

SRH-024

VOLUME III

GERMAN NAVAL COMMUNICATION INTELLIGENCE

VOLUME III

GERMAN NAVAL COMMUNICATION INTELLIGENCE

AND

COMPROMISE OF ALLIED CIPHERS

\*\*\*\*\*

Table of Contents

Chapter I	Organization and Working of German Naval Communication Intelligence.
II	Intelligence Disseminated to U/B's and the Sources Acknowledged in U/B Traffic.
III	German Intelligence on Allied Convoys in the Atlantic.
IV	Compromise of Naval Ciphers #3 and #5
	Appendix A: Cases of Presumed and Confirmed Compromise 1943-1945
	Appendix B: Confirmed Cases of Allied Cipher Compromise in 1942
V	"E-Dienst" on Board U-Boats.
VI	German-Japanese Cooperation in Communication Intelligence.
VII	German Fears of the Compromise of their Naval Cipher.

DECLASSIFIED per Part 3, E. O. 12858  
by Director, NSA/Chief, CSS

TC Date: 10 July 92

CHAPTER I

ORGANIZATION AND WORKING OF GERMAN  
NAVAL COMMUNICATION INTELLIGENCE.

("Funkaufklaerung": "B-Dienst")

\* \* \* \* \*

Table of Contents

1. In relation to German Naval Organization.
2. Subdivision of 4 SKL "Marinenachrichtendienst", Naval Communications Service.
3. 4 SKL/III "Funkaufklaerung" (Radio Intelligence).
4. The German R.I. Bulletin and handling of Ultra.
5. Concentration of German C.I. on Allied Convoy traffic.
6. Use of Non-RI Material.

~~TOP SECRET~~

ORGANIZATION AND WORKING OF GERMAN NAVAL  
COMMUNICATION INTELLIGENCE.  
("Funkaufklaerung"; "B-Dienst").

1.  
In relation to German Naval  
Organization.

The German Naval Intercept service and related Intelligence activities formed part of the division of Naval Communications, which in turn formed one of the six numbered "Naval War Staffs" ("Seekriegsleitungen", abbr., "SKL"). Late in 1944 these War Staffs were as follows:

OEM:	Naval High Command:	Grand Adm. Doenitz
Stabschef SKL:	Vice Chief of Naval Staff:	Vice Adm. Meisel
1 SKL:	Operations:	R. Adm. Hans Meyer
2 SKL/BdUop:	U/B operations:	R. Adm. Godt (Doenitz*)
3 SKL:	Intelligence:	R. Adm. Otto Schulz
4 SKL:	<u>Communications</u>	<u>R. Adm. Stummel</u>
5 SKL:	Radar research	
6 SKL:	Hydrography & Meteorology	

(\*Doenitz retained high command of submarines.)

2.  
Subdivisions of 4 SKL, "Marinenachrichtendienst",  
Naval Communications Service.

Chef MND: R. Adm. Stummel

I. Central Office. Captain Moeller.

II. German Communications. Captain Lucan.

Radio communications, stations, frequencies, etc.  
Naval codes and ciphers. Security.  
Recognition signals.  
Landlines.

III. Radio Intelligence ("Funkaufklaerung"). Capt. Kupfer.

Intercept, traffic analysis, low-grade recoveries.  
Cryptanalysis.

IV. Radar. This section was formed in August, 1943, in an attempt to combat Allied location of U/B's and included research on Allied non-radar location devices as well as radar. Special effort went into construction of search receiving equipment.

Location: After the bombardment of Berlin in Nov., 1943, section I moved to Keralle with Docnitz and staff. Sections II and III moved to Bismarck and later to Borswalde. When the Russians reached the Oder in 1945, 4 SKL moved to Wilhelmshaven area.\*  
(\*Ref. Ultra/ZIP/ZG/337).

3.  
4 SKL/III "Funkaufklaerung"  
(Radio Intelligence).

(a) Intercept Net.

The intercept net was organized, in part at least, into Naval D/F divisions (M.P.A.), Naval D/F main stations (M.P.H.S.), and Naval D/F subsidiary stations (M.P.H.S.). Before the loss of Italy the German Navy probably maintained about 50 intercept stations covering the Black Sea, Mediterranean, Baltic, Arctic, and Atlantic waters. Emphasis in the case of Atlantic stations was of course on British naval and R.A.F. traffic, including R/T. Of particular interest was M.P.A. Flanders, located in the Castle of Sint Andries near Bruges, where the operators captured from U-604 were trained. In addition to interception, D/F work, and the training of B-Dienst operators, M.P.A. Flanders received and

~~TOP-SECRET-ULTRA~~

broke low to medium grade British Naval traffic, such as Lexo and Faxo. Some of the other principal outlying stations performed similar intelligence duties, and issued routine summaries for their respective areas. B-groups were also maintained on various command staffs in occupied territory, to whom were sent daily recoveries of delivery groups and lettered coordinates for the English position reporting system.

(b) Headquarters of 4 SKL/III.

All high grade naval traffic was forwarded to 4 SKL/III in Germany, together with D/F's, traffic analysis, and low grade decoding results. The home station was organized into 2 sections, according to the Jap. Nav. Att.: "Auswertung" ("Evaluation") and cryptanalysis. The number of workers was said to be 800 in the early part of 1944, but it is not clear whether this figure applied to both sections or to cryptanalysis alone.

(i) "Auswertung" ("Evaluation").

The full extent of this section's functions is not at present known but its various subdivisions covered the following activities:

Intercept of enemy traffic.

Reconstruction of letter coordinates (from position reporting systems such as SP/2274).

Recovery of delivery groups. (Ref. Ultra/ZIP/20/310).

The above duties suggest that the evaluation section was responsible for D/F correlation and traffic analysis in general.

~~TOP SECRET-ULTRA~~

(ii) Cryptanalysis.

The internal organization and workings of this section are as yet little known. After the armistice with Italy, officers of the Italian Naval C.I. organization (S.I.S.), informed the Allies that they had worked in close collaboration with the Germans, and yet the Italians had never found out much about the inside of the German organization. Rome and Berlin had exchanged technical information and captured cryptographic documents, Rome, however, in the role of a subordinate. Neither maintained a permanent liaison with the other, although visits were exchanged. (Ref. GCCS Intell. Memo. #66).

4.

The German R.I. bulletin and handling of Ultra.

A German Naval R.I. Bulletin, dated 23 June 1944, was captured in Italy in September 1944. A weekly publication, this bulletin offered the most complete cross-section ever seen here of 4 SKL/III's work. Just what section of 4 SKL/III compiled it is not clear, but it contains a large amount of material that would probably come from the "Ansvwertung" section. Presumably a correlation room existed, to which were passed the final results of the entire C.I. organization. The bulletin is carefully organized and apparently follows a relatively fixed form.

~~TOP-SECRET-ULTRA~~

(a) Distribution of Bulletin.

According to the introductory printed pages, 25 copies of the bulletin were made, 22 of which were distributed and 3 held in reserve. The distribution list is considerably longer than is customary in the case of USN R.I. bulletins.

Distribution outside of Naval High Command (8 copies):

Naval Group Command West, Staff (located at Paris and in charge of Naval surface units based on Biscay and Channel ports as well as coastal defense and Channel convoys)

Battle Group (Task group Tirpitz and 4th DD Flotilla in north Norway)

Comsubs Norway/Adm. Northern waters at Narvik

Naval Liaison with Wehrmacht Field Headquarters

German Naval Command Italy

10th Flieger Corps via Air Fleet 3 (West Europe)

GAF Lofoten (the part of the Luftwaffe responsible for reconnaissance on Arctic convoys for Russia)

Small Battle Units Command, (set up early in 1944, in charge of midget subs, explosive motor boats, special commandoes for mining and sabotage)

Distribution within Naval High Command:

6 copies to various sections in Cominch and CMC including U/B operational command (i.e. Chief of SKL, 1 SKL section, 2 SKL/BIU op)

4 copies to ONI (3 SKL)

1 copy to radar and electronics research (5 SKL)

3 copies within 4 SKL itself including one to the DMC.

~~TOP-SECRET-ULTRA~~



(b) Grades of R.I. Information and its Dissemination by dispatch.

Two kinds of R.I. information are distinguished according to their source:

"B-reports or B-information": based on traffic analysis and the reading of open or encoded messages.

"X-B-reports or X-B-information": based on the decryption of high grade traffic.

The captured bulletin contained both "B" and "X-B", the latter being distinguished from the former by framing or boxing in heavy black lines. To avoid any uncertainty which might arise in the interpretation of the information presented in the bulletin a standard form is indicated for degrees of reliability. Any unqualified statement could be taken as certain on the part of the reader. It should be noted, however, that this highest degree of reliability could apply to a good D/F fix as well as to a decrypted statement. "Probably" or "approximately" and "presume" or "presumably" qualified the lesser degrees of reliability in that order. In addition to the bulletin, "X-B situation reports" were issued daily by radio. No examples of these have been seen here. GC&CS describes them as daily summaries, sent out over the signature of the R.I. organization, which contain information from all intelligence sources, but mainly from B-service itself. (XIP/IS/233, p. 1). In addition

~~TOP-SECRET-ULTRA~~

to the above standard dissemination, R.I. material of an urgent operational nature might be sent by dispatch provided it was properly paraphrased and made no reference to source. This practice was to be limited to the most exceptional circumstances, particularly in the case of "X-B" information, for, as pointed out by the Bulletin's printed introduction: "Should the enemy learn that X-B reports are obtained by the deciphering of his radio messages", he would destroy the work of months - even years - by changing his cipher data, and thus one of the most important sources of information for the execution of the Naval war would be destroyed. Had the German Navy observed these instructions more carefully, it might have been impossible for the Atlantic Section to demonstrate the existence and source of "X-B" information.

(c) The Captured Bulletin's Information, its Organization and Scope.

