Interrogation Report on POW TEMP Enrique

[Handwritten notes]

Date: 26/7/45

[Signature]

DOR for [Redacted]
Attached is a copy of a interrogation report on POW Enrique

who worked at OKW 4 SKL III, 1943 - 1944, thereafter serving

with the 5 Groups HERVI and HANNO as assistant cryptographer

and translator.

Items of particular interest are:

Pages 9 - 12. Details of cryptanalytic work on British Naval Code

(Multiplex) (Braun - Auxiliary Vessels).

"Traffic became unreadable on 1st January 1944 and continued
to be so" - page 10.

Page 20.

(a) Naval Cipher No. 3 (Frankfurt). - No success after
February 1943.

(b) LODH and CONUL. - Traffic read until the end.
FIRST DETAILED INTERROGATION REPORT ON

TEMP Enrique.

Name : TEMP Enrique.
Rank : Matrose (Civilian in equivalent rank).
Unit : "B" GRUPPE SAN REMO (German Navy).
Function: Asst cryptographer & translator, later WT Mechanic.
P.P. No. : 02516 (?)
Captured: 10 May 45, GENOA.
Secret No : M35/611
Interrogated: CSDIO/CMF 1 - 12 Jun 45.

INDEX

1. PRELIMINARY................................................................. 2
2. HISTORY AND MOVEMENTS.................................................. 2
3. ORGANISATION OF GERMAN NAVY INTERCEPT SERVICE ("B" - DIENST)..... 3
   a. CEN SSK............................................................... 3
   b. Chef MND............................................................ 3
   c. 8 SSK III............................................................ 3
   i. Cryptographic Service........................................... 3
      (a) The "General Referate".................................... 3
      (b) The "Referate".............................................. 3
      (c) The Seas &/or Groups..................................... 4
      (d) Personnel.................................................... 4
   ii. Intercept and DF Service....................................... 5
      (a) The Naval DF HQs (MF Abt)............................. 5
      (b) The Naval Main DF Stns (MfHS).......................... 6
      (c) The Naval DF Sub-Stns (MPNz).......................... 6
      (d) The "B" Gruppen............................................ 6
   4. LOCATIONS (A - C)..................................................... 7
   5. EQUIPMENT (A - C).................................................... 8
   6. WORK AT 8 REFERAT (MUNCHEN BRAUN) - THE AUXILIARY VESSELS CODE....9
      a. History............................................................ 9
      b. Description of Code and Recipher System.................. 10
      i. The Code Book............................................... 10
      ii. The Recipher System....................................... 11
      iii. Traffic and Indicators................................... 11
   C. Cryptography - Methods and Results................................ 12
      i. Sorting of traffic.......................................... 12
      ii. Breaking the Recipher, Methods used..................... 12
      iii. Breaking the Recipher, Details.......................... 13
         (a) Pairs of indicators...................................... 13
         (b) "Suspected" subtractor group........................... 13
         (c) Chance repeats.......................................... 14
         (d) "Rolling".................................................. 15
         (e) Deciphering of indicator groups....................... 16
            (1) "Chain of indicators".............................. 16
            (2) "Ring of indicators"............................... 16
INDEX (continued).

(f) Differencing ............................................. 17
(i) " as an aid to rodcipher & code breaking .................. 17
(x) " for the purpose of mixing pairs ("Serian") ............ 18

IV. Registration of Code Groups .................................. 19

7. WORK AT AN REFERAT (FRANKFURT) & OTHER SITES ......... 20
A. The FRANKFURT System .................................... 20
B. RN and US Navy Tactical Codes ............................. 20

8. THE U-BOAT DF SERVICE .................................... 21

9. WORK AT GRUPPEN NEIyi. AND SAN REMO .................. 21

10. PERSONALITIES .............................................. 21

Appendix "A" - Pattern of German Navy Intercept W/T Form ....... 23
  "P" = " " " " " " " " " Log Book Form ..................... 24
  "Q" = Details of W/T Stations covered by German Navy Intercept
       Service, Call signs & Frequencies memorised by PW ........ 25
  "R" = Description and use of "Rollmaschine" (v. sketch) ........ 29
  "S" = PW's description of U-BOAT Special DF apparatus and ex-
       ploits of a DF Operator (in German and English translation) 31

1. PRELIMINARY

PW is a fairly bright young man of 26 of mixed German and Spanish origin. He
claims to be a Spanish subject. His story is an unusual one, and his manner
does not inspire confidence; at the same time there seems to be no obvious reason
why he should want to mislead, unless he hopes to be repatriated to GERMANY thereby
avoiding internment. He talks freely, almost too willingly. Technical information
is believed to be fairly sound, in spite of the fact that PW is not a cryptographer.
PW speaks English, German, Spanish, French and a little Italian.

Reliability: Fair. (Interrogated by A.G.B.)

2. HISTORY AND MOVEMENTS

29 Aug 1918 : Born in BARCELONA as the son (posthumously) of a Spanish father,
Guillermo TEMPE, and of a German mother Maria née KUNZ. His
mother remarried, in 1927, a German teacher, SCHÜLER, who owned
a private school in BARCELONA. (SCHÜLER, born in 1900, served
as a naval cadet in the first World War and joined the German
Navy again during the present war. He comes of naval stock, one of
his uncles being an admiral).

1933 - 38 : Visited German High School at CALLE NÓVA 4, BARCELONA.
Jul - Aug 39 : Went to BERLIN to learn pharmacy. Apprenticed to Messrs BIEDELE
              HAHN.

Summer 41 : Started work at Reichsverwaltung Osthannover.
Mar 43 : Called up to German Navy, and on account of his knowledge of
         English, posted to Cryptographic Service. (OKM SKL CHEF MENIII).
Mär. 43 : Started work after a fortnight's course.
Dec 44 : Transferred for reasons of health to ITALY, and posted first to
         "B" Gruppe NEIyi. Later to "B" Gruppe SAN REMO.
23 Apr 45 : "B Gruppe" SÀN REMO left for GENOA, but was stopped by a Partisan
             road block at COGIELEFO. PW intervened and organised the bloodless
             surrender of the group, consisting of an officer and 40 ORs. Remained
             with Partisans.
10 May 45 : Reported to British Naval Officer at GENOA, and taken into custody
two days later.
3. ORGANISATION OF GERMAN NAVY INTEREST SERVICE ("B" DIENST).

A. GERMAN NAVY HIGH COMMAND - K. VAL W.R. DIRECTORATES.
(REFEREIDO DER MARINE - SEKRETSLEITUNGEN - hereafter referred to as OCM SKL).

FW knew of the existence of four Naval War Directorates (SEKRETSLEITUNGEN = SKL) numbered 1 to 4, which he described as the "tactical commands" of the German Navy High Command (OKM). SKL 4 - known as 4. SKL after 1 May 44 - controlled the four HQs or bureaus dealing with the Naval Signals Service (KRIEGS NACHRICHTEN DIENST = MND) - see B. below.

B. HQs NAVY SIGS SERVICE (CHEF MARINE NACHRICHTEN DIENST = Chef MND).

Until 1 May 44, there were four HQs of the German Naval Signals Service u/c SKL 4. These were called Chef MND I - IV, their full address always being preceded by reference to High Command and Directorate, for instance OCM SKL Chef MND IV.

Chef MND I & II dealt with German Navy Signals System and own codes "W" and ciphers.

Chef MND III dealt with Intercept incl. DF and Cryptography ("FUNK ABWEHRUNG" or "BEOBACHTUNGSDIENST" = "B" DIENST and ENTLIEFERUNG = "E")

Chef MND IV dealt with Radiolocation and Defence against Radiolocation ("FUNK MEß " i.e. "ORTUNGSWEISE und ASCH" = "EWER unv")

After 1 May 44 these HQs were known as 4. SKL I - IV, all under 4. SKL.

C. 4 SKL III (Formerly OCM SKL CHEF MND III).

This HQ, till 1 May 44 Chef MND III, when its organisation was the same, is best described under its respective functions of Cryptography, and Intercept and DF. It may be assumed that on the advice of the Referate dealing with cryptography the HQ controlled the intercept and cryptographic work (low-grade only) carried out by the Naval DF and Intercept units. It is not certain whether the HQ also controlled admin and technical matters in these units.

I. CRYPTOGRAPHIC SERVICE (BERLIN).

FW does not know how the Evaluation Dept (AUSWERTUNG) fitted into the organisation. For purposes of cryptography work was organised into two "General Referate" and a number of "Referate", Sea and Groups.

(a) The "General Referate"

These were two in number, one called General Referat "F" dealing with ROYAL NAVY traffic and RUSSIAN NAVY, and the other General Referat "G" on "AMERICAN Ablaufitäler" dealing with US NAVY. As FW joined the organisation in May 43 he did not know how work was subdivided among Referate - general and ordinary - in the days when the French, Italian, Yugoslav and Greek navies etc had to be watched on the air. FW only knew the organisation of General Referat "F". This was subdivided in several Referate and smaller seas or groups, according to countries, type of traffic, tasks and geographical subdivision of enemy wireless networks. See (b) and (c) below.

(b) The Referate of General Referat "F"

There were some five Referate in all, which had both a name and a cover-name.
Referat | Cover name | Function
---|---|---
Fu Referat | FRANKFURT | Worked on High Grade R.N. codes.
Fn Referat | Muenchen Braun | Worked on R.N. Auxiliary Vessels code in use in HOME WATERS and ATLANTIC as far South as FROSTOWN (receiver changing twice monthly).
Fn Referat | Muenchen Braun | Worked on R.N. Auxiliary Vessels code in use in MEDITERRANEAN and INDIAN OCEAN (receiver changing three times a month).
? Referat | KOELEN | No details known.
? Referat | GALLIEN | Worked on Russian Naval traffic.
Fn Referat (after Dec 43) | ? | Worked on Naval Attache's traffic (see further (c) below).

One Referat dealt with SWEDISH Naval traffic.

(c) The Secs and/or Groups of General Referat "F".

