indicating, non-printing machine, could ever be. There seems to be no reason to suppose that the Germans have mechanized their E machines and provided any of them with automatic printing. It is also true that the Germans themselves apparently regard their crypto-teleprinter as more secure than their E machine and are continually modifying the former, trying to increase its security. Nevertheless it will probably remain true that E traffic will continue for sometime to be the main British source of factual information and operational intelligence regarding the GA and GAF.

In the control of intercept the Liaison Section exercises advisory powers but in the control over cryptanalytic processing speed, it has absolute powers—the last word, in fact.

The whole day's traffic in each cryptonet goes in a book together with technical data regarding frequency, calls, time of origin, etc. These texts are read and point values are assigned them as indicated above.

In their work, Wing Commander Oeser and Captain Crawford are assisted by three women who have been in the section for a couple of years and worked in various other sections of Hut 3 before that. Their experience on the intelligence side is sufficiently broad to make them capable of assessing the operational value of the messages.

E. THE SIGNALS SECTION

This section, under Captain Turner, is responsible for forwarding the signals and teletype reports agreed upon among the advisers in Hut 3 to the respective Ministries, to overseas commands, and to other points with which communications with Hut 3 must be maintained. It was stated by Wing Commander Jones that on the average 75000 to 10,000 sheets of paper pass through the Signals Section daily; that during active operations in the Tunisian Campaign approximately 100 "signals" were sent daily to the commands there.

The messages as they come from the Duty Officer in draft form bear an indication of the command or headquarters to which

SECRET

DECLASSIFIED

Authority NND 963016

By Wp NARA Date 6/6/03

SECRET

they should go. Each message is logged and given a serial number; the source, the priority, the originator, reference number, etc., are shown. The message is then passed to a typist, who makes 10 copies for multiple distribution. One of these copies goes to the Communications Center at BP where the message is teleprinted to the Ministries or, if to be sent by radio as a "signal" to an overseas command, is cryptographed and then transmitted by BP's own radio station at Windy Ridge, near London, the keying being by remote control from BP. Only Typex with special settings (Leonard) and 1-time pad systems are used for cryptographing MSS material. The 1-time pad systems are used in the forward regions where Typex machines cannot be safely held.

The original message is then returned to the Signals Section where a second logging takes place to show additional information such as time of transmission; priority; transmission message number; a BP number for the cipher office operator, etc.

As noted above the Typex, code, and radio operations are not directly under Captain Turner, the chief of the section, but he merely passes the messages for these operations to the Communications Center of BP. The latter will be briefly described at the end of this section.

At this point it might be well to indicate that the communication network employed to transmit this material of a highly secret operational nature to overseas commands is separate and distinct from any military, naval, or air force administrative or operational networks employed by service agencies. The circuits used comprise a special system called the SCU or "Special Communications Unit"; this has already been referred to in a preceding section of the report.

One of the interesting things which I learned in my visit to this section was that they take great precautions so as to prevent disclosing the nature of the information transmitted by radio over the Special Communication Unit networks. For example, several weeks before the end of the Tunisian Campaign it was realized that, unless precautions were taken in advance, there would be a sudden tapering off of traffic over the circuits hitherto used for forwarding the intelligence coming from Hut 3 to the twelve Mediterranean points mentioned in another part of this report. Consequently, an elaborate plan was drawn up for the transmission of "dummy" traffic equivalent in

SECRET

DECLASSIFIED

Authority NND 963016
By 4p NARA Date 6/6/03

SECRET

character and amount to that which was normally carried during active operations. In setting up the plan, detailed studies were made of actual traffic for the preceding few weeks so as to obtain statistical bases for accurate camouflage. They not only studied the lengths of messages, the number of "Z" messages of each kind, the times of origin, etc., so as to insure that the simulated messages would be almost identical externally with the real traffic, but also they even went to the trouble of ascertaining quite accurately the usual delay time incident to enciphering or encoding the messages, so that the time of origin shown on the message and the time of transmission (or intercept) would show the normal delay in each circuit. In addition, elaborate instructions were drawn up with reference to the number and kinds of requests for checks and repeats that should be sent back to BP so as to correspond with what would normally be expected to come from the Mediterranean stations, so that even in this respect the dummy traffic would also appear legitimate. As for the texts of the dummy messages, these consisted of 1-time pad groups prepared exactly as are the pads used for enciphering code; the pages of the pads were, in fact, destroyed as their groups were used up. Special indicators were provided so that no time was lost in recognizing the dummy traffic. This elaborate procedure and camouflage went on for a sufficient period after the collapse of the Germans in Tunisia (about 4 or 5 days) so as to provide a good cover, and then the traffic was allowed to taper off gradually until its final disappearance about ten days after the end of the operations.