If the captured copy of 23 June 1944 is a fair sample, the German Naval R.I. Bulletin shows the advantage which comes from centralizing the correlation of all interception results. (The captured bulletin covers the period from 12 - 18 June.) It includes studies on topics of current operational interest such as the reconstruction of Atlantic convoy cycles as well as charts showing locations of contacts and attacks reported by Allied units. At the request of OP-20-G, the USN Communications Security section (OP-20-E) examined the document but found "no evidence that U.S. cryptographic systems have been successfully attacked". Other

than the monitoring of RAMS circuits, German attention was concentrated on British Naval circuits, most of which had been subjected to close analysis. Although the information on US - Gibraltar convoys was accurate as far as it went, it was not classified by the Germans as "X-B". Information on US - UK convoys, however, was in part classified as "X-B". No report has been received from the British on the sources of the German information given in the Bulletin but these sources would presumably be described as "low-grade".

5.

Concentration of German C.I.  
on Allied Convoy Traffic.

The captured Bulletin tends to confirm the natural supposition that the German Navy's C.I. organization would concentrate its energies on serving the most important operational part of the Navy, the U/B, and thus would specialize in Allied convoy traffic. That the enemy was adept at exploiting all sources in arriving at a clear and current picture of the convoy situation was shown many times in U/B traffic. There were exceptions, involving curious cases of omission difficult to explain, but on the whole German R.I. did furnish the U/B Navy with that essential requisite for the successful prosecution of the U/B war: good convoy intelligence. The stereotyped nature of convoy traffic may have simplified the German problem so that analysis and delivery group recoveries would suffice to keep the

~~TOP SECRET-ULTRA~~

convoy chart well posted and up to date. Against this background, however, they were able at times to read the actual convoy messages in combined cipher and thus clarify and correct their plots as well as accumulate invaluable knowledge of convoy habits and procedures.

6.  
Use of Non-RI Material.

It will have been noted that four copies of the RI Bulletin were routed to 3 SKL (German OHI) and that the daily "X-B situation report" drew on non-communication sources. The captured Bulletin of 23 June, however, contains little that can be traced directly to outside sources except for the use of Agents' reports in connection with Gibraltar convoys. The extent to which the German RI organization was itself responsible for the correlation of its own material with that from non-RI sources is not known. The fact remains that it undoubtedly furnished the most important intelligence for U/B Command. Before discussing German Convoy Intelligence, it is necessary to review the kinds of information sent to U/B's at sea, with particular reference to the various sources, both RI and Non-RI, which were acknowledged in U/B traffic.

CHAPTER II

INTELLIGENCE DISSEMINATED TO U/B'S AND THE SOURCES  
ACKNOWLEDGED IN U/B TRAFFIC.

\*\*\*\*\*

Table of Contents

1. Dissemination to U/B's at Sea.
2. The course of the war as reflected in Intelligence sent to U/B's at sea.
3. Sources acknowledged in U/B traffic.
4. Aerial Reconnaissance.
5. Submarine Reconnaissance and Observations of Enemy Conduct.
6. Agents.
7. Prisoners of War, Survivors of encounters at Sea.
8. Radio Interception.

INTELLIGENCE DISSEMINATED TO U/B'S AND THE SOURCES  
ACKNOWLEDGED IN U/B TRAFFIC

1.  
Dissemination to U/B's at Sea.

A constant effort was certainly made to inform U/B's at sea of any intelligence which might assist them in their task. Thus, in addition to information on convoys and independents, both general and particular in its application for the offensive war, hundreds of messages concerned Allied A/S activities. Intelligence for the U/B's defensive war included not only the number and disposition of A/S units, whether surface or air, but also tactics, armament, and especially A/S location devices. From time to time general estimates of Allied defenses for the various U/B operational areas were added to the voluminous files of instructions which U/B's were obliged to carry and which were kept up to date by radio transmissions. The nature and tempo of the U/B war required, in German eyes at least, a reliance on radio communications not only for the dissemination of current intelligence for offensive operations but also every scrap of information that could be gotten together on Allied defenses. Hence the reader of U/B traffic was supplied with a surprisingly large background for judging German anxieties, suspicions, fears, and misconceptions, together with plans and hopes, or expedients, for counter action. As the U/B task changed

or as the conditions surrounding its execution altered, the intelligence sent to U/B's was modified.

2.

The course of the war as reflected in Intelligence sent to U/B's at sea.

(a) During the winter offensive, 1942 - 43.

Intelligence disseminated to U/B's during the winter offensive of 1942-43 was almost altogether on convoys, with emphasis on US-UK lanes. Other intelligence was issued only in so far as it bore upon or could be worked in with the convoy offensive. Intercepts of Allied contact and attack reports were rarely repeated on U/B circuits, and then merely to request a clarification from the U/B's concerned.\* Reports of M/V sinkings in distant areas were occasionally relayed on appropriate circuits with requests for the identity of the U/B's responsible for the sinkings.

(b) During the summer of 1943.

As the U/B went on the defensive and sought out distant areas for operations, a distinct type of U/B message gradually became a commonplace, and was to remain such: viz., the repetition of Allied contact and attack reports. These Allied reports became

\* For examples, see 1034/2/1/43: B-Service report of attack on U/B in OS N. - 55 W.; Mohr (U-124) replied. Also 1324/5/2/43 to Group NORDSTURM: "We have two English reports of attack". Gretschel (U-707) replied.

a kind of substitute for U/B unit transmissions in view of the increasing need for radio silence on the part of the U/B. The general defense situation reports for the Atlantic became remarkable for length and for new editions. Instead of convoy intelligence on the old scale, traffic situation reports for distant coastal areas and the Caribbean were on the air.

(c) Resumption of convoy offensive. Winter 1943 - 44.

The renewal of the North Atlantic convoy offensive brought back the convoy intelligence messages. Indicative of German difficulties in finding the convoys of an enemy who was reading everything the German Navy put on the air and reading it currently was the appearance of new types of intelligence messages: the relay of D/F fixes on Allied unit transmissions and special reports from intercept parties on board U/B's. Allied knowledge of the U/B's whereabouts was reflected in the constant flow of messages which endeavored to analyze the success of Allied location devices. The repetition of contact and attack reports continued, increasing noticeably in the spring of 1944, particularly for the Biscay area, and gradually working around to include the Indian Ocean as well. The disposition and habits of USN CVE groups were pressing concerns which necessitated revisions of current orders on the defense situation in an effort to determine where and when U/B's might safely surface. Attempts were made to evaluate all the underwater sounds reported by U/B's in terms of new kinds of acoustic search buoys,



counterdevices for the acoustic torpedo, bluff, or marine biology.

(d) After the summer of 1944.

The German attempt to fight with an outmoded U/B which could not escape detection by a superior enemy gradually filled U/B traffic with messages concerning the problem of U/B defense. A time was reached when U/B traffic seemed to reflect more Allied activity than German activity. With the introduction of the Schnorchel U/B German interest in underwater sounds was intensified and concern with Allied radar remained as acute as ever. Operational intelligence messages became very detailed accounts of Allied shipping in coastal areas. In April 1945 the "Harke" gesture towards a revival of convoy warfare was accompanied by convoy intelligence indicating that the convoy plot had been kept up to date even though not used.

3.

Sources acknowledged in  
U/B traffic.

A summary of the various sources of intelligence which were acknowledged in U/B traffic will not contain any startling revelations, for these sources are the ones which the enemy is expected to have. They should be borne in mind, however, for it was against this background that one had to judge possible sources when no acknowledgment was given.

4.

Aerial Reconnaissance.

~~TOP SECRET-ULTRA~~

It was not always possible to know when convoy intelligence could be accounted for by GAF sightings, even when the convoys were in the areas of GAF range, for acknowledgments were not consistently made. Such a source could usually be presumed with a degree of safety in the Mediterranean, along the England-Gibraltar convoy lane, along the Arctic route to Russia, and to some extent over the western approaches to Great Britain. Attempts were made in the spring of 1944 to home U/B's on England-America convoys by means of special LR A/C in area 20 W.

5.

Submarine Reconnaissance and  
Observations of Enemy Conduct.

Submarines were themselves used in the effort to accumulate detailed observations of shipping and defense in distant coastal areas. The cumulative results were customarily repeated as "Situation and Traffic Reports" for the benefit of U/B's about to enter the area concerned. Some of this information could be traced to a particular U/B's own transmitted reports, but here again there was no certainty on many points. U/B war logs were sometimes acknowledged as the source. When Schnorchel U/B's undertook a close-in blockade of British ports during the winter of 1944-45 their situation reports on British coastal waters became especially detailed and systematic. The "Halm" ("Blade of grass") series of Officers sent to U/B's on 13-14

February 1945 offered a correlation of information on shipping which undoubtedly used non-U/B sources. By such means U/B's were given a clear and accurate summary against which to judge the significance of their own observations. In addition to reconnaissance, U/B's were required to make special reports on Allied location devices, briefs of which were transmitted by radio. In this way it was possible to follow the struggles of the U/B with allied radar, from the reports of radar transmissions intercepted on the early U/B search receivers through all the subsequent attempts to isolate the mysterious source of Allied superiority. A numbered series of "Experience Messages" kept U/B's informed of Allied A/S behavior and German interpretations.

6.  
Agents.

(a) Gibraltar area. Information from agents, as seen through U/B traffic, was confined largely to the Gibraltar area: Ceuta, Cape Tres Forcas, Gibraltar, Alboran, Cape Spartel. The Germans followed all ship movements in and out of the Straits. Cape Spartel would report size and composition of an inbound convoy and its escort, giving exact time of sighting, line of bearing, and speed. Gibraltar would follow up with what ships had put in to or out of Gibraltar. German aerial reconnaissance would pick up the convoy after it had passed into the Mediterranean. All of this information was relayed on Mediterranean U/B circuits, or on

Atlantic circuits in the case of an outbound convoy. Clandestine traffic from the agents themselves was available to the Atlantic Section.