These were smaller moles in General Referat "F" formed either ad-hoc and disbanded when work was ended, or permanent sub-divisions of General Referat "F" whose functions were not large enough to warrant the formation of a Referat. (NOTE: for the purpose of this report a Sec will be the name given to the former type of moleus, and a Group that given to the latter type). The groups were either run as separate moles or 4 SUB III, or worked as specialised subordinate units of various Referate. P? remembered:

Secs:
- STEPTIN: formed after the sinking of the BISMARCK, and only existed for about a fortnight.
- HAMBURG: no details known.
- BREMEN: worked from about 42 to 44, on Naval Attache's traffic.

Groups:
- FRIITZ OTTO (Fo): formed about end 43. Worked for Fu Referat (Muenchen Braun) on differencing.
- FRIITZ MAX (Fn): formed before 43. In Dec 43 took over the STEPTIN, HAMBURG and BREMEN Secs, and became Fn Referat.
- FRIITZ Quatsch (Fq): dealt with Crypto work at the Naval Main DF Stns (see II. b, below). Worked on tactical codes such as "LORD".
- "X" Gruppe: worked for Fu Referat. No details known.
- "ROLL" Gruppe: dealt with "rolling" for all Referate and Secs and/or Groups working on decipher breaking.

NOTE: The HOLLERITH Abteilung which may or may not have been part of the orgn was available for special work.

(d) Personnel:

A staff of about 700 to 800 civilians and Naval (incl Army and GaF transferred to Navy) personnel, male and female, worked at the HQ and in Crypto and Evaluation. Training was given to ALL personnel in offices by means of a 14 days course explaining generally the type, purpose and methods of the work.
Cryptographers attended the same special course which also lasted two weeks. FW stated that after 43 the OKH was constantly short of English speaking personnel. He also stated that he had been offered facilities to become an expert in cryptography, but that he had declined it. ("I felt that through my work I might do harm to a nation whose enemy I - a Spaniard (1) - am NOT.") Q's only got special try by working - unofficially - under an I/O watch (WACHTE) and trying to improve their knowledge. No special course was held as in OKH.

The staff worked in shifts called watches (WACHEN) under an I/O watch, (WACHTE) usually a PO specialized. Each watch consisted of approx 10 people, 1-2 Q's and 8 statisticians and translators. Rotation of watches proceeded as follows:

- on 3 days from 0800 to 1600 hrs.
- one day, off duty
- two days of "extra watch" (EUSCHEN) from 0900 to 1500 hrs, then as from the beginning again.

Security regs were strict. The official secrets act or regs were read out to personnel every month.

Office equipment was scarce, economy being the motto. Clerks had to buy their own India rubber outside and even getting a pencil was a task of some difficulty.

II. Naval DF and Intercept Service

There were three types of station set up for DF and Intercept, known generally as "Abt" - STELLEN, or, from a cryptographic point of view, AUSSENSTELLEN. Though the main work of most of the stations consisted of intercept of W/T and RT traffic, they were all referred to as DF (PHIL) Stations, i.e. Naval DF HQs (MARINE PHIL. AUSSENSTELLEN = M P Abt), Naval Main DF stations (MARINE PHIL HAUPTSTELLEN = MPHS), and Naval DF Sub-stations (MARINE PHIL NEUBERSTELLEN = MPN). There were also small dots called "B" - GEMEPEN.

Traffic intercepted of ROYAL NAVY, US NAVY, RUSSIAN & SWEDISH NAVIES, was sent in part by TP to 4 SKL III. Approx 2,000 messages a day were received in BERLIN from the Ausstenstellen. (Details sent by TP were the heading or preamble, and the first five and last five groups of all messages).

(a) Naval DF HQs (MP Abt)

These were the largest fixed sta. According to FW there were two in existence, one (MP Abt 'DEUTSCHES SUCHE') at WILHELMHAMBURG/SDENLEN, the other (MP Abt FLANDERN) at BRUGES (till mid-summer 44). They appear to have been formed during the war (FLANDERN for certain) or in any case raised to the status of HQs (ABTEILUNGEN). They came directly under 4 SKL III for operational control at least.

Their work was mainly intercept. Q's were attached for dealing with low grade traffic. In addition MP Abt FLANDERN trained, equipped and posted U-Boat DF and RT Intercept operators (see para 8 and App "B").

Both MP Abteilungen controlled a number of Naval DF Sub-stations (MINS).

See under (c) below.

Each MP Abt had the following personnel:

- approx 25 sets (acres = BERICHTE) with 100 WT operators.
  - 20 statisticians/clerks
  - 10 cryptographers
  - 10 orderly room and I/O personnel
  - 30 guard personnel
(b) Naval Main DF Stations (MHS)

There was a substantial number of these, some of which had been in existence since before the war, viz., MHS AKLÉNCK, LANDENBARGEN and SOEST. For other locations see para 4.

They dealt mainly with Intercept, and some under 4. SM III for operational control at least. They themselves controlled the work of the small dets ("B" - GRUPPEN), and of some of the MNS.

Personnel of each MHS was as follows:-

approx 15 sets (zones=BERECHIÈ) with 60 WT operators.
  " 10 statisticians/clerks.
  " 5 cryptographers.
  " 5 orderly room and I/J personal.
  " 20 guard personnel.

(c) Naval DF Sub-stations (MNS)

These, (for locations see para 4) concentrated chiefly on DF, though some Intercept work was done. They confined themselves to lower grade traffic. They came under either an MP Abt or an MHS. Thus, all MNS in NORWAY and the BALTIK area as far west as BIZERUM were under MP Abt DEUTSCHE BUCHT, those in HOLLAND, BELGIUM and NORTH FRANCE under MP Abt FLANDERN.

They formed a network called the "DF-network" (FELßNITZ), which however did not cooperate with the other services (Luftwaffe, etc.), for matters relating to AA defence, Coastal defence, bombing of convoys, etc. Stas used G/F LI for the purpose of intercept. E.g. if "ANSATZ Quatsch" was called over the telephone, this meant that a bearing had been obtained on a unit indicating a WT on 124.5 m (For F/L the call was "ANSATZ Quatsch - Fonie"). (Convoy escorts frequency, see also Appendix "C" para C.). The matter was reported to MP Abt FLANDERN and cuts and locations obtained reported to BERLIN. FW did not know how results were evaluated (? U-boats etc.).

Each MNS had as personnel:-

approx 5 sets (zones=BERECHIÈ) with 20 WT operators.
  1 DF operators
  2 orderly room and I/J personnel.
  Guards supplied by other Navy units.

(d) "B" - Gruppen

These were small intercept groups or dets placed in points of tactical importance. Sometimes in addition to being u/o of an MHS they were at the same time u/o of a local formation as well, e.g. "B" Gruppe NERVI was u/o 7 Security Div, but also under MNS KARUPSEE.

In ITALY at various times there were "B" Gruppen at ROME, VENICE, TREVISO, NERVI, SAN REMO and RIMINI.

Personnel varied from Group to Group. Thus NERVI had 1 officer, 2 Funkmeister, 6 NCOs, and 6 men, whereas SAN REMO had 1 officer and 40 GAs.

For details of work of "B" - Gruppen NERVI and SAN REMO see para 9.

NOTE: The following diagram illustrates the operational chain of command for the DF and Intercept Service:-

(see over)
4. LOCATIONS

NOTE: (Inf contained in sub-para C - G should be taken with some reserve).

A. OKM SKL Chief MND III
   (Renamed 1 May 44 - 4. SKL III)
   1. from beg war to 22/23 Nov 43)
      In OKM bldgs 72-76, TIRPITZ UFER, BERLIN, W.35, except General Referat "p" (Americana Abteilung) in the KUNSTSEIDE HAUSE 4, BERLIN, CHARLOTTENBURG.
      : from end Nov 43 to Feb/Mar 45
        : With OKM in PO GEN KASERN, EBERSWALDE nr BERLIN.
      : after Feb/Mar 45
        : KOLLERTH (? Abteilung
          : from 39 to Feb 44
            : Under NIKOLAI KIRCHE, BERLIN-THIERSDORF.
          : after Feb 44
            : EBERSWALDE.

B. Naval DF Hqs (MARINE FEHL ABTEILUNGEN)
   MP Abt DEUTSCHE BUCHT
     : till mid Jun 44
     : BRUGES (THIENHEND). Split into an MPH and a
   MP Abt FLANDERN
     : after bombing
     : both at BRUSSELS

C. Naval Main DF Stations (MARINE FEHL, HAUPTSTELLEN)
   MPH BRUSSELS
     : Outside BRUSSELS in or near Kings Castle.
   MPH HAMBURG
     : Near SWINEMUNDE; in existence before 1939.
   MPH BERLIN
     : NR BERLIN.
   MPH LANGENLENKEN
     : On Lake CONSTANZE. Existed before 1939.
   MPH SOEST
     : In RHINELAND nr COLOGNE. Most important sta; existed before 1939, Took US Navy traffic.
   MPH GROENINGEN
     : No details known
   MPH KIRKENESS
     : Formed in NORWAY in '40.
   MPH STAVANGER
     : Formed in NORWAY in '40.
   MPH HJERLING
     : Formed in N. DENMARK in '40.
D. Naval DF Sub-Stations (Marine Feld Poststellen).

**MPNS BRUSSELS**

- LONGCHAMPS, in blag nr the Belgian Terms Club. U/c MP Abt FLANDERN.

**MPNS BORKUM**

- U/c MP Abt DEUTSCHE BUCH. Did intercept work as well as DF.

**MPNS DEN HELDER**

- Cover name HELEN. After 6 Jun 44, also did intercept work. U/c MP Abt FLANDERN.

**MPNS MAISLOUIS**

- Cover name MAUSI. U/c MP Abt FLANDERN.

**MPNSs (two stas) BRUGES**

- Cover names: BRIGITE (DF on 100-200 m wave band (HERSTELLER), and BINO (DF on short wave traffic only). U/c MP Abt FLANDERN.