Reference was made on page 104 to the very important organization known as the "SCU" or "Special Communications Unit". There was, of course, no opportunity to observe any of the field echelons of this organization but I did have a fairly good look at the central operations office at BP, which forms a part of what is called the "Traffic Reception and Communications Center" in a building called "Block E".

The "Traffic Reception and Communications Center" has a staff of about 400 people and serves exactly the same functions as our Message Center in E Branch. The teleprinter room had, at the time of my visit, a battery of 64 teleprinters. They are operated by three shifts of 48 WAAF's, of which about 30 are on duty per shift. Some operators take care of two or three machines.

Since this office serves as a traffic reception center the largest part of its business is in connection with the

SECRET

DECLASSIFIED

Authority NND 963016

SECRET

By Wp NARA Date 6/6/03

incoming traffic from the intercept stations. The messages bear symbols to facilitate primary sorting and routing to the respective sections at BP to which they must go. The symbols are in the form of simple words, those beginning with A indicating traffic for the Air Section, those beginning with N, for the Naval Section, etc.

The messages are now forwarded by belt conveyor but I saw a pneumatic tube layout which I was told was soon going to replace the belt conveyor system.

Although most of the traffic comes by teleprinter to this central reception room, in several cases service is direct to the section involved, the teleprinters being in the respective sections themselves, thus considerably speeding up the reception of the messages which must be processed as fast as possible.

Some of the incoming traffic arrives not by teleprinter but by Morse radio siphon recorder. These messages come from overseas intercept stations and are enciphered by Typex machines before transmission. Decipherment of the siphon recorder slips is accomplished here by several WAAF operators who have been trained to interpret the siphon record and to operate the keyboard of the Typex machines simultaneously, thus saving one operation.

The outgoing teleprinted messages to the intercept stations, to the Ministries in London, and to other points in the U.K. also are handled in this teleprinter room, where fast service must be given.

The switching central for teleprinter service is also in Block E and was quite a large affair. It must be so because BP is in fact the most important center for intelligence operations of the whole British Government.

As regards the "signals" to overseas commands, the messages as drafted by the advisers in Hut 3 (or in some cases, by the various other sections of BP) come to the communications center for cryptographing and transmission. These are enciphered by Typex machines for the most part, although 1-time pads are also used. The operators who handle these "operational signals" are the oldest and most trusted WAAFs. At present the traffic is enciphered by 16 different keys and there are 60 Typex machines reserved for this purpose. After encipherment and before transmission all outgoing "signals" are deciphered by

DECLASSIFIED

Authority NND 963016

SECRET

By Wp NARA Date 6/6/03

another WAAF operator on a different Typex to insure the absence of errors. When I indicated that we saved this step by a tandem operation the officer in charge of this unit expressed deep interest in how this is done by us and stated that he would try it out on his own machines.

A brief visit was made to the radio room where keying of the transmitters by remote control takes place. (The radio station itself is located at Windy Ridge, just outside London) Also, incoming signals received at that station are "piped" to the communications center where the siphon recorders and automatic Creed printers were seen. At the time of my visit some high speed automatic printing (Creed) of incoming signals was observed. The incoming Morse signals were received on a perforated tape; the latter was then passed through a high-speed translator which printed the text on a narrow slip; the latter was then pasted up on sheets. It was said that this high-speed channel enabled them to receive a very large volume of traffic directly from the overseas intercept stations.

The BP terminal of the new Varioplex Cable circuit (three channels) is also in Block E. When I was shown the apparatus I was invited to send a greeting to Captain Maidment in New York, a very prompt reply being received.

The numerous teleprinters, Typex machines, etc., are serviced and kept in repair by a special maintenance staff attached to the "Traffic Reception and Communications Center".

It is obvious that the guiding heads of BP realized some time ago that the key to efficient operations in this field lies in speedy, effective, electrical communications. Accordingly they built up a fine organization to accomplish the purpose, using the best and latest machinery that could be obtained, and sparing no expense to further this important phase of their operations.

F. THE TRAFFIC ANALYSIS SECTION

It has been noted in connection with the discussion of the Central Party in Hut 6 that a certain amount of T/A work for Hut 6 people is done under Major Lewis, who is a member of No. VI Intelligence School¹. Major Gadd, who is in charge of

¹Since the foregoing was written, No. VI Intelligence School has been abolished as a separate entity. Major Lewis' section is now definitely a part of Mr. Welchman's organization, Major Gadd's section is likewise a part of W/C Jone's organization.