(b) Agents elsewhere. Particularly active in 1943 were the agents at Lourenco Marques and in the Cape Town area. Their traffic was also available to the Atlantic Section. It was possible to identify information passed to U/B's with specific reports which had gone in from these agents - both Italian and German. Occasionally information, presumably from agents, was disseminated on independent ships out of Takoradi, Lagos, Egypt, Persian Gulf, etc. In 1945 agents furnished information on shipping in Cherbourg, as well as the location of a minefield off Fastnet, Ireland. In addition to details on shipping in the Gibraltar area, Japanese Military Attache traffic from Lisbon to Berlin carried much information on trans-Atlantic convoys including dates of departure from the U.S. A "reliable" Italian agent claimed the U.S. Naval Attache's office in Lisbon as the source of his report on the disposition of the U.S. Fleet. (FPB 33, 3/11/44). The reports of agents in England were seen in Clandestine traffic via Spain. There is at least one case in which the sailing date of a US convoy (US 27) was attributed to an agents' report. (2013/16/12/43 to "Alsterufer" and "Osorno"). As a rule, however, German U/B traffic reflected only a small part of an organization which was apparently extensive and active but whose outline could not be discerned.

~~TOP SECRET-ULTIMATE~~

7.  
Prisoners of War, Survivors  
of encounters at Sea.

Statements from survivors were occasionally passed immediately to Control by U/B captains. On one such occasion information on an England bound convoy (SC 118) was forwarded while the operation was still in progress. U-266 (Jessen) sank a straggler and captured the ship's captain and engineer. Within a few hours Jessen transmitted the following:

Prisoner's statement: Endloff's convoy approximately 45 ships of which 15 are tankers. Broad formation, 10 columns. Destination North Channel. Inner and outer defense. Steamer frequency at present 50 meters.

Convoy formation: 10 columns, each with 4 to 5 ships. Distance between columns 900 meters. Distance between ships 550 meters. Speed 7-8.  
(2031/6, 0047, 0120/7/2/43).

Some information on the general routing of convoys and independents in the South Atlantic and on the Caribbean-New York run was gained in this manner. With the increasing effectiveness of Allied A/S measures U/B's were urged to take prisoners, especially from A/C shot down, and interrogate them on tactics and devices for U/B location. In December, 1943, a prisoner from a Wellington helped materially in dispelling German fears of submarine location by amazingly effective search receivers.

8.  
Radio Interception.

(a) Direction Finding: Prior to the fall of 1943 little

or no attempt had been made to supply U/B's with current D/F's. Beginning with the resumption of the North Atlantic battle, however, U/B circuits relayed an increasing number of fixes on Allied unit transmissions. During January, 1944, for example, no less than 51 D/F fixes were sent to U/B's in the North Atlantic. The area covered was usually north of 40 N. and east of 30 W., but a few fixes were made as far west as 56 W. It does not appear that effective use was or could be made of this information by U/B's at sea, although a certain amount of correlation with the current convoy chart was attempted from shore for their immediate benefit.

(b) Traffic Analysis: Acknowledgments of traffic analysis as a source of information were sometimes seen in Mediterranean traffic, and more frequently in Arctic U/B traffic. In 1944-45 U/B's in the Far East were furnished with the results of Japanese traffic analysis on the movements of major fleet units in the Indian Ocean. Although the acknowledgment of traffic analysis as a major source of information on Atlantic convoys was extremely rare, it was assumed in the Atlantic Section that German knowledge of the convoy cycles came principally from this source, particularly in view of the stereotyped nature of convoy traffic. GC&CS recognized that valuable information on Atlantic convoys was gained through the recovery of delivery groups and the study of call signs, on which it was known that German C.I. placed considerable emphasis. (See ZIP/ZG/252, p. 4). Captured German documents:

\*In addition to the Naval RI Bulletin of 23 June 1944 already referred to, see ZIP/SAC/P.7, a GAF RI bulletin.

~~TOP SECRET - ULTRA~~

have confirmed the extensive use of traffic analysis not only in reconstructing convoy cycles but also in the correct identification of convoys by designator and number. RAF Coastal Command traffic was also exploited in connection with convoy movements. The GAF C.I. organization worked in close collaboration with the Navy in such matters.

(c) Allied transmissions in plain language or in self-evident code: The repetitions of M/V distress signals, RAMS submarine contact and attack reports, and A/C reports on U/B's were frequently acknowledged by the phrase "according to B-Service". It became quite evident that German intercept service guarded the RAMS circuits with care and that U/B Command correlated these reports with his submarine tracks, issuing orders and reprimands on the basis of them. The Atlantic Section watched the repetitions of these reports in German traffic and invited COMINCH's attention to the advantages derived from them by the enemy.

(d) Interception by U/B's.

Although there are a few cases of U/B monitoring on the international distress frequency in connection with attacks on merchantmen, U/B traffic does not show this to have been of any importance. It was certainly never stressed by Command. The only serious attempt, by U/B's at sea, to exploit Allied radio transmissions was that made on convoy voice traffic, for which trained operators were provided in 1943. (See "B-Dienst on Board

Chapter V).  
U/Boats"). The most persistent attempt at interception of Allied transmissions was that directed against radar. In addition to warning for the individual U/B, radar interception was intended to build up a knowledge of Allied radar characteristics and tactics. Early in 1944 certain U/B's were equipped with special search gear and trained men to carry out "Feldwache" tests in an effort to determine what frequencies the Allies might be using which the standard U/B receiver could not pick up.



CHAPTER III

GERMAN INTELLIGENCE ON ALLIED CONVOYS IN THE ATLANTIC.

Ch  
II

\* \* \* \* \*

Table of Contents.

1. "Convoy Expected."
2. In relation to cipher compromise.
3. Convoy Chart for Blockade Runners, Dec. 1943 - Jan. 1944.
4. North Atlantic Convoys.
5. US-North Africa Convoys.
6. Notable Failures to Disseminate information on US-Gibraltar Convoys.
7. UK-Africa Convoys.
8. Analysis of Convoy Communications made by Atlantic Section; Recommendations submitted to Cominch.

~~TOP SECRET~~

GERMAN INTELLIGENCE ON ALLIED CONVOYS IN THE ATLANTIC.

1.  
"Convoy Expected".

The enemy possessed at all times a reasonably clear picture of Atlantic convoys with varying degrees of accuracy as to routes and day by day plotting. Although independents were not neglected, information on convoys was obviously more important for the U/B war. Even when group operations were abandoned, knowledge of convoy gathering and dispersal points, ports of entry and departure, and the shipping lanes in coastal areas remained essential. As a rule, convoys were referred to in terms of general course, e.g. "northeastbound convoy", followed by area and date of expected arrival, the area usually being the patrol line itself. In only a few cases, during the fall of 1943, were convoys ever referred to in U/B traffic by initials (e.g. 1626/16/9/43, "OH", "ONS" to Group LEUTHEM). That the enemy knew the correct convoy designators and numbers, however, was clearly shown in Blackade Runner traffic (Dec. 1943 - Jan. 1944), to say nothing of the evidence now available in captured documents.

2.  
In relation to cipher  
compromise.

The "convoy expected" messages came from a background of correlation which included all the sources mentioned in the

preceding chapter, with the addition of important punctuation from the reading of convoy dispatches in combined cipher. General convoy intelligence is being discussed here before going into cipher compromise (for which, see next chapter), because the latter represents a refinement of the "convoy expected" messages, both from the German point of view and from that of the Atlantic Section. There is no way of determining at present to what extent information from cipher compromise was interwoven with the standard convoy expectations. For the most part general convoy intelligence and expectations of particular convoys were not sent in the Offizier cipher which was shown by experience to be the normal means for relaying decryption intelligence. There could be no assurance, however, that decryption intelligence had not played a part in patrol line shifts and formations not ordered by Offizier. There is no reason to believe that the Germans were always consistent in observing their own security regulations.

3.  
Convoy Chart for Blockade  
Runners, Dec. 1943 - Jan. 1944.

The most complete single statement of German convoy intelligence ever seen here in German Naval traffic came in a series of messages to homebound Blockade Runners in December 1943 and January 1944. These messages apparently reproduced

the enemy's current convoy chart for the North Atlantic, including the Gibraltar lanes. The convoys then at sea were correctly identified both by designators and numbers, and accurate information on convoy cycles, speeds, and general routing was given.

(a) US-UK convoys, General:

- "1) Convoys from Halifax to England (abbrev 'HX') and Sidney-Canada-England convoys (abbrev 'SC') and English convoys (abbrev 'ON' or 'ONS') generally navigate a great circle from which deviation occurs only if threat from U-boats warrants. Therefore convoys are paired on fixed lanes. The northern portion of these fixed lanes is by far the most navigated". (0105/17 Dec. ALLE 66).
- "2) 'HX' and 'ON' convoys have a day's run of 204 miles. 'SC' and 'ONS' a day's run of 150. 'HX' and 'ON' convoys run at intervals of 6 and 7 days alternately, 'SC' and 'ONS' at intervals of 13 days.
- 3) Stragglers are to be expected after every convoy. They are routed on constantly changing courses." (0253/17 Dec. ALLE 67).

(b) US-Gibraltar convoys, General:

"Designations: 'UG' = US to Gibraltar  
'GU' = Gibraltar to US  
Add 'S' for slow, 'F' for fast.  
(0854/5 ALLE 91)  
(1054/22)

Cycle: 10 days

Speed: 204 miles per day (8.5 knots) for 'S'.  
(0854/5 ALLE 91)

Route: Between 32 N. and 36 N. from 63 W. to Gib.  
(0854/5 ALLE 91)

Escort: ... varies. ((Details)) not exactly known here. Far ranging recce by A/C and close escort by DD's and DE's must be assumed".  
(1540/8 ALLE 92).