**MPNS OIP GRIEZEN**

- Bombed out in May 44, moved to NUREN T. Did Intercept work as well as DF. U/c MP Abt FLANDERN.

(? MINS T. ORAIN.

- Perhaps existed till 45 (?).

**E. German Navy Sigs Experimental Comands (Nachtlichter Versuchs Kommando)**

- NVK - KIEL (L. 6.NUH)
- NVK - PELEZERLREG (nr LIEBECK).

**F. German Navy Intercept and DF Stas in Spain.**

These were known under cover names and had locations stated below:

- M.LK CAS at MADRID
- M.LK RIVEN at SEVILLA
- M.LK NORGE at VIGO

**G. "E" Gruppen IN ITAL (dates not certain).**

- ROME
- VENICE
- TRIESTE
- NERVI (under MPNS KARESSE). Still in existence Apr 45 (?)
- S.L. REMO (under MPNS KARESSE). Still in existence Apr 45.
- ELSI (plus 7T stas).

**5. EQUIPMENT.**

FW supplied details of RT and JT intercept and DF equipment used by some of the Intercept Stas working under 4 SKL III.
### Table: Types of Sets Used

<table>
<thead>
<tr>
<th>Type</th>
<th>Makers:</th>
<th>Used At:</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.</td>
<td><strong>Intercept Sets:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>HRO (see + below)</td>
<td>National Company (sic)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MP Abt FLINDERN; FLINDERN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MHIS BRUSSELS &amp; GRONINGEN</td>
</tr>
<tr>
<td></td>
<td>OR 101</td>
<td>Philips</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DRGM</td>
<td>Societe Radio Francaise</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RL4 RADIONS</td>
<td>Dr. Elts - VIENNA</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SCHLIEFENLAND</td>
<td>Lorenz - BERLIN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MHIS GRONINGEN &amp; KARESSEE</td>
</tr>
<tr>
<td></td>
<td>SKYRIDER</td>
<td>USI firm, name not known to P7</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>S.ID IR UNW</td>
<td>Sadiir (FRANCE)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MHIS GRONINGEN; MPH EDENHUT</td>
</tr>
<tr>
<td></td>
<td>Fu HED UNW</td>
<td>German made, firm not known to P7</td>
</tr>
<tr>
<td>B.</td>
<td><strong>Intercept Sets:</strong></td>
<td>National Company (sic)</td>
</tr>
<tr>
<td></td>
<td>HRO (see + below)</td>
<td>MP Abt FLINDERN; MHIS GRONINGEN</td>
</tr>
<tr>
<td></td>
<td>LO 6 K</td>
<td>Lorenz - BERLIN</td>
</tr>
<tr>
<td></td>
<td>LO 6 L</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SCHLIEFENLAND</td>
<td></td>
</tr>
<tr>
<td>C.</td>
<td><strong>DF Sets (for WT and ER)</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>E P 2</td>
<td>Telefunken</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MP Abt FLINDERN; MHIS GRONINGEN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MPH DEN HELDER</td>
</tr>
<tr>
<td></td>
<td>aDOCK OR 101</td>
<td>Philips</td>
</tr>
</tbody>
</table>

*P7 stated that HRO sets were known to exist in BELGIUM and that the German authorities made drives to requisition them. Soldiers, sailors etc were promised 14 days leave if they helped to unearth such sets. "These sets are the best for intercept work" P7 said.*

### Notes:

6. **Work of Fn REFERAT (MUNICH BRUN).** The auxiliary vessels code.

4. **History**

(FW worked on this code from Mar 43 to Dec 44). It was the name by which the Germans referred to the code used by trawlers, etc, in contact with land bases, ports and other auxiliary vessels. FW could not say whether the RN referred to it by this name or not. The Germans had been working on this code since the war began. The Fn REFERAT (MUNICH BRUN) dealt exclusively with traffic in this code covering HOME WATERS and ATLANTIC as far south as FREETOWN.

When FW joined the Fn REFERAT the current code-book had been in use for about nine months. The code was deciphered with the aid of subtractors tables or code (WURMBOUCH) which changed fortnightly. (Code group subtracted from recipher group - FW quoted formula W-Cmp 10a WURMBOUCH minus CODEGRUPPEN-FUNKRUPPEN).

FW thought that this code book was the 3rd edition in use (?) It had been reconstructed to the extent of 60 to 70% with the aid of a previously current code.
book captured on CRETE, or another island in the MEDITERRANEAN. The captured book had been photographed and issued in the form of a photostat copy to the EJ group. It bore the title "N.W.L CODE No 5". Thus MW concludes that the book in use from approx Jul 42 to Apr 43 was called "N.W.L CODE No 6", but said he was not sure of this.

The (?) No 6 Code Book was changed at end Apr or beg May 43, but the same recipher book continued to be used. From beg May 43 to approx Jul 43, nothing was read until a cryptographer, Cadet (Fechburg) LUSEBRINK (later Sub Lieutenant) noticed that analysis of May, Jun & Jul traffic revealed that FREMACH had continued to use the (?) No 6 code book for 14 days after all other bases etc had changed over to the new book. This overlap allowed the German Navy cryptographers to break part of the new book.

In Dec 43 the recipher book was changed, the code book introduced in Apr/May 43 continuing to be in use. The recipher book or set of tables was now changed daily. The period of approx four weeks (?) 1 Dec 43 to 1 Jan 44 was considered by MW as a transition period, for on 1 Jan 44, the traffic became unreadable and continued to be so till Dec 44, when MW left the OKM. (Matches were now - in 44 - only two per day 1.31. 0000 to 1200 hrs and 1200 to 2000 hrs). From friends letters to MW, in ITALY in 45, it appears that results were XEU in 45 also. When the change took place on 1 Jan 44, the Germans started studying the traffic and after a while assumed that the code book had been changed, once more, as well as the recipher book or set of tables. They suspected that the recipher book or set of tables (TURNBURH) was changed daily by means of use of a stencil (EINE SCHLÜSSEL) which altered the order in which recipher groups were selected for reciphering code groups.

B. Description of Code and Recipher System

I. The Code Books

MW described No 5 Code of which he had seen a photostat copy as a four-figure book of 30,000 groups, in reality a set of three books each with groups ranging from 0000 to 9999. The code was issued in the form of an encode volume and a decode volume, each in three parts. The three parts of each volume were:

- the Ships List - containing all RN & (?) US Navy HQs (INDEXHEFELN)
- the Main Code - code book proper.
- the Geographical List - containing all geographical names.

Code groups from either of the a/m parts of the code were used in conjunction with indicators (NÜCHDIEGUNGSKRUPPEN). These were listed at the beginning of the volume (encode and/or decode)

Indicators were: SL = "following group is to be taken from Ships List"
C = " " " " " " " Main Code"
Geo = " " " " " Geogr. List"

A number of four-figure groups were provided as variants for the clear indicators (SL or C or Geo). MW thought clear Geo was allotted 20 code groups. Spellers were used in Main Code with approx 10 variants each. The clear word GEFO was allotted 50 code groups. MW also thought that the code (volume containing three parts) included a "settle code" (GEBNITZCODE) at the end of the book, but that this was never used by auxiliary vessels. Asked how many groups there were on each page of the code book, MW said he was not sure but thought there were probably 50 to a page.

No (?) 6 Code - partially reconstructed by MW 43 - was the same clear book, with a different arrangement of code groups. MW thought the last book the German Navy Cryptographers read, i.e. in use from end Apr or beg May 43 to end Dec 43, was No (?) 7.

MW quoted from memory the following code groups out of either book (?) 6 or book (?) 7.
II. The recipher system.

The recipher book or set of tables (WURMBUCH) consisted of approx 100 pages, each page having 5 columns and 20 - 30 lines. The Germans had reconstructed this to the extent of knowing the following details of its use:

(a) at the front of the recipher book, or set of tables, there was a list of "starting point indicators" giving page and line on which reciphering begins, e.g., 8888 = page 30 line 9. These indicator groups were four-figure groups printed on a page and hatted. "Starting point" meant always the middle group, i.e., the third on any given line.

(b) with the end of a separate table - on the last page of the book, probably these recipher indicators were uncoupled (reciphered once more = UBER-SCHLÜSSEL) so that the indicator which was signalled had to be broken before finding the group giving the "starting point". This table contained ciphers ranging from 00 to 99, and against these were placed the uncoupled subtractors for any "unciphered" indicator - e.g., 8888 = page 30 line 9, is subtracted from 7818 and uncoupled to 9030 and this process is indicated by means of ciphers 25. PW stated that clerks at OCM had told him that at the beginning of the war the recipher indicator was not uncoupled. Ciphers 25 was signalled as part of the five-figure recipher and code indicator group in message, see III. below.

(c) recipher pages or tables were divided into pages (or tables) for reciphering addresses and signatures and pages (or tables) for reciphering text. The Germans thought that even pages (the pages on the left of the book) were used for reciphering, addresses and signatures and marked them in red, (der NOBEL WURM) and that uneven pages (on the right of the book) were used for reciphering text and marked them in green (der GRÜNE WURM). This continued till Dec 43, after which all recipher groups were taken from the same pages or tables, the latter changing daily. The reciphering of a message proceeded in this manner: assume uncoupled recipher indicator to read 8888, which means "starting point" is on page 30 line 9 (always middle - 3rd - group) and that the address is six groups long; the 3rd, 4th and 5th groups of line 9 and the 1st, 2nd and 3rd groups on line 10 of page 30 (even, red) would be used to recipher the encoded address. The first encoded group of the text would then be reciphered by means of the 4th group on line 10 of page 31 (uneven, green) and so on, and if the text was long, the last group, line 1 on page 33 would be used, etc. Signatures were NOT signalled, (usually a message - in code - contained address only if retransmitted by W, etc., i.e. in case of doubt as to who originated was. Otherwise there was NO address either. E.g., (FINN subtractor) SI (NO) FROM FOCUS (GREN? subtractor) text).