DECLASSIFIED

Authority NND 963016

By wp NARA Date 6/6/03

SECRET

Hut 3 T/A studies, also belongs to this school, does T/A work, as does Major Lewis, but the former operates in more direct collaboration with the Intelligence people in Hut 3 than with the cryptanalytic people in Hut 6. There is perhaps a bit of overlapping and duplication of work as between what Major Lewis' party does and what Major Gadd's party does, but in view of the flexibility of their organization and because the two groups work practically side by side there is not as much duplication as might be anticipated.

There are five sections under Major Gadd, shown in the accompanying diagram. Their functions are as follows:

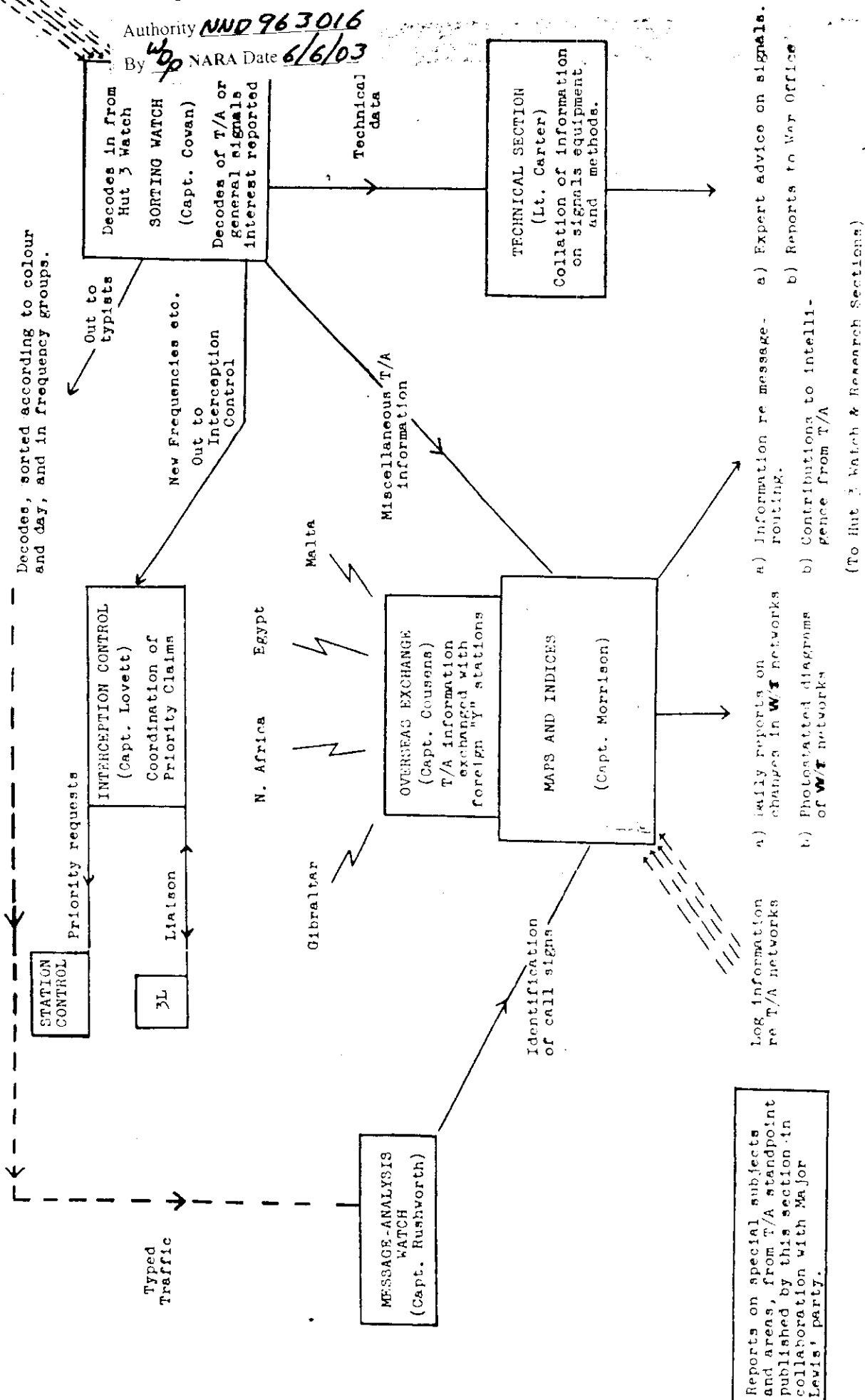
- (1) The Sorting Watch. This is under Captain Cowan and really constitutes what has been described above as the German Book Room. Decipherments containing T/A information or information in connection with the German communications in general are studied very carefully. New frequencies, new routings, and so on are reported to the Intercept Control Section mentioned above. It also sends miscellaneous radio information to the Maps and Indices Section under Captain Morrison, as well as technical data concerning radio communication to the Technical Section under Lt. Carter.
- (2) The Research Section. This is under Captain Rushworth. It maintains close liaison with the Fusion Room people of Hut 6 under Major Lewis but the main object of the research is to provide information for the Intelligence people in Hut 3 rather than the cryptanalytic people in Hut 6. The section endeavors to tie up call signs with signatures and addresses so that the origin and destination can be established for messages lacking these elements. It also keeps track of the general contents and character of traffic on the various cryptonets, of the various methods of routing messages, of the usual topics of conversation between units or individuals, etc. All of this is of value to the Operational Watch and advisers in Hut 3 in reporting messages to the Ministries and preparing signals to overseas commands. It is also of considerable use to Wing Commander Oeser in his studies on intelligence and processing priorities.