(c) Dead Reckoning for particular convoys:

On 16 December 1943 Blockade Runners "Osorno" and

"Alsterufer" received D/R estimates for the following convoys: EX 270, SC 149, ON 215, ONS 25, and UGS 27. On the 18th, England-Mediterranean convoys KMS 36, MKS 33, and MKS 34 were added. (1900, 1933, 1948, 2013/16/12 DAN 7-10; 1013, 1037, 1102/18/12 DAN 33-35).

D/R plots on GUS 26 and UGS 30 were sent on 5 January, (0854/5 ALLE 91). The convoy identifications were correct. D/R estimates for US-UK convoys were given in terms of successive "standing lines". For example, convoy EX 270 was plotted for 18 December as being somewhere along a line extending from 51 N., 36 W. to 43 N., 35 W. The "standing lines" for EX 270 and SC 149 ran approximately from the standard eastbound convoy route "B" on the north to standard route "C" on the south and did in fact lie across the routes taken by these convoys. Had any one of the "standing lines" west of 30 W. been occupied by U/B's after the fashion of the preceding winter, contact would have been made at about the estimated time. Group RUEGEN, then in the area E. of 30 W., was informed of these "eastbound" convoys, but, strangely enough, the timing given to the U/B's was not as accurate as that given the Blockade Runners. The plotting of ON 215 and ONS 25 was rather poor. GUS 26 and UGS 30 were plotted with fair accuracy in the area between the Azores and Bermuda.

4.  
North Atlantic Convoys (US-UK).

Accumulated evidence indicates that convoys which were

~~TOP SECRET-ULTRA~~

not "expected" by U/B's were simply those in which the enemy could not take an operational interest. As the North Atlantic began to fill up with U/B's in January 1943, the number of "convoy expected" messages increased, accompanying the formations of lines for practically every major eastbound convoy from the middle of January to the end of May. On the whole a high standard of accuracy was maintained. Convoy diversions were sometimes learned from decryption in time to rearrange U/B patrol lines appropriately. In addition, the large number of U/B's and the pattern of their arrangement in groups tended to negate convoy diversions by covering the major possible diversion routes. Contacts were thus made by U/B's other than those for which the convoy was originally intended. German knowledge of the entire convoy situation was in this way constantly clarified and amplified. During the summer of 1943 there was no check on the convoy plot such as had been furnished by U/B operations. Despite this lack, convoy expectations began again promptly and accurately with the resumption of the North Atlantic offensive in September, 1943. More "convoy expected" messages marked the unsuccessful campaign of 1943-44 than the campaign of the preceding winter. From an average of about 7 a month during the winter campaign of 1942-43, these messages rose to an average of about 10 per month during the following winter. This increase signified the lack of success, reflecting not only a

carry-over of unused patrol lines but also the willingness of patrol lines to take Westbound as well as Eastbound convoys. Furthermore, convoy intelligence assumed a new function in 1943-44 which had been unheard of in the North Atlantic during the preceding winter; warning to U/B's of the possibility of encountering carrier borne A/C and other forms of A/S activity. Of the 38 HX and SC convoys which sailed for England from 13 September, 1943 to 22 February, 1944 no less than 34 were referred to in U/B traffic; of the 35 ON and ONS convoys during the same period, 27 were mentioned. There are several instances in which U/B Command showed a knowledge that could not have been gained simply from convoy cycle plotting, quite apart from the presumed and confirmed cases of cipher compromise. For example, when Group CORONEL was formed in December 1943 to operate against "a slow westbound convoy", Command must have known not only that ONS 24 and ON 214 were not proceeding on similar routes, as had been customary, but also that it was ONS 24 which was taking the northerly route. The insight which the Germans gained solely by analysis of the heavy volume of stereotyped combined cipher traffic on US-UK convoys probably found valuable supplementary information in local British "low-grade" communications.

5.

US-North Africa Convoys.

Although the German Navy had no advance information on the North African landings in November, 1942, they had no difficulty

in building up a knowledge of US-North Africa convoys from agents in the Gibraltar area, traffic analysis, and GAF reconnaissance. In addition a large amount of convoy radio traffic in the Mediterranean was sent in combined cipher. U/B group operations and convoy expectations on the US-Gibraltar lane may not have functioned with a smoothness comparable to that on the US-UK lanes, but no lack of intelligence seems thereby indicated. There are, however, the possible failures of intelligence which are discussed in paragraph 6 below.

(a) To summer, 1943. Operational Intelligence.

During the only period in which U/B groups kept vigil on the US-Gibraltar lane (winter 42-43) at least 4 eastbound convoys were "expected", one of them UGS 6, on basis of cipher compromise. Only 1 westbound convoy, GUS 4, is known to have been awaited; cipher compromise also played a part in this case. The best operations, with the possible exception of UGS 6, seem to have resulted from accidental contacts. Group DELPHIN's destruction of the tanker convoy TM-1 in January was due to an early sighting by a U/B bound for the Trinidad area. Consubs recognized the target, however, as the first Trinidad-North Africa convoy. When U/B's (Group TRUTZ) returned to the US-Gibraltar lane in June 1943, after an absence of two months, they were certainly provided



with good intelligence; in fact the formation of Group TRUTZ must have been due in large part to compromise of Flight 10's routing dispatch. The enemy was also aware of GUS 7A and, later, of GUS 8A, but did not show any realization in traffic of UGS 9 which was proceeding near Flight 10.

(b) Interest increases in winter 1943-44.

Information on US-Gibraltar convoys did not reappear in U/B traffic until the fall of 1943, when U-177 (Gysae), returning from an extended patrol off So. Africa, was given D/R positions for UGS 18. The positions were a good 10 degrees ahead of the convoy's progress, indicating a German plotting at 10 to 10.5 knots whereas the convoy was making 9. Gysae received the information primarily for warning. Warning seemed the purpose of subsequent dissemination of intelligence on these convoys, which increased noticeably during the winter. In December D/R plots on convoys UGS 26 and GUS 23 were sent to 5 U/B's which were crossing the lane. The positions were much nearer the truth than those for UGS 18 had been, but they did not show any exact knowledge of the standard route. While not precise, they were still sufficiently accurate to have effected contact by a suitably disposed patrol line. From January to March, 1944 each successive UGS and GUS convoy (UGS 27-34, GUS 26-32) was referred to in terms of Gibraltar arrival or departure for benefit of U/B's trying to enter the Mediterranean. Thereafter such information was disseminated only on the few occasions when U/B's were ordered to individual patrols in the Gibraltar approaches.

~~TOP SECRET ULTRA~~

6.  
Notable Failures to Disseminate  
Information on US-Gibraltar convoys:

One assumes that the Germans kept a current plot on UGS-GUS convoys in which some confidence was felt. It is therefore difficult to account for certain failures to warn supply subs or to change their R/V positions during June, July and November 1943. Two supply subs were sunk and one endangered in positions which either show poor convoy intelligence or a failure to correlate and use such intelligence as was at hand. Although no D/R positions farther west than 37 W. were ever given to U/B's, Blockade Runners had been furnished with D/R positions on UGS 30 and GUS 26 as far west as Bermuda. The latter had been originated by a non-U/B section of the Navy (1 SKL), but it is hard to believe that U/B operational command (2 SKL/BdU op) did not have access to all available information and that it was not capable of plotting convoys all the way across with operational accuracy, or what was deemed operational accuracy.

- (a) Case of refueler Grygan, U-118, sunk 1410Z/12 June 1943, in 30.49 N. - 33.49 W. by TG 21.12 (Bogue).

Plans for Grygan's refueling station in 30.45 N. - 33.40 W. were announced in U/B traffic on 31 May. On 12 June he was sighted on the surface and sunk within 6 miles of this position. No change had been ordered in his R/V assignment despite German knowledge that between 31 May and 12 June considerable A/C

protected Allied shipping had passed through this area. At no time during this interim did Command show any real awareness of the true situation. He did know about Flight 10 and GUS 7A but he apparently knew nothing of UGS 9 or of TG 21.12. Czygan was warned late on 5 June that an eastbound convoy with A/C escort could be expected on 7 June, but this was after the Bogue had attacked the TRUTZ line. Command had Flight 10 in mind and not UGS 9. The danger from UGS 9 was much greater than that from Flight 10, for the latter had altered course to north after passing through the TRUTZ line on 5 June while TG 21.12 had turned south to cover UGS 9, which was proceeding along 29.30 N. Schnoor, U-460, another supply sub, was in the immediate vicinity. Command showed no awareness of UGS 9 until after Manseck (U-758) had accidentally sighted the convoy and had been so heavily bombed for his trouble that he prepared Command for the loss of his boat, after having explained that he had been attacked by carrier-borne planes. Manseck pulled off to the south. Not until then were the two supply subs warned that Manseck's sightings were probably on an eastbound convoy and that they should watch out for carrier A/C while going to Manseck's rescue. By following Manseck's southerly course Schnoor and Czygan were drawn out of harm's way. But after Manseck had been found, still afloat, and turned over to Schnoor's custody, Czygan returned to his original R/V assignment -- in time to meet TG 21.12 on its return sweep. It should be pointed out that the area south of the Azores had been used

~~TOP SECRET ULTRA~~

for refueling R/V's many times in the past without mishap. One might also argue that Command had every reason to believe the 3-4 day old wake of a convoy a safe place for a refueling R/V. Gysan's sinking, however, surely indicates, besides ignorance of UGS 9, that Command was unprepared for the offensive nature of a task group that might engage in free maneuvers of its own.

(b) Case of refueler Metz, U-487, sunk 13 July, 1943, in 27.15 N. - 34.18 W. by TG 21.12.

The important nature of Metz's assignment in July has been dealt with elsewhere. His loss was an irreparable misfortune. One might then expect that the best of German intelligence would have been concentrated on his safety. Yet he had not quite arrived at his assigned R/V position, 27.09 N. - 33.27 W., when he was sunk 1700Z.13. C&R's plot for GUS 9 at 2000Z/13 was 27.01 N. - 33.39 W., within 9 miles of the R/V position assigned to Metz. In blocking the US-Gibraltar lane to the north of 30 N. with Group FRUTZ, U/B Command had contributed materially to the southerly routing of GUS 9 which had brought TG 21.12 to Metz.