(d) Recipher groups (4 - figures) were subtractor groups from which code groups (4 figures) were subtracted (non-carrying). The German cryptographers at OCM used the formula $F = W - O$ i.e., macromgram group (READ GROUPS) = recipher group (WURM minus code group (CODECUPPER)). E.g., $W$ = 0000 $O$ = 1234 $F$ = 9876

$F = W$ will equal c.

III. Traffic and indicators.

Intercepted messages had the following lay out - $F$, quoted an example from memory (figure groups NOT real) - e.g.,

(see over)
\[ E_n = 2 \cdot D_n = V = 276x = 25 \cdot 173GB \]

25000 9030 9030 9030 25000 25 173GB

where \( E_n \) (SL.H.WT sta) is a land WT sta,
- ZWAX = trawler
- W = repeated
- ZWAX = trawler
- 25 173GB = Date and TOO group
- 25000 stands for bigram 25 camouflage the recipher indicator group (8888) to 9030 and 000 code book indicator (VEREBLIRKUNJIRUEPH) 100 variants provided.
- 9030 is camouflage recipher indicator (8888).

C. Cryptography - Methods and Results.

I. Sorting of Traffic

Intercepted traffic brought to OCM SKL Chef MOID III (after 1 May 44: SKL III) was first sorted out according to code books (VEREBLIRKUNJIRUEPH) in a depot referred to by FY as the VEREBLIRKUNJIRUEPH (i.e., TRAFFIC SORTING OFFICE). This was done by clerks instructed, to do the sorting by looking for certain characteristics in the preamble of the message (Fu SPRUCHKEFF). The details concerning traffic in all types of known codes (reconstructed or under study) were supplied to traffic sorters by the registration or indexing personnel.

II. Breaking the Reciprier - Methods Used

The next stage was the research and/or work on breaking the recipher. (Note: Messages came to MUNICHEN BR. UN where only one type of code was being worked on, so that once C's knew the traffic was in that code (MILITARY VESSELS CODE) on breaking the recipher went straight ahead). All periods FY was connected with OCM this work proceeded more or less on the same lines. FY is no cryptographer and can therefore not describe how the recipher was first broken, methods or approach etc. FY can, however, describe the "drill" in some detail. There were six methods or ways in which the recipher book or tables could be broken (Mar 43 and earlier - Dec 45). These were:

(a) with the aid of two or more messages with the same indicators, say messages A and B both starting and ending with 25000 9030 (9030 25000). This constituted what the Germans called "eine SERIE". It amounted to working on two messages reciphered with subtractors taken from the same "starting point" in the book, during the same fortnight.

(b) with two or more messages with the same "suspected" recipher group (mit selben VEREBLIRKUNJIRUEPH).

(c) with two or more messages containing chance repeats (durch reine DOPPELVOORKOMMEN) - this was done with the aid of ROLLERITH machines.

(d) through "rolling" (durch ROLLEN), a process reconsitituting the use of a device called the "ROLLMACHINE" (see APP "D") of report) whereby hypothetical maconigram groups were formed with the aid of known maconigram groups ("Bildlen von kuenstlichen Fu-gruppen durch bekannte Fu-gruppen")

(e) through (breaking) deciphering of indicator groups (durch Entschluessen der Einsatzgruppen) either (i) through a "chain of indicators" (eine SCHLUESSEL-KETTE) or (ii) through a "ring of indicators" (ein SCHLUESSEL-RING)

(f) by means of differenting (MUTVERSCHLIESEN).
III. Breaking the Reipher - Details.

(a) Messages with pairs of indicators

E.g. messages A and B:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>B</td>
</tr>
<tr>
<td>3 pen</td>
<td>gbxz</td>
</tr>
<tr>
<td>(v) vpu</td>
<td>(v) mta</td>
</tr>
</tbody>
</table>

1) 25000
2) 9030
3) 2560 1500
4) 1735 4725
5) 8020 6000
6) ....
7) ....
8) ....

By means of call-signs of originator and addresses a fitting (suitable) clear text was assumed for message A. The code groups corresponding to such clear text were looked up and written under the line in place marked #, (drawn in black pencil), say 9040, 3020, 1975 etc, and then the "suspected" subtractor (VERDECHTS-WURM) group was calculated and written above the line in black pencil, in place marked ($) . (Nach). The "suspected" subtractor groups in the above example would have been 1500 4725, 9995 etc. If, when applied to message B, these "suspected" subtractor groups (1500, 4725, 9995 etc) gave code groups, say 0982, 5720, 3925, which stood for clear text of that type of message, then the "suspected" subtractor group was "confirmed" (der Turn wurde echt gemacht) and underlined in red and registered as a confirmed subtractor group (Echter Turn). It could be used for the current fortnight. The Messages A and B were then said to form a "SERIE". If three messages were in a "SERIE", work would be easier, however this was not often the case. When, during the work of breaking the reipher (TURNLEHN), the point was reached where spellers were used, progress was slower, but headway could be made going from A to B and then from B to ..., fitting in syllables or letters in one and confirming them in the other message. Time and date groups helped in the work. Time was encoded say 18 (group) and 00 (group). Cryptographers always tried 00 first.

This method was always tried first before going over to (b) or (c) etc, below. If messages were of the same length this was considered favourable and up to 70% of the text of telegrams could be read. The Germans estimated to intercept about six pairs of messages with the same indicators per day - thus getting six "SERIEN". Such occurrences were all the more frequent the nearer the end of the 15 day period approached.

(b) Messages with the same "suspected" reipher (subtractor) group.

(SERIEN mit selben VERDECHTS WURM).

Example: addresses (call signs) of message:

from: (v) MLU = SCAPA WT

to: 2 GZB = C GZB = GXXZ = Lango (trawler) with SI code name of 1230

(SERP: GXXZ is call sign of ship from the "INDICATIF d'APPLES" encoded to GGZB and reiphered to 2GZB).
The CA assumed that group 3020 stood for clear SI and that the clear concept was encoded by means of code group 9043 (known). He then calculated the "suspected" subtractor (VERDACHTSDECKEL) i.e. 2063, and marked it with a red dot (in place marked ©) to show that it is a "suspected" subtractor.

This was done mostly for addresses (red subtractors). These "suspected" subtractors were then indexed (REGISTRIERT) and if another message with the same "suspected" subtractor was found it was placed next to the first one to be worked on. However, the second message had to show the same "suspected" subtractor group (say 2063) in either the same place in the message (in this case 3rd group and the message was then referred to as an "identical key series" (eine SCHLÜSSELKLÄGERICHE SERIE), or in a place at intervals of 5 (number of columns in the replicier book) (HASSENGLEICH) i.e. 5th, 13th, 18th group, etc, in which case it was called a "bitar series" (eine BISS-SERIE), AND also the subtractor had to be of the same colour (red or green).

If the "suspected" subtractor, when applied to both messages, formed a "SERIE" and yielded clear text fitting these two messages, the subtractor was continued, underlined in red and registered. Approx 5 pairs of messages could be broken - up to 70% of text - every day. This was an average figure, FW said, results being always better towards the end of the 15 day period. Short messages yielded good results, because it was known in this case that the subtractor must be green (text only). E.g. message intercepted: from a trawler to GRIMSBY or vice versa:

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

Text is fitted in such as: sweep completed, or request gate etc or if from GRIMSBY to trawler e.g.: gate arranged.

This saved a fair amount of time as fewer possibilities (place of clear text and subtractors) had to be tried out.

(c) With the aid of messages containing chance repeats (reine DOPPELWÖRMER)

E.g.

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>25705</td>
<td>35999</td>
</tr>
</tbody>
</table>

With the aid of HOLLERITH machines pairs of - or more - messages were sought in which the same maroonogram group (FU-GRUPPE) occurred in the same place, removed at an interval of 5, or multiples of 5, groups (HASSENGLEICH); in this instance 5th, 13th group etc. FW said that in approx 50% of cases this was more coincidence (ZUWEIL) i.e.

E.g.

<table>
<thead>
<tr>
<th>Code</th>
<th>Maroonogram group</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>1500</td>
</tr>
<tr>
<td>Y</td>
<td>1500</td>
</tr>
</tbody>
</table>
the percentage of coincidences (50%) being roughly the same for both red and green subtractors. However, all cases were tried out and if, say, in the above example, clear text fitted in message A (3rd group, 1500), the same clear text was assumed to be in the 3rd group of message B as well. If the assumption proved to be correct, about 70% of the messages concerned could be read (Aug/Sep 43).

(a) Finding pairs of messages ("SERIEN") through "rolling" (durch ROLLER).

This work was done with the assistance of the "ROLL" Gruppen (see para 3. 0. 10 and Appendix "D" of report) and by using material supplied by the HOLLERITH machine (?) sub-sec. The various stages of the work are listed below:

(i) - with the aid of HOLLERITH machines a catalogue was drawn up, of all moronigram groups intercepted, listing groups in numerical order, from 0000 to 9999.

(ii) - the catalogue of intercepted moronigram groups listed traffic for a fortnight and separated - by means of markings - red from green subtractor-groups.

(iii) - high frequency known code-groups were then set on the machine (for "drill" see Appendix "D" of report).

(iv) - all known confirmed subtractor groups (bekannte echte WURMER) were then taken out of the reconstructed recipher book (WURMERGRUPPEN) and put through the machine in the hope of getting "artificial moronigram groups" (KUNSTLICHE FUNKGRUPPEN). These were looked for in the catalogue mentioned above and if found to occur in two messages in the same place, or at intervals of five, or multiples of five, the messages in which these "artificial moronigram groups" occurred were located and a pair ("SERIE") formed. The work was then handed over to cryptographers ("WURMERGRUPPEN").