SECRET

DECLASSIFIED

Authority **NND 963016**
By **46p** NARA Date **6/6/03**

MAJOR GADD'S SECTION OF No. VI I.S.



DECLASSIFIED

Authority NND 963016

By wp NARA Date 6/6/03

SECRET

- (3) The Intercept Control Section. This section functions in this connection for the whole of BP and is under Captain Lovett. It has as its principal function the coordination of priority claims as between the people in Hut 3, Hut 6, No. IV Intelligence School, the Air Section, the Naval Section, etc. There is in this connection, of course, very direct liaison between Captain Lovett and Wing Commander Oeser, who sets up, as regards E traffic, the various processing and intercept priorities based upon the intelligence value of the various cryptonets.
- (4) The Technical Section. This is under Lt. Carter, who correlates information coming out of deciphered messages and dealing with German radio equipment and methods. He is able to supply expert advice to the intercept stations with regard to the German radio sets and he also makes reports to the War Office in the same connection.
- (5) The Maps and Indices Section. This is under Captain Morrison. He receives from Major Lewis' Log Reading Section information coming out of the logs with respect to the radio networks of the GA and GAF. He also receives information concerning identification of call signs from the Research Section under Captain Rushworth and miscellaneous radio information from the Sorting Watch under Captain Cowan. In connection with this section there is a group which is called the Overseas Exchange. Here is where T/A information is exchanged with "Y" stations overseas. This subsection is under Captain Cousens. The Maps and Indices Section puts out daily reports on changes in the GA and GAF networks and diagrams of those networks. It sends out to Major Eabage and to the Operational and Back Room Watches of Hut 3 information regarding message routing and contributions to intelligence from T/A.

This whole section under Major Gadd gets out reports on special subjects and geographical areas from a T/A standpoint. This is done in collaboration with Major Lewis' party. As noted above the principal function of the whole party is in connection with the identification of call signs and the adding up of intelligence by providing signatures where they are lacking, by bringing

DECLASSIFIED

Authority NND 963016

By wp NARA Date 6/6/03

SECRET

to the knowledge of the Intelligence people things which are not apparent from T/A research alone, and supplying data for predicting what will be carried over particular frequencies in the event of reorganization of the German networks.

G. THE GERMAN BOOK ROOM

The function of this section is to prepare in book form a copy of every message on each E cryptonet regardless of its contents, and regardless of whether or not it has been teleprinted to the Ministries or sent abroad in the form of a signal. The books are intended merely for internal distribution, reference, and study by the various sections of EP.

From the Watch Room a register is received in the German Book Room showing reference data regarding every message which should arrive in the room. On their arrival in this room the actual messages are checked against the register. The messages as received have been already sorted according to cryptonets (this is done in Major Gadd's section). A second sort is made here, the messages being arranged according to the German time of origin. There is, therefore, finally a book containing all of the messages in each cryptonet arranged in this manner for each day. Six copies of each book are made. At the beginning of each book there is an index of the frequencies or cryptonets covered.

Each message shows the following data:

- (1) Frequency on which message was first sent.
- (2) Register number of message.
- (3) Intercept station symbol.
- (4) German time of origin.
- (5) Time of interception.
- (6) Calls.
- (7) Whether KR (urgent) or not.