(c) Case of refueler Bartke, U-488, November, 1943.

The loss of U-115 and U-487 may have started the policy of warning U/B's when crossing the US-Gibraltar lane, for this type of message was not seen during the summer of 1943. Gysae was warned in September. Nevertheless, Bartke was twice seriously endangered by convoys during his November cruise without receiving any warning from Control. While passing from one R/V position to another in the area mid-way between Bermuda and the Azores he was

~~CONFIDENTIAL~~

surely within 60 miles of GUS 19 on the evening of 7 November. Again on 9 November he crossed UGS 23's path not many miles ahead of that convoy. Bartke later reported that he had been depth charged and damaged on 8 November. Approaching Biscay on his return cruise, Bartke was given a D/R position on a Gibraltar-England convoy. Warning messages were not sent because of a near collision on the German U/B convoy chart; U/B's were warned, when warned, even <sup>on</sup> a remote chance of encounter. For one thing, Command's day by day knowledge of a U/B's position was not necessarily accurate. Hence it seems reasonable to suppose that Bartke would have been informed had the German chart shown any convoys at all between Bermuda and the Azores.

(d) Comment on German Intelligence US-Gibraltar convoys, August and September, 1943.

As of 15 September, 1943 BdU gave the following account of US-Gibraltar convoy routes in Operational Order #56 (Memo document):

"The convoy routes lie between 30° and 40° North latitude; the convoys coming from America travel in the southern part, those going to America in the northern part of this lane. Extensive detours, particularly to the south, after attacks on this traffic."

On 16 August 1943 Current Order #11 carried this statement to all U/B's at sea:

"For the protection of America-Gibraltar convoys, one or more carriers are located in the area CD ((from 34 to 43 N., 26 to 35W.)) and DF (from 26 to 34 N.,

35 to 45 W)). Many repulsed attacks and the unexplained loss of several subs homeward bound testify to this. In sum, carrier-based aircraft can always be counted on in the whole sea area between Gibraltar, New York and 25 degrees North. All the machines, even the carrier-based planes, are probably fitted with radar..."

One assumes that the September information on convoy routes was available in June and July. Current Order #11, however, seems to speak directly from the costly experiences of June and July. And yet Operational Order #56 declares that:

"Since the spring of 1943 the enemy has assigned auxiliary carriers to the area between 25° and 40° West, which is otherwise hard to patrol. These are escorted by from 2 to 4 destroyers, watch over the area mentioned and in case of U/B attacks come to the aid of the endangered convoys."

Apparently the detailed implications of this paragraph were not anticipated, or, if anticipated, were left blank to be filled in by experience.

#### 7. UK-Africa Convoys.

At times inbound and outbound U/B's were informed of convoys on the UK-Gibraltar lane, either for purposes of operation or for warning. During the period from April to June 1943, 5 Officer messages were sent to U/B's along the NW African coast informing them of D/R positions on UK-African convoys. These cases could be studied here to a limited extent only since the convoys were entirely British and no convoy files were available.

It was later learned that GC&CS presumed these to be instances of compromise, probably derived from dispatches sent in combined cipher #3. (See Appendix on "Cases of Presumed and Confirmed Compromise of Allied Communications, 1943-45").

8.  
Analysis of Convoy communications  
made by Atlantic Section; Recommendations  
submitted to Cominch.

Because of the renewed persistence of convoy intelligence in German traffic in the fall of 1943 the Atlantic Section felt obliged to follow up its studies on cipher compromise by an examination of convoy communications procedure and habits. It was of course recognized that the tremendous convoy undertaking could not in practice satisfy all the demands of security theory, but the apparent ease with which the German CI organization maintained its hold on Allied convoys, particularly US-UK, suggested that some improvement could be made in our own communications, quite apart from the introduction of Naval Cipher #5, which had immediately followed the demonstration of extensive compromise in #3.

(a) Findings.

It was found that standard procedure made the task of enemy traffic analysts relatively easy. In addition to the heavy reliance on combined cipher, tables "M" and "S", with the subsequent overburdening of a weak system, the timing of the many radio dispatches concerned with each convoy observed a pattern as regular

as that of the sailings themselves. In the case of HX-SC convoys during the fall of 1943 the ocean route was broadcast by CINCCMA approximately 4 days prior to each sailing. On the day of sailing and at a set interval after the sailing, each convoy was again announced in the fixed pattern messages from ports of departure and from the authorities concerned with escort relief at the ocean meeting point. The ocean meeting point usually gave rise to exchanges of dispatches between escort commanders and shore commands. A convoy diversion would be followed immediately by a RAMS broadcast. In the case of US-Mediterranean convoys correct identifications in Blockade Runner traffic had aroused particular interest here, but intensive study of available data had failed to prove cipher compromise. The investigation of UGS-GUS communications for the period from November 1943 through January 1944, however, did show beyond question that traffic analysis of the Mediterranean end alone should suffice for maintaining and correcting knowledge of the convoy cycle. A surprisingly large amount of fixed pattern radio traffic was broadcast in the world-wide table of Combined cipher for the information of practically every Allied command of any description in the Mediterranean area. These dispatches followed a fixed timing in relation to the convoy's progress. The check made by agents at the Straits or by GAF reconnaissance seemed almost unnecessary as far as major convoys were concerned.

(b) Recommendation.

The results of these studies were made available to USN



Communications Security and COMINCH. To eliminate the dependence on combined cipher in the Mediterranean the introduction of more cipher machines was hastened. For US-UK convoy communications certain remedial measures were drawn up and submitted to the Director of Naval Communications, who incorporated them in a memorandum for Cominch (F-34). It was recommended that:

- a. All shore authorities and ships in Western Atlantic be notified by dispatch that messages should be sent in 'A' or 'K' rather than in 'M' or 'S' Table when the 10th Fleet C&R is the only US authority included in the address.
- b. All shore authorities and escort vessels in the Western Atlantic be notified by dispatch that messages addressed to US authorities in addition to 10th Fleet C&R, but of whom no immediate action is required, be sent as in (a), above, with appropriate passing instructions in the text.
- c. Cincopa make greater use of aircraft to carry home messages for ships and that such aircraft report last location of convoy rather than that escorts break radio silence to report positions.
- d. Admiralty modify convoy instructions particularly to stress the great danger of breaking radio silence and using homing procedure in the mid-Atlantic.
- e. Admiralty and Cincopa examine the standard reports required by shore authorities and escorts in connection with convoys with a view to eliminating unnecessary reports or stereotyped patterns."

CHAPTER IV

COMPROMISE OF NAVAL CIPHERS #3 and #5.  
(Anglo - U.S.)

With two Appendices listing cases  
of presumed and confirmed cipher  
compromise.

Ch  
I

\* \* \* \* \*

Table of Contents

1. Statistical Summary, with comment.
2. Fears of Compromise, February, 1943.
3. Fears communicated.
4. Further evidence, March 1943.
  - a) RAUBGRAB, Convoy HX 229
  - b) Convoy TO-2
  - c) Convoy UGS 6
5. Compromise established, May 1943. Convoy HX 237.
6. Demonstration of Compromise accepted. Action taken.
7. More compromise - to 10 June 1943.
8. Comment: The enemy's own Ultra intelligence during U/B decline.
9. Compromise of Naval Cipher #5 feared. September 1943.
10. German awareness of standard convoy routes.
11. Evidence accumulates. SC 142 and U-220.
12. HX 257, ON 203. COMINCH communicates apprehension to First Sea Lord.
13. Compromise of Naval Cipher #5 confirmed. October 1943. HX 261.
14. SC 146 diversion compromised. November 1943.
15. Indications of Combined Cipher Compromise cease in U/B traffic.

~~TOP SECRET ULTRA~~

COMPROMISE OF NAVAL CIPHERS #3 and #5  
(Anglo - U.S.)

With two Appendices listing cases  
of presumed and confirmed cipher  
compromise.

1.  
Statistical Summary,  
with comment.

For the period from January through June 1943 there are at least 39 cases in U/B traffic of presumed or confirmed compromise of Allied naval radio communications. These cases are listed in Appendix A together with cases which appeared after this period. Appendix B, taken from a British study, lists confirmed cases of cipher compromise for 1942. The enemy sources referred to in Appendix B were not available to the Atlantic Section of 20-G. Nearly all of the 39 cases for January-June 1943 whose sources have been identified involved Naval Cipher #3, tables "M" and "S", and it is probable that those whose sources were not identified likewise involved this cipher.

~~TOP-SECRET-ULTRA~~

**TABULATION for January - June 1943.**  
 (The case numbers refer to Appendix A)

<u>Month</u>	<u>Precise Source Unknown</u>	<u>Confirmed Source Identified</u>	<u>Total</u>
January	3	1 (case 1) (British Nav. Code)	4
February	4	1 (case 5) (Nav. Cipher #3)	5
March	3	1 (case 3) (Nav. Cipher #3)	4
April	2	1 (case 3) (Nav. Cipher #3)	3
May	7	8 (9)	15 (16)
June	<u>6</u>	<u>2</u>	<u>8</u>
	25	14 (15)	39 (40)

(Appendix A contains 40 for this period rather than 39 with the addition of a case in May, taken from British records. The German message involved was not sent to U/B's. See case 5 for May.)

After the introduction of Naval Cipher #5 in June only 2 cases of confirmed compromise were recorded, one in October and one in November, 1943.

(a) Comment.

For a discussion of delay in Allied counteraction the reader is referred to the chapter on German Intelligence in Volume I. The present chapter's concern is with cipher compromise in relation to the Atlantic Section of USN CI and to the information currently available to it. The tabulation above, however, incorporates a British study received after the compromise of Naval Cipher #3

had been definitely demonstrated here. In no one of the 3 cases listed above as confirmed for the period February through April 1943 was the compromised Allied dispatch available to the Atlantic Section. Nor were these dispatches found in the Navy Department's files.