(v) - the cryptographer(s) then proceeded along these lines: E.g. messages A and N :-

<table>
<thead>
<tr>
<th>A</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>1567</td>
<td>3026</td>
</tr>
<tr>
<td>1738</td>
<td><strong>3026</strong> or in 8th, 13th, 18th groups, etc.</td>
</tr>
</tbody>
</table>

(vi) - the code-group (e.g. 9044 = code for SI) was known. The cryptographer then tried to find out if the "artificial moronigram groups" 3026 found to occur in messages A and N were a reciphered version of the same code-group, or whether it was perhaps a coincidence. In the latter case the messages were separated, no pair ("SERIE") being found. If, however, by fitting in a code group for relevant clear text, that code-group appeared to have been used - with recipher - in making up the "artificial moronigram groups" now found in these messages, then work proceeded on the two messages A and N.

(vii) - the messages were then placed side by side and the subtractor groups which had been used to recipher the known code groups in message A were applied to the same (or relative) moronigram groups ("artificial") in message N.

(viii) - FW stated that this work was done at the end of the 15 day period.

(ix) - results were mainly of historical interest.
(a) Finding pairs of messages ("SERIEN") by means of breaking or deciphering of indicator groups (durch Entschlüsselung der EINSATZGRUPPEN (or) KENNGRUPPEN).

This could be done by attempting to break "a chain of indicators" (eine SCHLÜSSELKETTE) or "a ring of indicators" (ein SCHLUSSELRING).

(i) "A chain of indicators".

A pair or more messages ("SERIEN") found by other methods (a - c) were required. E.g.

\[
\begin{array}{c|c}
A & B \\
25000 & 51000 \\
1527 & 5715 \\
& & \\
& & \\
\end{array}
\]

(NOTE: It did not matter if trigrams in five figure groups were the same or not, because they indicated type of code book and had many variants. 000 could be the same as 123, etc., in clear.)

Assumption: The messages A and B, being in the same "SERIE", have actually been deciphered by means of the same table and the deciphering proceeded from the same "starting point". Groups 1527 and 5715 are camouflaged (deciphered) "starting point" indicators, the four figure group with which deciphering was done being indicated by bigrams 25 and 51 respectively. (Of para 6.B.II.b.). It was therefore assumed that the uncamouflaged "starting point" indicator in such a case was 0000 (die RELATIVE GRUPPE) therefore the camouflage or decipher groups against bigrams 25 and 51 (on last page of decipher book) would have been 1527 and 5715 respectively. (The German QAs referred to 0000 in this case as the RELATIVE GRUPPE). These "assumed" decipher groups (die argumenen WURM) were then used as sub-tractors for all deciphered (camouflaged) indicators in messages against bigrams 25 and 51 which had been registered, and were outside pairs ("SERIEN"), for the 15 day period. (Decipher indicators (EINSATZGRUPPEN or KENNGRUPPEN) were registered in numerical order for easy reference). Thus:

<table>
<thead>
<tr>
<th>Messages with bigrams:</th>
<th>(AW)</th>
<th>1527</th>
<th>1527</th>
<th>1527</th>
<th>1527</th>
</tr>
</thead>
<tbody>
<tr>
<td>(P)</td>
<td>5090</td>
<td>6523</td>
<td>7956</td>
<td>8719</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6537</td>
<td>5004</td>
<td>4671</td>
<td>3618</td>
<td></td>
</tr>
<tr>
<td>(AW)</td>
<td>5715</td>
<td>5715</td>
<td>5715</td>
<td>5715</td>
<td></td>
</tr>
<tr>
<td>(P)</td>
<td>6949</td>
<td>4570</td>
<td>4671</td>
<td>9182</td>
<td></td>
</tr>
</tbody>
</table>

The common difference of 4671 was regarded as proof that the "starting point" indicator - uncamouflaged - was the same in the case of these two messages (X and Y). The complement of this difference (6439 = 0000 - 4671) was taken as the difference between the original decipher camouflage groups used to conceal the true "starting point" indicator. A new "SERIE" was thus formed, it being assumed and proved that, under the camouflage, messages X and Y were deciphered with the same subtractor (WURM). The pair of messages was then handed over to cryptographers, who carried on working as at - (a)--------above.

(ii) "A ring of indicators".

This was achieved when, by taking all messages with all bigram decipher camouflage indicators, the "chain of indicators" could be completed for traffic passed during the relevant fortnight. In such cases all messages could be linked together via their bigram decipher camouflage indicators. (Interrogator's Note: PW was not very knowledgeable or certain on this point).
The text contains a detailed explanation of the method used by the German army to break into additional 150 - 200 pairs of messages. The method involved the use of a "chain" and a "ring of indicators". The work was done at the end of the fortnight and took about 1 - 2 days. It was done by extra matches (PLUSHÄCHEN). This brought the total of 300 - 400 pairs of messages per fortnight - found by methods (a) to (d) above - to approx 500 - 600.

(f) **Differencing (DIFFERENZIEREN).**

PW described this method as "a variety of rolling" ("Eine Abart des Rollens"). Two kinds of differencing work were done at OKM:

(i) - differencing as an aid to decipher and code breaking; this was always done with the aid of the catalogue of differences (DIFFERENZENKATALOG).

(ii) - differencing done for the purpose of finding pairs of messages ("SERIEN") and "biter series" (BISSE zu Serien); this type of work was begun in or after Dec 43 when the Fo (FRITZ OTTO) Group was specially formed for that purpose and carried on working on old material after 1 Jan 44 without results.

I. - **Differencing as an aid to decipher and code breaking.**

This was done when approx 20% of the code book was known, not before.

Two messages in a pair ("SERIEN") were wanted. Each group in one message was "differenced" (DIFFERENZIEREN) through all groups in the other message and vice versa. The smaller difference was always taken. Differencing was always done by hand - PW said no calculating machines were ever used at OKM - and all results were catalogued from 0000 to 4999.

**Example:**

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9043</td>
<td>code for SI</td>
</tr>
<tr>
<td>6528</td>
<td>&quot; = 0 in C HLYMOUTH</td>
</tr>
<tr>
<td>3525</td>
<td>catalogued = SI - 0 in C HLYMOUTH</td>
</tr>
</tbody>
</table>

Work proceeded on the principle of $F_1 - F_2 = C^2 - C_1$ when the same subtractor was used ("Wenn der selbe Wurm Zugrunke liegt"), where $F_1$ and $F_2$ are marcomagram groups (FUNKGRUPPEN) and $C_2$ and $C_1$ are code groups (CODERGRUPPEN), in messages 1 and 2. Cryptographers resorted to differencing when attempts to break the code in a pair of messages ("SERIEN") showed no results. The group(s) in the messages where C's stopped, were differenced (smaller difference) same place in message or intervals of five, and the resulting four figure group was looked up in the catalogue of differences in an attempt to find clear groups which might fit in both messages. This was done separately for red and green subtractors.

**Example:**

<table>
<thead>
<tr>
<th>Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>11) 8765</td>
</tr>
<tr>
<td>12) ....</td>
</tr>
</tbody>
</table>
The difference between the 11th groups in messages 1 and B i.e. 3579 was found in the catalogue to be for instance:

<table>
<thead>
<tr>
<th>Difference between:</th>
<th>WEATHER</th>
<th>SAIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>SI</td>
<td>NOAA HOLYHEAD</td>
<td></td>
</tr>
<tr>
<td>FROM</td>
<td>REPEATED (W)</td>
<td></td>
</tr>
<tr>
<td>SPELL</td>
<td>GEO LIST</td>
<td></td>
</tr>
<tr>
<td>etc</td>
<td>etc</td>
<td></td>
</tr>
</tbody>
</table>

If none of the above fitted in the text, differentiating for groups 12, or 12 and 17, or 12 and 22, etc. were tried, and so on. FW stated that many GIs preferred to avoid differentiating work, saying that "there were too many possibilities" to work on.

II - Differentiating for purpose of finding pairs of messages ("SERIEN").

This type of work, which was done after the end of a current fortnight, necessitated knowledge of the code book to the extent of 50% - FW did not explain why Group Fo (FRITZ OTTO) persisted in carrying on working after 1 Jan 44, when both recipher and code changed.

Two messages which were NOT in pairs ("SERIEN") and were "routine messages", were picked out. "Routine messages" were recognised by means of their preamble (TUSCHKOPF). FW quoted from memory none of these signalling "routine messages":

| FROMTOWN | 3 JUN (SCHLA) |
| SOLX WEATHER | 3 QTR = AIG 298 (HOLYHEAD) |
| AIG 31 | COAC = HOLL.1.X = AIG 306 or 312 |
| HESSTONE - RENAST | AIG 54 |
| SHIPS TO ROSBY | (Q3S) (gates) |

All groups in two messages of this type had to be differentiated place for place and at intervals of five (STELLENLEICH and HELSENLEICH). This was hard work, FW said, and had to be done by hand. FW was of the opinion that with the HOLLERITH machines available to OKH this work would not have been practicable by mechanical means.

The formula on the basis of which this work was done was: F1 - F2 = D, where F1 and F2 are morsegram groups (TUSCHKOPF) and D is the difference between F1 and F2, whether large or small (F2 always subtracted from F1). From this: D + 01 = 02 when 01 and 02 are code groups in messages 1 and 2. Strips of paper were used, like the one illustrated below (X), on which were marked messages, say A and B, i.e. all groups in B subtracted from their opposite numbers in A, the relationship of groups (STELLENLEICH or HELSENLEICH) and the differences.

**E.g.:**

<table>
<thead>
<tr>
<th>A - B</th>
<th>Morsegram Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHASE</td>
<td>(F1) (F2)</td>
</tr>
<tr>
<td>1 - 5</td>
<td>9013 - 7654 = 2499</td>
</tr>
<tr>
<td>2499</td>
<td>0015 - 9923 = 1102</td>
</tr>
<tr>
<td>1102</td>
<td>9091 - 1123 = 8978</td>
</tr>
<tr>
<td>3 8978</td>
<td>4 ...</td>
</tr>
</tbody>
</table>
On another strip of paper (Y) below were written all known code groups which occurred most frequently in message A. Assuming "routine message" was sent from AIG 31 and following groups were included:

(Y)

SL = 804.3 (real example)
bound = 0033
sail = 1234
PLYMOUTH = 6533

Strip (Y) was then placed under strip (X) and groups added, in the same places or at intervals of five (STELLE FUR STELLE ODER PHASENLEICH).