SECRET

DECLASSIFIED

Authority NND 963016

By Wp NARA Date 6/6/03

SECRET

- (8) Number of parts.
- (9) External or message indicator.
- (10) Actual indicator.
- (11) German emended text.
- (12) References to the teleprint number, or report number, or message number if sent by signal.

An exact copy of the German text of the message is made. Items that were spelled out in the original but are indicated only by symbols in the typed form are underlined. For example, if the number 54 was spelled out as "fünf vier" in the message, it would be typed out as 54 and underlined.

In addition to typing up the E messages the German Book Room also types up in the same form all of the Double Playfair traffic and the Geheimschreiber traffic. The latter is typed up in a somewhat different manner from that in which the E is typed up and appears in the book according to the frequency, serial number, and time the transmission ended.

The German Book Room has a total of 27 women of which only two are purely clerical. They must know German quite well and must be of good intelligence. After a training period of three or four days they are set to work. For the first month a more experienced operator checks everything that the trainee does.

The German Book Room handles about 1000 messages each day and operates in two shifts. About the only reference material maintained in the section consists of a special list of German abbreviations and their meanings, with indications as to how the abbreviations should be capitalized for the purposes of standarization.

SECRET

SECRET

APPENDIX

THE NUMBER OF PLUGGING POSSIBILITIES ON THE
GERMAN MILITARY ENIGMA MACHINE¹

Let us first consider the case where no letter is self-steckered. The first pair can be chosen in $\frac{1}{2}(26 \cdot 25)$ ways, the second in $\frac{1}{2}(24 \cdot 23)$ ways,, the last (thirteenth) in $\frac{1}{2}(2 \cdot 1)$ ways. The number of choices is, then,

$$\frac{1}{2}(26 \cdot 25) \cdot \frac{1}{2}(24 \cdot 23) \dots \frac{1}{2}(2 \cdot 1) = \frac{26!}{2^{13}}$$

But since we are interested in the steckerung, which disregards the order in which the pairs are chosen and is concerned only with the combination of the 13 pairs involved, we see that the total number of steckerung possibilities when no letter is self-steckered, is:

$$A_0 = \frac{26!}{2^{13} \cdot 13!}$$

Similarly, if one pair of letters is left self-steckered, the corresponding number of possibilities is:

$$\begin{aligned} A_1 &= \frac{\frac{1}{2}(26 \cdot 25) \cdot \frac{1}{2}(24 \cdot 23) \dots \cdot \frac{1}{2}(4 \cdot 3)}{12!} \\ &= \frac{26!}{2^{12} \cdot 12! \cdot 2!} \end{aligned}$$

In general, if α pairs of letters are left self-steckered and if A_α is the total number of steckerung possibilities for this case, then

$$A_\alpha = \frac{26!}{2^{13-\alpha} (13-\alpha)! (2\alpha)!}$$

¹Prepared by Daniel M. Dribin, T/3 Signal Corps (29 June 1943).

SECRET

DECLASSIFIED

Authority NND 963016

By 4p NARA Date 6/6/03

SECRET

The maximum A_d occurs when $d = 2$, as is evident from the following numerical values or by taking the ratios of successive A_d .

$$A_0 = 7,905,853,580,625$$

$$A_1 = 102,776,096,548,125$$

$$A_2 = 205,552,193,096,250$$

$$A_3 = 150,738,274,937,250$$

$$A_4 = 53,835,098,191,875$$

$$A_5 = 10,767,019,638,375$$

$$A_6 = 1,305,093,289,500$$

$$A_7 = 100,391,791,500$$

$$A_8 = 5,019,539,575$$

$$A_9 = 165,038,875$$

$$A_{10} = 3,453,450$$

$$A_{11} = 44,850$$

$$A_{12} = 325$$

$$A_{13} = 1$$

SECRET

DECLASSIFIED

Authority NND 963016By wp NARA Date 6/6/03

$$x = \frac{26!}{2^{13-x} (13-x)! (2x)!}$$

$$\begin{aligned} A_1 &= 13A_0 \\ A_2 &= 2A_1 \\ A_3 &= 11/15 A_2 \\ A_4 &= 5/14 A_3 \\ A_5 &= 1/5 A_4 \\ A_6 &= 4/33 A_5 \\ A_7 &= 1/13 A_6 \\ A_8 &= 1/20 A_7 \\ A_9 &= 5/153 A_8 \\ A_{10} &= 2/95 A_9 \\ A_{11} &= 1/77 A_{10} \\ A_{12} &= 1/138 A_{11} \\ A_{13}(-1) &= 1/325 A_{12} \end{aligned}$$

Number of Stepping Possibilities (= A_x)