2.

Fears of Compromise,  
February, 1943.

The highly successful attack on Convoy ON 166 in February 1943 crystalized suspicions of cipher compromise, although compromise could not be demonstrated at that time. Last minute shifts in the patrol lines of Groups RITTER and NEPTUN at 2322A and 2330A on 18 February showed clearly that German Admiralty had abandoned the idea of operating on an expected Eastbound convoy (HX 226) and was rapidly reforming his lines for a Westbound convoy (ON 166). Within a few minutes of these changes, at 2349A/18 a third group of U/B's, KNAPPEN, was formed to swing out to the southeast of the NEPTUN-RITTER line and thus cut off any possible southerly diversion of the convoy. It was KNAPPEN that made contact on the morning of the 20th, U-604's (Hoeltring) hydrophones having picked up the convoy screws. Three diversions had been sent to ON 166 on 17-18 February in Naval Cipher #3, table "B", as the convoy attempted to clear the U/B area by proceeding on a southerly course.

In addition, several position reports had been sent by the convoy before 17 February in table "S". That U/B Command had accurate information on the convoy can scarcely be questioned. The disposition and shifting of the U/B groups between 18 and 20 February suggest knowledge of the convoy's diversion rather than reckoning based on the convoy's own pos reports. Of the three diversions sent, the first one, 1001Z/17 from CINCWA, seems the most likely suspect, not only from the point of view of the time lag, but also in view of the U/B disposition. This first diversion would have sent the convoy through the RITTER line just to the south of its mid point. The straggler's route would have passed through KNAPPEN's line.

3.  
Fears Communicated.

On 26 February the Atlantic Section sent a memorandum to COMINCH calling attention to the extraordinary and effective sequence of changes in the U/B lines from 18 to 20 February, and the fear of compromise was orally communicated to COMINCH by the CO of the Atlantic Section.

4.  
Further evidence, March  
1943.

- a) RAUBGRAF, Convoy HX 229
- b) Convoy FO-2
- c) Convoy UGS 6.

(a) RAUBGRAF, Convoy HX 229.

The RAUBGRAF operation in mid March on HX 229 and SC 122,

"the greatest success yet achieved against a convoy", was probably assisted in large part by a compromised diversion dispatch, sent in the world-wide table of combined cipher. U/B traffic suggests that HX 229 was the one involved in compromise rather than SC 122, which was proceeding on approximately the same route with HX 229. After the operation was well underway Command recognized that he had two convoys, but the one first contacted and the one which Command seemed to be looking for was presumably HX 229 rather than SC 122. It will be helpful to list the critical Allied and U/B dispatches in their chronological relation.

041704Z March: Original route for HX 229, sent in Nav. Cipher #3, "M".

1602Z/13 : HX 229 diverted; ordered to turn due east on reaching 49 N., 48 W. ("J"). Sent in Nav. Cipher #3, "M".

(The presence of U/B's across the original route between Newfoundland and Greenland was known.)

1214A/14 : RAUBGRAF ordered to form new line off Newfoundland for 15 March in expectation of a "northeastbound convoy".

(HX 229's original route would have bisected this line at about 50.30 N., 47 W.)

1847A/14 : Before RAUBGRAF could reform on the line for the 15th, it was suddenly ordered to head for area 49.40 N., 42.15 W. at high speed.

1920A/14 : RAUBGRAF line ordered for 1200A/15 from 51.15 N., 42.05 W. to 49.27 N., 40.55 W. "Get hold of eastbound convoy to which further groups can be detailed later."

It is difficult to account for RAUBGRAF's sudden shift without assuming compromise. Between the time of the order for the first RAUBGRAF line and the high speed heading (1214A to 1847A/14), 5 RAUBGRAF subs transmitted, two to give their positions and three to report land-based A/C. There was nothing in these reports which could have justified Command's conclusion that a NE convoy not yet sighted was turning into an E convoy. It was not until 2300A/14, more than four hours after RAUBGRAF's "diversion", that Command had anything like a sighting from a submarine. At that time Walkerling (U-91) reported having seen smoke clouds at 2030A in 49.57 N., 46.45 W., but he had been bombed and forced off by A/C before he could investigate. Walkerling remained close, for he made contact on a DD the following evening. It was Feiler (U-653) who finally established contact on the convoy itself on the morning of the 16th. Feiler had been detached from the group and was headed for a refueler off to the southeast. Meanwhile RAUBGRAF U/B's were going through several maneuvers involving such fine points as a 15 mile shift to the south, accompanied by such phrases as "The convoy must be found!" (0443/15). During this interim Command was consistently putting his successive reconnaissance lines a few miles too far north for BX 229. The lines would have caught SC 122 had that convoy not been several hours ahead of the line schedule. The possibility of a compromised dispatch to SC 122 can not be altogether excluded, for the heading point ordered at

~~TOP SECRET~~



1847A/14 actually lay between the routes of SC 122 and HK 229, but orders to U/B's showed no awareness of two convoys and U/B maneuvers pointed to HK 229. German uncertainty as to the precise location of the convoy and Command's failure to arrange his U/B's with requisite precision before Feiler's accidental contact probably indicate that Command did not possess a complete recovery of the HK 229 diversion dispatch. It should be noted that neither in the case of HK 229 nor in the case of ON 166 were the critical German messages sent in Offizier setting.

(b) Convoy TO-2.

On 15 March U/B's in the Trinidad area were informed by Offizier message of the expected arrival of a convoy (TO-2) at Trinidad on 21 March. The convoy's position as of 2000A/13 March was given along with three points on her ocean route. Her ETA was explained by the Germans as based on dead reckoning with a speed of 13 knots. This Offizier was read on 22 March and in a memorandum of that date the Atlantic Section called COMINCH's attention to it, stating that "the message gives an accurate description of the convoy's course ..." This judgment was not based on the convoy's dispatches, which were not available in 20-G but on the daily convoy position estimates of COM 10th Fleet C & R. When access to the convoy files had been gained later on, no dispatch could be found in TO-2's file which would have accounted for the 2000A/13 convoy position given in the German Offizier. The following correspondences, however, were found in MOIC Gibraltar's

Secret 2242A/10 March to USS Roper and Decatur: sent in Naval

Cipher #3, table "S":

NOIC Gibraltar

Point F: 18.05 N., 43.56 W.  
" G: 15.02 N., 51.55 W.  
" H: 11.30 N., 60.02 W.  
Speed of advance: 13 knots

German Offizier

"It is proceeding via  
18.09 N., 44.02 W.  
15.09 N., 52.03 W.  
11.33 N., 60.09 W." 13 knots  
(The above positions are the  
mid-points of German grid  
squares.)

It was later learned that GCACS traced the German Offizier to two Allied dispatches, one from F.O. Gibraltar on 10 March (2247A) and the other from FOC WAF on 13 March (1402), both in naval cipher #3, table "S". Neither of these dispatches was seen in the convoy files in C & R. Presumably the second of these dispatches contained the estimated position of the convoy for 2000A/13.

(c) Convoy UGS 6.

In February some 5 U/B's of the 740 ton class departed France under orders "Seewolf". Their heading point was deciphered as off Cape May, a decipherment soon confirmed by clarification from Control which resulted from an error by one of the U/B's. From area 42 N., 45 W. "Seewolf" U/B's were suddenly diverted to the southward where they intercepted UGS 6 on 13 March, west and a little south of Flores. That the above operation involved the compromise of UGS 6's ocean route seemed highly probable, but gaps in German traffic (noon 7 to noon 9 March and noon 11 to noon 12 March) made complete investigation impossible. Evidence tending to confirm compromise in this case turned up in January 1944, when Warbach (U-953)

was informed in Officer setting that "until March 1943, traffic proceeded to port ((Casablanca)) via DF 2196 ((34.03 N., 08.00W))". (1517/19 Jan. '44). Point "Z" on the ocean route for UGS 6 was 34.04 N., 08.01 W.

5.  
Compromise established,  
May 1943. Convoy HX 237.

The Atlantic Section's wall chart on 5 May showed Convoys HX 237 and SG 129 on a diversion route that would safely clear the south end of the long RHEIN-ELBE patrol line whose position off Flemish Cap had been accurately fixed by decryption. At this point the current reading of traffic stopped temporarily, but U/B contact seemed very unlikely. When B'B' short signals, with the group count known to be predominantly convoy sighting reports, were fixed by D/F the following afternoon in the convoy's path, it was clear that RHEIN-ELBE subs had made a rapid sweep to the southeast and had found the convoy, for there were no other U/B's in the general area at that time except the members of these groups. When the traffic became available, a few days later, attention was immediately concentrated on three Officer messages. Grammatical variations of the crib "Ein erwarteter Geleitzug" ("an expected convoy") were tried and the compromising information came out.

(a) Investigation of first Officer.

"2307/7

To: ((Groups) RHEIN and ELBE

---Offizier G---

An expected convoy was in LD 2684 ((BC 7684  
43.57 N. - 48.25 W.)) on 6 May 2330B. Precise course not known, but approximately eastward. Speed 9.3."

TOP-SECRET-ULTRA

A careful study was at once undertaken but for several days yielded no satisfactory result because the Atlantic Section had not received all the pertinent Allied dispatches. Not until access to COM 10th Fleet Convoy and Routing had been gained via COMINCH was it possible to find the source of compromise. The examination of the convoy files showed that German cryptanalysts had had a good depth with which to work, for the diversion of the convoys, complicated by a bad fog off Newfoundland Banks, had led to frequent exchanges of dispatches between shore authorities and the escorts - all in Naval Cipher #3, table "S". On May 7, for example, there were at least 6 transmissions from escorts (5 from G2 and 1 from W6). While there was no way of determining how many dispatches the Germans had read, the first Officer could be traced without question to

W6 Secret 062130Z to Cincema (in Nav. Cipher #3, table "S")

HX 237's position 43.56 N., 48.27 W., course 131, speed 9.5.