(X)

\[
\begin{array}{c|c|c}
A & B \\
\hline
\text{PHASE 1 - 5} & 24.99 & \text{24.99} \\
\hline
1) 904.3 & \text{904.3} & 14.32 \\
\end{array}
\]

It was then assumed that 14.32 was the corresponding code group in message B, under recipient. Code group 14.32 was looked up in the reconstructed Code book and if the clear word or syllable or text fitted message B, it was assumed that it was "good" and the next group was tried. PW illustrated this as follows: Assuming 14.32 in message B (Y) FREETOWN = spell and the next group was tried and - spellers being expected - this group was either CA or MO. As a fair number of Spanish and Portuguese ships were known to call at FREETOWN the spellers CA or MO could be assumed to stand for the first syllable of CABO or MONEE respectively. If the next group or two fitted the message, the full name of the ship(s) could be found with the aid of GROENE's Handbook of World Merchant Fleets (II.SCHENBCH DERR WELT-MERCHANTFLotten). (Note: these mercantile ships lists etc. were useful only in case of neutral ships being mentioned in messages). If groups thus found fitted the messages, the subractors (F - O = V) were registered and also tried out by "rolling" (of (d) above).

PW stated that the main aim of this method was to find new code groups. Most successes were achieved with FREETOWN traffic. Being in possession of 50% of code groups (reconstructed) the Cryptographers could get up to 70% by working according to this method.

IV) Registration of Code groups.

This was done by a team of three men referred to as code-interpreters (CODEDEUTER). All decoded material went to them and code groups were entered on cards, with indices of frequency etc. Code groups were classified as:

(a) Genuine code groups (GEHE CODE GRUPPEN), marked with two crosses and underlined in red,

\[ \text{e.g.} \quad \text{SP} \]

(b) Half-genuine code groups (HALBEGE CODE GRUPPEN), marked only with one cross.

(c) Assumed code groups (UNBEICHTE CODEGRUPPEN) - no marks.

A code group was considered to be genuine if it fitted in approx 100 places, half-genuine if it fitted in approx 50 places and an assumed one if it occurred in approx 10-20 places.

7. WORK AT FJ REPORT (FRANKFURT) AND OTHER SUB-UNITS

A. The Frankfurt System (WERFHERN FRANKFURT).

This was the cover name for a FN code used by ships other than auxiliary vessels. FJ thought it was a high grade code used by Flag Officers as well. It was read tall end Feb 43, after that date no results were obtained as far as FJ knew.

B. FN and US Navy Tactical Codes.

I. General

FJ stated that characteristic of most of these codes was the fact that they were all letter-codes and that only certain letters of the alphabet were signalled. Some codes were read at Intercept and DF HQs and/or Stats only, some were read at the OKM as well - see below.

FJ remembered details of the following codes:

- **LOXO** (3-letter code) and the **COFOX** (4-letter code) read throughout the war till (?) 44. SECTION 31 at SOUTHEIND transmitted traffic in these codes; work was done in FJ Group.

- **MEDOX** (3-letter code), used in the MEDITERRANEAN, was read in '44.

- **NYKO** (4-letter code) and the **SYKO** (4-letter code) were read till Mar 43, when they went out of use.

- **TXJO** and the **EDOO** (? letter codes) were read at OKM in (?) FJ Group; they were known as Invasion Codes (LANDING CODES).

- US Navy 5-letter codes **AQUA**, **BANK** and **(NO)** were in operation after 6 Jun 44 and occasionally read at OKM, perhaps by FJ Group.

II. Details of **LOXO** and **COFOX** Codes.

The **LOXO** was worked upon at MP 1st FLANDERN at BRUGES and also at the OKM in the FJ Group where traffic from stats other than 31 SOUTHEIND was available. Work in the FJ Group was under the direction of Dr. THOM (see para 10 PERSONALITIES in report). Results of cryptographo work at BRUGES were sent to the OKM in BERLIN for evaluation and completion. No captured tables or docs referring to LOXO were available, but it was broken successfully and read all the time. The system or the tables - FJ was not sure which - charged in Oct/Nov 44, but traffic continued to be read. The **LOXO** was used for encoding traffic dealing with gates control in the THAMES Estuary by STA 31 at SOUTHEIND, also by CHINESE and patrol vessels. The Germans found out that they could always break into the SOUTHEIND traffic and every effort was made to take it. Station 31 being rather weak, when FJ abt FLANDERN moved from BRUGES to BRUSSELS in Jan 44 they set up a "directional antennas" (eine RICHTANTEN) of 1000 m length trained on the exact bearing of SOUTHEIND. The code was signalled in 5 letters; included among those used were: F, H, J, K, M, N, Q, S, T, U, X, Z. The Code was reciphered, the recipher changing daily.

The **COFOX** was on the same lines as the system outlined above. However, it was not used so frequently. It was also read at BRUGES. The Code was operated by the same type of ships and perhaps on inter-convoy traffic.
8. U-BOAT DF SERVICE (see also para 3 C.II a and Appendix "E" of report).

One of the targets of MF abt FLANDERN at BRUGES was the training and equipping of Intercept and DF operators for the German submarine service. Operators were required to speak English well and reach a good standard in RF interception and DF operation. FW stated that he knew of six operators who had sailed on board U-boats, but could only recall the name of one, a PO(WT) (Funk Mat) GROSSMANN, to whom he had spoken, and who claimed to have helped in the sinking of a British Cruiser in May/June 44. The German Navy Intercept Service had decided - after Apr 43 - to attempt to place convoy escorts and meeting points at sea by means of RF intercept and DF methods on board U-boats. FW stated that until end Apr 43 code breaking results could be given to U-boats. After end Apr 43, when cryptographic results were still obtained, but with greater difficulty, it was decided to utilize these for strategic purposes mainly and rely - if possible - on U-boat DF for locating targets.

The operator sailed as part of the crew and was equipped with a TELEFUNKEN-EP2 special DF set (SPEZLLESELER). (For details of EP2 and planned new equipment, see Appendix "E" of report). When the U-boat surfaced - desirable at times when convoy escorts were on the air - the operator would listen in and get the bearing. The reading had to be reported to the Captain at once. FW thinks that one bearing was considered sufficient to give rough location of escorts and/or convoy because: (i) if heard on the air ships could be at a maximum distance of 100 miles (RT range), (ii) Allied convoys stretched over some distance - between leading and last ship - and (iii) what was really wanted was the bearing for setting a course in that direction. FW however confessed that possibly the Germans oversimplified the problem and overlooked such factors as a convoy changing its course after netting calls, or traffic being passed at a time when a U-boat dared not surface. Asked if DF was ever attempted from more than one U-boat and results communicated by WI to get a "cut", FW replied he did not think so, as "no U-boat would dare to signal with enemy ships around".

Operators were instructed to listen-in to netting calls on the frequency 2410 Kcs (wavelength 124.5 m). (See also Appendix "E" para C.).

9. WORK AT "B" GRUPPE NERVI AND S/N REMO. (FW worked in these units as a WF mechanic from Dec 44)

Work in the "B" Gruppe consisted in watching traffic on RF and RT, and such code and cipher work as was done was carried out with the help of material provided by ORM or an MPS (in the case of NERVI and S/N REMO by MEHS KUERSCHER).

"B" Gruppe NERVI watched the "speedboats - frequency" (SCHNELL -BOOTSVELLE) of 2150 Kcs. This frequency was watched both from the land station at the group and from on board Italian and German Navy Units sailing in the LIGURIA/S EA e.g. (7) Italian T33s (destroyers or torpedo boats), L.NAV. barques for anti tt. Two operators (one for RF and one for RT) sailed on e.g. a ship or convoy and reported to Captain on ship (o ship) any contents of messages intercepted from Allied ships trying to attack them. Traffic taken at NERVI by operators stationed on land was sent to MEHS KUERSCHER.

"B" Gruppe S/N REMO watched mostly RT traffic originated by the French. The frequency of French patrol boat traffic was 2715 Kcs and traffic was in a code made up of cover names (on TELEX-PHEL lines) with names of colours for clear figures. The code changed at the end of Mar 45. FW stated that traffic was partly read, mainly because the French were so careless.

10. PERSONALITIES.

(Ranks are given in German with English equivalents in brackets, where applicable.)

Kpt-mjr-See (Captain) BON.TZ Head of the German "B" Gruppe 43. Rumoured to have been replaced by KUERSCHER below because he failed to make arrangements for security of documents which were all destroyed in a bombing raid on night of 22/23 Nov 43.
Kapitäen (Cmdr) BUDE

Oberregierungsrat Dr FRUNKE

Funk Mat (PO(WT)) GROSSMANN

Kpt-Mjr-See (Captain) KUFFER

Fähnrich (Cadet) later Leutnant (Sub-Lieut) LÜSBRINK

Regierungsrat Dr SCHEUERLE

Amtsrat SCHULZE

Amtsrat SCHÜLZE

Leutnant (Sub-Lieut)
Dr SLUDF Arnim

Admiral (dnl) STÜMSEL

Regierungsrat Dr THOM.

Oberregierungsrat TR. NOW

I/o Evaluation (Chef der ÜNNSWERTUNG) in Chef 133d III, later 4. SKL III. Ths them at beg 44.

Head of Generalreferat ? dealing with US Navy traffic.

U-Boat DF operator.

Replaced BON.TZ above at beg Dec 43 as head of Chef MND III (later 4. SKL III).

I/o watch (KLICHMÜTTER) in Fu Referat (MÜNCHEN BRÜNN) and did good work on Auxiliary Vessels Code (FREEFOWN traffic).

Took over Fu Referat when formed, in Dec 43, by amalgamation of STETIN, HAMBURG, and BREMEN Sees.

Worked under Generalreferat "F" on SWEDISH Naval traffic in Jul 44. An ex JT operator, O.R.