Allied dispatch

time: 2130Z  
43.56 N.  
48.27 W.

German Info.

2330B  
43.57 N. (mid point of  
48.25 W. Ger. grid square)

The Germans had apparently failed to make a complete recovery and remained in ignorance of the southerly diversion until the evening of 8 May.

(b) Investigation of second Officer.

~~TOP SECRET~~

"0025/9

To: Group RHEIN

---Offizier X---

The expected convoy, according to sure report, is further south and further ahead than assumed. A patrol line must therefore be drawn up by 2000B on 9 May extending from OG 2927 ((BD 7927-43.33 N. - 34.55 W.)) to VA 9154 ((GE 4154 - 39.45 N. - 35.02 W.)). Maintain radio silence."

Although there could be little doubt that the second Offizier derived its information from compromise, it was not possible to identify the specific Allied dispatch in question. It was clear that German Command had discovered the southerly diversion between 2051B and 2310B on 8 May, for at 2051 the failure of the U/B's to make contact had led to an order for a sweep on course 060 speed 8, thus indicating that a northerly route was deemed possible. At 2310B the order to sweep on course 060 was cancelled and U/B's were put on course 120 at top speed. U-359 (Forstner) made contact the following afternoon in 41 N., 37 W. Any one of several dispatches between CINCCHA and convoy escort, which resulted from difficulties in trying to change course, would have yielded the information, especially CINCCHA 060900Z to W6 and CINCCHA 061530Z to escorts, both in table "5".

(c) The third Offizier and the Straggler B/V.

"0952/11

---Offizier X---

To: ((Group)) DROSSEL

Eastbound Clausen convoy will be in Nav. Sq. 9552 ((44.21 N., 27.15 W.)) at 1600B May 11.

The Clausen referred to in the third Offizier was the C.O. of U-403. This U/B had regained contact on BX 237 the preceding day.

10 May, by following an obliging tug until it rejoined the convoy. The tug was the ship "Dexterous". It is mentioned here because "Dexterous" was in part responsible for the broadcast of Straggler R/V for the 11th that was sent to Group BROSSAL in the third Officer.

Allied (CINEMA Liverpool  
090901)

German Info.

R/V 1400Z/11 in  
44.22 N. - 27.20 W.

1600B/11 in 44.21 N. - 27.15 W.  
(mid point of German grid square)

Escort had informed CINEMA Liverpool that "Dexterous" had strayed and requested that she be informed of R/V positions, adding that what books she held was not known. CINEMA Liverpool broadcast the R/V positions in 090901, which was sent in Nav. Code #3, Aux. Vessel System SP 02358/44 and marked RAMS. It was assumed here that the message must have been repeated in Naval Cipher #3, as was the custom in such cases, but no such dispatch could be found in C & R. There were other puzzling points for which satisfactory explanations could not be obtained. (For British conclusions see Appendix to this chapter, case 4 under May '43.).

## 6.

Demonstration of Compromise  
accepted. Action taken.

The demonstration of Compromise was at once submitted to COMINCH. Meanwhile the British had arrived at the same conclusion and recommended certain precautions for the month of June until a new basic book (No. 5) could become effective. The insecurity of

naval cipher #3 was attributed to:

- (a) "compromise of portions of aviation base book due to heavy use over long periods.
- (b) overload of 'M' and 'S' tables in spite of 10 day change.
- (c) ease with which enemy can classify messages in naval cipher 3 due to distinctive combined call signs."

(Ref. Ultra personal for Admiral King from First Sea Lord 072250, 072255, 072302 June '43).

The proposed countermeasures consisted largely in weekly changes of "M" and "S" tables. In view of the continuing evidence of compromise, which increased markedly during this period, the interim cipher safeguards could not be accepted as satisfactory. In consequence Naval Cipher #5 was brought into effect on 10 June.

7.

More compromise - to 10 June 1943.

During May and the first 10 days of June 22 cases of compromise (confirmed or presumed) appeared in U/B traffic. Three of these cases are of particular interest to the U.S. Navy.

a) COMINCH U.S. SUB NOTICES:

Conf. 291613Z/May  
(in part)

"USS Herring on patrol within 20 miles of 54 N. 42 W. USS Haddock on patrol vicinity 51 N. - 35W."

GERMAN OFFIZIERS:

((Positions are converted from grid))

1531B/31 May:

"On evening of 29 May an American sub was on patrol within 20 miles from 53.57 N., 41.55 W. Another one in 50.57 N., 34.55 W. submerged by day, on surface at night."

COMMENT: While the last phrase in the Offizier did not appear in COMINCH, the Germans had presumably read it before and may have assumed that the last sentence in the sub notice, which they did not read, contained this ordinary and sensible conclusion. TIME INTERVAL: 45 hours.

Conf. 051606Z June:

1729B/8 June

"Hake on patrol vicinity 53.20 - 37.00. Haddo on patrol vicinity 51.00 - 35.00. Herring 54.41 - 28.48 submerged by day enroute 54.45 - 28.01. ETA 051800 thence to 54.01 - 22.02. ETA 061800 surfaced at discretion."

"American sub Hake on 5 June patrolling area of 53.21 N.- 37.05 W.; sub Haddo in 51.03 N.- 34.55 W."

2311B/8 June

"USA submarine Herring was 54.39 N, - 28.45 W. on 5 June; course not known, proceeding submerged by day."

COMMENT: TIME INTERVAL: 71 hours.

(b) Flight 10 (with note on GUS 7A).

COMINCH secret 211944Z May informed GESF, NOB Bermuda, and others in Naval Cipher #3 that 19 British LCI(L)'s were to sail about 24 May from Norfolk to Bermuda. NOB Bermuda was to direct from Bermuda to Gibraltar according to the ocean route which was given. In Offizier 1106B/24 May, German Command ordered 16 subs to leave their stations in the North Atlantic and head at once for area 35.15 N., - 42.05 W. The U/B's had to reach their destination by 2000B/31 May. An explanation was not forthcoming until 1832B/29 May:

1. Action is planned against West-East convoy expected in the patrol line from 1 June to 6 June. Speed 8 - 8.5.
2. Beginning 1 June an Eastbound convoy is expected approximately in area of Struckmeier's position consisting of storm landing boats of 250 tons and of their attendant tankers protected by escorts... No operation against this. Take advantage of opportunities for shots against valuable targets (tankers). Do not report when you sight this convoy..."

~~TOP SECRET~~



The West-East convoy was undoubtedly FLIGHT 10. The position of Struckmeier (U-608) should have been approximately 33 N. - 43 W., since he was the third man from the south end of the line (Group TRUTZ), which had been ordered on 26 May to run due north and south along the 43rd meridian from 39 to 32 N. It was to be occupied by 0800B/1 June. Position "H" for Flight 10 was given as 33.01 N. - 43.15 W. in the COMINCH dispatch referred to above.

Note on GUS 7A.

If it seemed peculiar for a long patrol line to expect a convoy at its southern end rather than at the middle, this oddity may have been explained on 1 June (1021B) when Group TRUTZ was informed by Offizier that:

"Beginning noon today, count also on Westbound convoy. When you sight it, operate on it."

The "westbound convoy", GUS 7A, would have passed through the northern half of the TRUTZ line, according to its original route as ordered in GMSF secret 240300Z May. Knowledge of this route would explain the peculiar formation of TRUTZ, as designed to catch two convoys at the same time, but would not account for the long delay in informing U/B's. GMSF 240300Z was not believed compromised, for it had been sent in ECM 35. The possibility of another source for compromise, however, could not be excluded, since at this time daily position reports were being sent in Naval Cipher #3 by various shore authorities.

8.

Comment: The enemy's own Ultra intelligence during U/B decline.

If one may judge from U/B traffic, German Ultra intelligence had never been better than it was just at that period when the decline in U/B fortunes became so evident. The increase in Ultra intelligence disseminated to U/B's during this period may and probably does represent a corresponding increase in the amount available. The way in which it was used, however, suggests a desperate and hurried attempt to give all possible information to the U/B's at sea. In trying to give his men an additional advantage, Command certainly disregarded security regulations - without compensation - for the risk he ran. In effect, he was sacrificing his best source of intelligence at a time when his fleet was incapable of using this intelligence. The last U/B group attempt in May to destroy an America-England convoy (Group MOSEL, HX 239) made use of a decrypted dispatch giving straggler R/V positions, yet the operation ended on 24 May in miserable failure. At least 6 U/B's were sunk, and Command had to stop the operation while the convoy was still in sight. As U/boat after U-boat was requested to "Report position at once" ("Standort sofort melden"), Command was trying to review the total situation in a series of long messages. He promised suitable changes in operational areas until such time as his boats could be provided with adequate protection against aircraft. It was just 12 hours later that he

ordered the southern heading to intercept Flight 10. German R.I. had surely influenced his choice of the Gibraltar lane as the place where he might find convoys less well defended. Our decryption of his plans, however, had led to the formation of the Bogue task group, which reached the Trutz patrol line before the convoys.

9.  
Compromise of Naval Cipher  
#5 feared. September 1943.

The dispersal of the U/B fleet during the summer of 1943, following the abandonment of Atlantic convoy lanes, made it impossible to judge how effective the introduction of Naval Cipher #5 had been, since German information on convoys could not be put to any immediate operational use. Instead of convoy intelligence, U/B's were receiving relays of Allied contact and attack reports. With September's resumption of the offensive against convoys attention was again directed to the intelligence which appeared in the timing and arrangement of the patrol lines as well as in "convoy expected" messages to U/B's. Group LEUTHEM was prepared for the initial attack with the familiar signs of convoy intelligence. In addition, two of LEUTHEM's 21 U/B's were equipped with intercept teams prepared to hear and D/F convoy voice traffic. At 1626B/16 September Comsubs sent the following to LEUTHEM:

- "1. Operation on westbound convoys only. Beginning 21 September, Convoy 'ONS' is expected; 23 September, Convoy 'ON'. Both westbound. Possibly late.