Head (Referatsleiter) of Fu Referat (FRANKFURT).

Till 1 May 44 "Ajtant" to STÜMSEL. Should know of Adic defence measures planned by Chef MND IV (later 4. SKL IV). Has lived in the „ARGENTINE“, speaks Spanish.

Head of Chef MND (I-IV) in 43 - May 44. Interested himself mainly in Adic defence.

Head of Fu Group, dealing mainly with LOKO. Ex MP Ltb-MÜNDEN (BRUGES).

Head of Generalreferat "p" (CT.BRITANNI & RUSSIA). Peace time cryptographer, perhaps ex-MHS LANGSÄRGEN (Lake CONSTANZ).

C.S.D.I.C.,
C.M.F.
3 Jul '45
<table>
<thead>
<tr>
<th>Intercept Sta</th>
<th>Presetable</th>
<th>Space used for Registration etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>FUSCHBACH KOEFF</td>
<td>203/9030</td>
</tr>
<tr>
<td>Ranges (Area)</td>
<td>No.</td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td>Date</td>
<td></td>
</tr>
<tr>
<td>Frequency</td>
<td>FREQUENC</td>
<td></td>
</tr>
<tr>
<td>Time of Taking</td>
<td>AUFN. UHRZEIT:</td>
<td></td>
</tr>
<tr>
<td>From</td>
<td>VON</td>
<td></td>
</tr>
<tr>
<td>To</td>
<td>AN:</td>
<td></td>
</tr>
<tr>
<td>No. of Groups</td>
<td>GRUPPEN No.</td>
<td>200 Group</td>
</tr>
<tr>
<td>TLM:</td>
<td>UHRZEIT GRUPPS.</td>
<td></td>
</tr>
</tbody>
</table>

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>25000</td>
<td>18</td>
</tr>
<tr>
<td>2</td>
<td>9030</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>2560</td>
<td>9043</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>30</td>
<td></td>
</tr>
</tbody>
</table>
Appendix "B"

PATTERN OF GERMAN NAVY INTERCEPT
LOG BOOK FORM
("B" STELLEN TAGESBUCH FORMULAR)

<table>
<thead>
<tr>
<th>Intercept Sta.</th>
<th>Zone:</th>
<th>Operator:</th>
<th>Date:</th>
<th>No:</th>
</tr>
</thead>
<tbody>
<tr>
<td>B-STELLE:</td>
<td>HERZICH:</td>
<td>HILFER:</td>
<td>DATUM:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Frequency</th>
<th>From.</th>
<th>To.</th>
<th>Contents and Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>KHz</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>VON</td>
<td>AN</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

 contents and Remarks

INHALT UND BEMERKUNGEN:
Appendix "C" (Of para 3.C.II. of report)

Details of HF STS Covered by the German Navy Intercept Service, C.II. Signs & Frequencies Memorised by Pw.

1. HF STS Covered by German Navy Intercept Service (1943-1945).

United Kingdom:

Whitehall
Chester
Solel
South
Hazel
Grimsby
Great Yarmouth
Sheerness
Southend
Dover
Brightlingsea
Ramsgate
North Foreland Radio
Port E. Trick Radio
Falmouth
Penzance

 Dependencies:

A.J. Polis
Malay
Honolulu
Summit R.A.F.
CCG Solo
Guantanamo
Kodak
Sydney

Bases in Occupied Territories incl. Indigenous Seats:

Beirut
Cairo
Biserta
Tunis
Rabat
Casablanca
Port Lavat
Diego Sulrez (Madagascar)
Zones
Rio
Palermo
Nice

British Empire:

Halifax
St. John's
Vancouver
Suva (Fiji)
Fiji Islands
Trincomalee (Ceylon)
Ceylon
Bombay
Deli
A. and Ceylon
Basra

 Dependencies:

Nicola (Cyprus)
Gibraltar
Riunel (Malta)
Freep
St. Helena
| Aveiro
Selm Kop Pt.
T. Kordi
Requim
Arnhem
Belgian
Flinders Ild.
Kuwait
B. CALL SIGNS.

I. NAVAL GENERAL CALL SIGNS.

<table>
<thead>
<tr>
<th>PERIOD</th>
<th>STATION</th>
<th>CALL SIGNS:</th>
<th>WT</th>
<th>FT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1943/44</td>
<td>Whitstable</td>
<td>GTL</td>
<td>GYE</td>
<td>GYB</td>
</tr>
<tr>
<td></td>
<td>Cleethorpes</td>
<td>GWP</td>
<td>MFC</td>
<td>BULL TANNER/SCHAP</td>
</tr>
<tr>
<td></td>
<td>Grimsby</td>
<td>MFC</td>
<td>MTU</td>
<td>DOVER</td>
</tr>
<tr>
<td></td>
<td>Scapa Flow</td>
<td>MTU</td>
<td>MLD</td>
<td>MAD</td>
</tr>
<tr>
<td></td>
<td>Dover</td>
<td>MTU</td>
<td>MLD</td>
<td>MAD</td>
</tr>
<tr>
<td></td>
<td>Liverpool</td>
<td>MLD</td>
<td>MLD</td>
<td>RIBLE, SILEX, G.LEX, LIVERG</td>
</tr>
<tr>
<td></td>
<td>Inchekeith</td>
<td>MLG</td>
<td>MLD</td>
<td>SILEX</td>
</tr>
<tr>
<td></td>
<td>May Island</td>
<td>MOSES</td>
<td>MOSES</td>
<td>MONTS</td>
</tr>
<tr>
<td></td>
<td>Devonport</td>
<td>MTN</td>
<td>BULL SAFETY/SHEERNESS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sheerness</td>
<td>BULL SAFETY/SHEERNESS</td>
<td>BULL SAFETY/SHEERNESS</td>
<td>BULL SAFETY/SHEERNESS</td>
</tr>
<tr>
<td></td>
<td>Southend</td>
<td>BULL SAFETY/SHEERNESS</td>
<td>BULL SAFETY/SHEERNESS</td>
<td>BULL SAFETY/SHEERNESS</td>
</tr>
<tr>
<td></td>
<td>Prestown</td>
<td>VPY</td>
<td>VPY</td>
<td>VPY</td>
</tr>
<tr>
<td></td>
<td>Helicon</td>
<td>VPK</td>
<td>MLD</td>
<td>MLD</td>
</tr>
<tr>
<td></td>
<td>Gibraltar</td>
<td>GYX</td>
<td>MLD</td>
<td>MLD</td>
</tr>
<tr>
<td></td>
<td>Halifax</td>
<td>GYX</td>
<td>MLD</td>
<td>MLD</td>
</tr>
<tr>
<td></td>
<td>Annopolis</td>
<td>NA4</td>
<td>NA4</td>
<td>NA4</td>
</tr>
<tr>
<td></td>
<td>Subgot/Albq</td>
<td>NA4</td>
<td>NA4</td>
<td>NA4</td>
</tr>
<tr>
<td></td>
<td>Locolou Lai/Honolulu</td>
<td>NFM</td>
<td>NFM</td>
<td>NFM</td>
</tr>
<tr>
<td></td>
<td>Cherbourg</td>
<td>NJS</td>
<td>NJS</td>
<td>NJS</td>
</tr>
<tr>
<td></td>
<td>Paris</td>
<td>NJI</td>
<td>NJI</td>
<td>NJI</td>
</tr>
<tr>
<td></td>
<td>Marseille</td>
<td>FUM</td>
<td>FUM</td>
<td>FUM</td>
</tr>
<tr>
<td></td>
<td>Leoghon</td>
<td>MJD</td>
<td>MJD</td>
<td>MJD</td>
</tr>
</tbody>
</table>

II. NAVAL BASES AND AUTHORITIES.

1943/44

| SHIPS AND AUTHORITIES IN AREA F5 PRESTOWN | 3 PEO |

III. USED BY:?

1944

<table>
<thead>
<tr>
<th>CODE NAMES:</th>
<th>figure - letter - figure</th>
</tr>
</thead>
<tbody>
<tr>
<td>RUP会MEN</td>
<td>6 - letter - letter - letter</td>
</tr>
<tr>
<td>&quot;</td>
<td>7 - letter - letter - letter</td>
</tr>
</tbody>
</table>
IV. SHIPS AT SEAL.

1943/44 (CODE NUMBERS: from A to Z)

V. INTER-LILIED CODE NUMBERS (INTER-LIILITE RUPF.LIEN):

1943/44 letter - figure - letter - figure - letter.

VI. TRAWLER CODE NUMBERS as PER "INDICATIVE D'IDENTIFICATION":


VII. DELIVERY GROUPS (VERTEILER GRUPPEN):

UD = also intended for.

1943/44 QQ = pass to.

HJ = Ldnv. (admiralty)

VIII. DELIVERY - DRESSSES (VERTEILER DRESSEN):


IX. WAVELENGTHS AND FREQUENCIES - (1941-45):

(NO: FW quoted either wavelengths in m, and/or frequencies in KCs. These have been converted into Kcs and are shown in col. 3.)

<table>
<thead>
<tr>
<th>WAVELENGTH (m)</th>
<th>FREQUENCY (MC)</th>
<th>FREQUENCY (Kcs)</th>
<th>USED BY SHIPS AND IN ZONES</th>
</tr>
</thead>
<tbody>
<tr>
<td>35</td>
<td>8.2</td>
<td>8200</td>
<td>MTBs (KLEMM-LIPFURST ENDE) in the ENGLISH CHANNEL.</td>
</tr>
<tr>
<td></td>
<td>8.4</td>
<td>8400</td>
<td></td>
</tr>
<tr>
<td></td>
<td>8.5</td>
<td>8500</td>
<td></td>
</tr>
<tr>
<td>93</td>
<td>2.7</td>
<td>2700</td>
<td></td>
</tr>
<tr>
<td>97</td>
<td>3028.8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>110</td>
<td>2.716</td>
<td>2716</td>
<td></td>
</tr>
<tr>
<td>113</td>
<td>2.5</td>
<td>2500</td>
<td></td>
</tr>
<tr>
<td>120</td>
<td>2.5</td>
<td>2500</td>
<td></td>
</tr>
<tr>
<td>122.4</td>
<td>2.5</td>
<td>2500</td>
<td></td>
</tr>
<tr>
<td>124.5</td>
<td>2.41</td>
<td>2410</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.45</td>
<td>2450</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.24</td>
<td>2240</td>
<td></td>
</tr>
<tr>
<td>137</td>
<td>2.26</td>
<td>2260</td>
<td></td>
</tr>
<tr>
<td>137.6</td>
<td></td>
<td>2107.7</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.15</td>
<td>2150</td>
<td></td>
</tr>
<tr>
<td>147.5</td>
<td>2.04</td>
<td>2040</td>
<td></td>
</tr>
</tbody>
</table>

(Note: FW quoted either wavelengths in m, and/or frequencies in KCs. These have been converted into Kcs and are shown in col. 3.)

M.T.Bs (KLEMM-LIPFURST ENDE) in the ENGLISH CHANNEL.

N. France, after the invasion.

Stns: NJS & NJI in N. France.

F.R.M. - BREST.

INVE.SSION REL. (N. France).

C/O PORTSMOUTH, PLYMOUTH.

CONVOY ESCORT FREQUENCIES (GELEITZUGSWEIN).

R. TROIS S. FRANCE O&ST- (BREST, PL & P2).

UNKNOWN (T. REAR, NORTON, CROSSWISE).

SCALE, INCHKEITH, ISLAND (FOGOS).

LIVERPOOL M.D. TO "RUBIE" (G. O. W. APPROACHES).

SPEEDBOATS IN MEDITERRANEAN (Gulf of GENOA).

R. MSG. TE TO "BISHOP".)
### Table

<table>
<thead>
<tr>
<th>WAVELENGTH (m)</th>
<th>FREQ. (MC)</th>
<th>FREQ. (Kos)</th>
<th>USED by SLS AND IN SONES:</th>
</tr>
</thead>
<tbody>
<tr>
<td>155.4</td>
<td>2.068</td>
<td>2068</td>
<td>SOUTHEND 31 to THEMES Control ship.</td>
</tr>
<tr>
<td>168.5</td>
<td>1.78</td>
<td>1780</td>
<td>SHERNESS.</td>
</tr>
<tr>
<td>170</td>
<td></td>
<td>1765</td>
<td>CIC MORE, GRIMSBY, GREAT YARMOUTH, NORTH FORELAND, PORT P. PATRICK RADIO.</td>
</tr>
<tr>
<td>172</td>
<td>1744.5</td>
<td></td>
<td>DOVER.</td>
</tr>
<tr>
<td>176</td>
<td>1704.6</td>
<td></td>
<td>Alternative frequencies (AUSWEICHWELLEN)</td>
</tr>
<tr>
<td>188</td>
<td>1638.4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix "p"

(of para 6.0.11.d. iv of report)

A. Description of ROLLERSCHING (FIG 1 on Appendix)

PW compared it to an abacus and gave the following details of its construction and handling. The machine is composed of a metal-sheet outer casing of which the top side is illustrated in FIG 1. (area a b c d). The top side of the machine has a cover which can be opened (area e f g h) and part of which (area e f i j) is covered with glass allowing operator to see the first "rollers" on each of the four axles (axles with rollers marked k l m n). The remaining part of the top cover (e f g h) i.e. area i j g h, has four open channels through which operator can see the rollers turn. On the "window" (area e f i j) and the left hand side of cover (a e o g) strips are provided on which the subtractor group set on the machine's top rollers and the code groups, can be marked before operating. The four axles (k l m n) have usually 10 (arctanuses 15) 'rollers' mounted on them. The machine is built in such manner that when the top cover (e f g h) is opened the "rollers" can move independently on the axles on which they are mounted. When the top cover is closed, the axles can be moved and all "rollers" on the one axle move with the axle, but not independently. The axles are not coupled, they have to be moved individually. A support is provided with the machine allowing operators to place it on their desks at an angle of approx 45° from the horizontal.

B. The "Rollers" (Cross-section illustrated in Fig 2 of Appendix).

The "Rollers" are made of wood or metal, diameter approx 1 inch and are marked from 0 to 9 in an anti-clock-wise direction. When the machine is operated the axles on which the "rollers" are mounted are turned in a clock-wise direction so that 1 follows 0, 2 follows 1 etc.

C. "Drill" for setting the machine. Suppose the groups (high frequency known code groups) 943, 2820, 6558 etc have to be put through the machine. They are written out on the strip at the side of the machine (area a e o g) starting from a line corresponding with the second row of "rollers". The top cover of the machine is opened, allowing "rollers" to move independently on their axles and the "rollers" are set at: (see Fig 1)

```
0000 on the top row
1067 " " 2nd "
8280 " 3rd "
4582 " 4th "
```

The group 0000 is the basic setting (GRUNDANSTELLUNG) for the subtractor trials and is always taken - arbitrarily - for the sake of convenience. PW stated one could set the machine at 1111 (on the top row of "rollers") or any figures, but one would have to carry on completing the cycle in any case (see D below).

D. "Rolling" - "drill". When the machine is set, all registered confirmed subtractor groups (found in the reconstructed recifier book - WURMBODEN) are turned on the top row of "rollers", in turn, and the resulting "artificial maricomgram groups" are compared with the catalogue of intercepted maricomgram groups. If any "artificial" groups are found to exist in the catalogue and in the two messages, these are made into a pair ("SCHIEF"). In FIG 1 complement digits of code groups are set with assumed subtractor 0000. In FIG 2 confirmed subtractor 127 has been set by "rolling" and "artificial" groups 2234, 9437 and 5729 obtained.

PW stated that this kind of work could be done by hand also, but that it would take much longer. Therefore, instead of taking frequent code groups 943, 2820, 6558 - suspected to be at the basis of some maricomgram groups in traffic - and trying to subtract them from all confirmed, registered subtractor groups
known to the cryptographers, such as:

<table>
<thead>
<tr>
<th>Subtractor Group (W)</th>
<th>1257</th>
<th>1257</th>
<th>1257</th>
<th>etc</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code Group (C)</td>
<td>0000</td>
<td>0000</td>
<td>0000</td>
<td></td>
</tr>
<tr>
<td>Maroonigram Group (F)</td>
<td>2214</td>
<td>9437</td>
<td>5739</td>
<td></td>
</tr>
</tbody>
</table>

the complement values of code group digits are set on the "rollers", assuming that on the top row code group 0000 is set as a starting point, and subtractor 1257 for instance, and others, are added. E.g.

<table>
<thead>
<tr>
<th>Subtractor Group (W):</th>
<th>1257</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code Group (C):</td>
<td>0000</td>
</tr>
<tr>
<td>Maroonigram Group (F):</td>
<td>1257</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Subtractor Groups (W):</th>
<th>1257</th>
<th>1257</th>
<th>1257</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code Groups (C):</td>
<td>1067</td>
<td>8280</td>
<td>4582</td>
</tr>
<tr>
<td>Maroonigram Groups (F):</td>
<td>2214</td>
<td>9437</td>
<td>5739</td>
</tr>
</tbody>
</table>

The machine has the advantage of allowing several code groups to be treated at the same time.

F. "Rolling" is done separately for red subtractors applied to addresses - code-groups and green subtractors applied to text-code-groups.
### Fig. 1

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>9043</td>
<td>1</td>
<td>0</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>2820</td>
<td>8</td>
<td>2</td>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td>6528</td>
<td>4</td>
<td>5</td>
<td>8</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Fig. 2

- **Axle**

### Fig. 3

```
1 2 5 7
2 2 1 4
9 4 3 7
5 7 3 9
```

"artificial maroongram groups" (KUENSTLICHE FUNKGRUPPEN)
Appendix **E** (of para 8 of report)

**FW TEMP's DESCRIPTION OF U-BOAT SPEILLL**
**IF APE.ER. TUS & F.WALT GROSSMANN'S EXPLOITS.**

U - Boot Spezialpeiler:

As U-Boot Spezialpeiler was initially the von Telefunken built "EP 2" with Peilrahmen and Hilfsantenne used. The EP 2 is an ordinary four-valve heterodyne receiver, working on batteries, for medium and long wave bands (700 - 2000 m). The Germans intended to use later on a "vision" DF set (SICHTPEILER) developed by the German Navy Sigs Experimental Command (Nachrichten Versuchs Kommando = NVK). The "vision" DF set permits the operator to get the beam on a cathode ray tube (BR. UNSCHER RHR), so that DFing is possible without a superimposed wave. This means that when DFing RT traffic, the latter can be taken down simultaneously.

According to his own description while sailing on board an U-boat, GROSSMANN intercepted an DFed RT traffic between two British Naval Units. As a result of DFing an attack was made on a British Cruiser. He stated that he confirmed the sinking as a result of listenng in to RT traffic after the catastrophe and during the salvaging operation.
**DISTRIBUTION**

<table>
<thead>
<tr>
<th>To</th>
<th>Copy No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC of S G-2, AFHQ</td>
<td>1</td>
</tr>
<tr>
<td>QOIS, MED</td>
<td>2 - 3</td>
</tr>
<tr>
<td>CIO HQ MAAP</td>
<td>4 - 5</td>
</tr>
<tr>
<td>G-2 (Sig s &quot;I&quot;) AFHQ</td>
<td>6 - 8</td>
</tr>
<tr>
<td>S.I.S.</td>
<td>9</td>
</tr>
<tr>
<td>G-2 (P/W) AFHQ</td>
<td>10</td>
</tr>
<tr>
<td>GSI (A), 15 Army Group</td>
<td>11</td>
</tr>
<tr>
<td>MI 8, War Office</td>
<td>12 - 14</td>
</tr>
<tr>
<td>MI 19, War Office</td>
<td>15</td>
</tr>
<tr>
<td>File</td>
<td>16 - 18</td>
</tr>
</tbody>
</table>