2. When sighting eastbound convoys, no operation, but take advantage of favorable chances to attack. Report only if sub is observed by enemy. After using attack opportunities, speediest return to position in patrol line."

The convoys were readily identified as ONS 18 and ON 202, which sailed 13 and 15 September respectively. The convoys were delayed, as the Germans had anticipated, and U/B's were kept informed of their progress. On the morning of 19 September U/B's were told to expect one of the westbound convoys "beginning today". ON 202 was attacked that night (200300Z). Inasmuch as the convoys had already been at sea for 4 and 6 days, it was necessary to account for <sup>the</sup> accuracy of revised German information. There were of course the possibilities of GAF reconnaissance and of D/F on unit transmissions, but the fact that convoy escort had reported to CINCNA twice on 16 September and once on 17 September in Naval Cipher #5 compelled the Atlantic Section to fear cipher compromise, especially since the dispatch of 17 September had been sent in the World Wide table ("M"). A detailed statement of the reasons for this fear was promptly submitted to COMINCH. The British, however, were not convinced in view of fact "that enemy at times possesses general picture of convoy cycles and nomenclature from various lowgrade sources including WTI". (GC&CS 191858 Sept. to 206).

10.

German awareness of standard  
convoy routes.

Quite apart from subsequent shifts in anticipation of

the convoys, LEUTHERN's original line lay across the standard route used by the majority of ON and ONS convoys since July. There was no reason to doubt that German Intelligence had been keeping accurate tab on North Atlantic convoys during the period of U/B inactivity and had an idea of the standard routes now being used. It might be noted that the standardization of convoy routes simplified the Atlantic Section's problem of deciphering the disguised German grid positions, for it had long been the practice to consult the convoy chart in the process of deducing disguised U/B heading points and lines, particularly in those cases which read "convoy expected".

11.

Evidence accumulates. SC 142  
and U-220.

After the first LEUTHERN operation U/B dispositions showed even more clearly that enemy coverage of convoy movements was reliable. On 22 September (1115B) a large minelaying-supply U/B, U-220 (Barber), was warned of an eastbound convoy (SC 142) in vicinity of 52 N., 33 W., an area through which most of the eastbound convoys had passed since July. Again, two dispatches sent on 17 September in table "S" could have accounted for the message to U-220.

12.

HX 257, ON 203. COMINCH communicates  
apprehension to First Sea Lord.

On 23 September LEUTHERN boats were informed that their next

operation would be against an eastbound convoy about 27 Sept. The convoy was HX 257. But on the following day plans were changed and U/B's were directed to proceed eastward at high speed to intercept what was clearly OH 203. This conduct was strongly reminiscent of the period when the Germans were known to have been reading the combined cipher. All the information necessary to account for the German activity could be found in dispatches sent in either the "M" or "S" tables. Hence, even though there was no definite proof of compromise, a detailed statement of the situation was again submitted to the appropriate authorities in Admiralty and to COMINCH, who communicated his apprehension to the First Sea Lord.

13.

Compromise of Naval Cipher #5  
confirmed. October 1943. HX 261.

On 19-20 October U/B's were en route from the mid-North Atlantic, where Group SCHLIEFFEN's operations had proved discouraging, to form a new line (Group SIEGFRIED) off Newfoundland. At 2239A/19 they received the following Officer:

"Eastbound convoy will be in Nav. Sq. AX 97 ((area 51 to 51.54 N., 29.30 to 31.00 W.)) at noon 20 October. No operation; count on strong A/C. Take advantage of chances that are offered."

The convoy, HX 261, had been diverted by CINCMA on 15 October in Table "M", the new route lying well to the south of both standard routes A and B. Of the messages from escort, sent in Table "S", G3's Secret 151659 to CINCMA was established by the

Atlantic Section as the source of German information.

03 Secret 151659 to Cincwa (Table "S")

"HX 261: request BAMS for  
noon R/V 19th: 50.18 - 35.35  
noon R/V 20th: 51.36 - 30.50."

That the Germans had not given the position as precisely as they might have was understandable, for no operation had been intended. GCACS concurred in the Atlantic Section's conclusion.

14.

SC 146 diversion compromised.  
November 1943.

By 7 November the last attempt to mass U/B's off Newfoundland was breaking up. U/B groups had been well informed on eastbound convoys but had been powerless before A/C. Forced to try more unorthodox tactics, Command formed Group EISENHART in an effort to escape Allied detection. As convoys SC 146 and HX 265 proceeded on a diversion course to the south of EISENHART's loose and sprawling arc, Command countered by moving EISENHART to the south and east, explaining on 12 November that:

"The shift in convoy routes which has occurred in the last few days necessitates a shift in your position." (1232/12).

and again on 14 November that,

"The persistent avoiding action of the convoys to the south makes another removal of the line necessary". (1113/14).

Late on the 14th (2300) U/B's received the following in Officer setting:

~~TOP-SECRET-ULTRA~~

- "1. Slow northeast bound convoy which is running approximately via Green IW 69, 5350, and Green AW 8610 is placed tonight by dead reckoning approximately in Green SP 48."

The correspondence between the German Offizier and the points contained in CINCCMA's diversion dispatch, sent in Table "M", could not have been mere coincidence.

CINCCMA Secr. 100606Z to Escorts SC 146 <u>New straggler's route</u>	Offizier <u>grid squares</u>
Point O: 46.22 N., 32.25 W.	45.36 N. to 46.30 N. 34.00 W. to 35.30 W.
Point P: 50.40 N., 25.40 W.	50.24 N. to 50.42 N. 25.30 W. to 26.00 W.
Point Q: 55.18 N., 17.10 W.	55.12 N. to 55.30 N. 17.00 W. to 17.30 W.

The new stragglers' route had been repeated in RAMS 100615Z, but past experience threw the weight of suspicion on CINCCMA's dispatch in table "M". Of CINCCMA's diversion, however, the Germans could have read only the last part, the part giving the stragglers' route, since their dead reckoning position for the convoy indicated that they did not know the diversion route of the convoy itself. Lack of agreement between Point "O" and its German counterpart was probably explained by a garbled German intercept copy or by a partial recovery. HX 265 had also been diverted by a dispatch in table "M". An Offizier sent to EISENHART on 15 November (2113/15) mentioned that "HX convoy steering NE is in the same area".



15.  
Indications of Combined Cipher  
Compromise cease in U/B traffic.

After KISENHART's attempt to operate on SC 146 no further cases of combined cipher compromise were seen in U/B traffic. If the German C.I. organization was having difficulties at home, for which, according to a JMA report, Italian betrayal was blamed, the U/B at sea was scarcely in a position to exploit convoy intelligence. U/B's had been told in October 1943 that locating convoys was the principal problem of the U/B war and that the solution of this problem was the U/B's own responsibility. To assist the U/B an effort was made to locate convoys by radio intercept teams on board, by relays of D/F fixes from shore, and finally by VL/B A/C. But instead of finding convoys, U/B's were being found by A/S forces, while the convoys proceeded more or less in peace. Whatever the cryptanalytic situation at home may have been, U/B traffic seemed barren of any high grade intelligence during the remainder of the war. Other than decodes of British low-grade traffic, of which there is no complete record here, U/B traffic carried only occasional decryption intelligence taken from merchant signals. (See Appendix A.)

APPENDIX A TO CHAPTER IV.

CASES OF  
PRESUMED AND CONFIRMED  
COMPROMISE  
of Allied Communications  
1943 - 1945

Listed below are German messages which are believed or are known to have contained information derived from decryption intelligence. The compromised Allied source (dispatch and system) is given where known. This list cannot be regarded as exhaustive even for U/B traffic, but it does include all cases suspected and examined for compromise by the Atlantic Section of 20-G. The list has been checked against British (GC & CS) investigations insofar as records of these investigations were available.

It will be noted that in nearly all cases the German messages were sent as OFFIZIER messages. That Ultra intelligence available to the Germans should have been disseminated in the cipher system reserved for matters of unusual importance and secrecy is natural enough, but the possibility remains that use may have been made of decryption intelligence in the normal or common U/B traffic. (The plain enigma system). Hence, in a few instances, messages of particular interest have been included in the list even though these messages were not sent as OFFIZIER.

~~TOP SECRET-ULTRA~~

NOTE ON COMPROMISE OF MERCHANT SIGNALS.

Members of the Italian Naval C.I. organization stated that Merchant signals were easily read and that there was no difficulty in obtaining a supply of documents from sunken ships. References to "Merchant Navy Code" appeared in JMA traffic in November 1942 when the German C.I. organization turned over photographic copies of the document to the Japanese, together with other relevant material. (See Chapter VI this volume, para. 6.) Little information, however, is available through U/B traffic on direct use of Merchant signals before 1944. Of the confirmed cases which appear at end of this Appendix, the case recorded for March 1944 aroused considerable anxiety, for the Allied dispatch involved contained a U/B estimate which was based on Ultra intelligence. (For a discussion of this point see Chapter VI this volume, para. 12).

GERMAN DISPATCH.

SOURCE.

DECEMBER, 1942

No OFFIZIER messages are available for this month. As a possible case of compromise the following is recorded:

1144/22/12

\*para. 3. Object: surrounding a convoy going southwest, which is expected on approximately the 23rd, RM 31 ((AL 31, area 53.15 N. - 22.45 W.))

No satisfactory accounting for this information could be found in Convoy & Routing files for this convoy, OH 154. The U/B's involved were Groups SPITZ and URGESTUM. The resulting operation was the most successful convoy operation in December.

JANUARY, 1943

1) 1108/7

OFFIZIER N

According to B-service it has been established that an English unit was detailed on 3 Jan. to patrol Neumann's ((U-117)) last provisioning area. Purpose may be: either to search for survivors (of sinking by Group Spitz), or to chase subs on the basis of D/F's from the numerous messages sent by Neumann's provisioning group, or both. Your attention is once more called to most extensive radio silence during provisioning... Avoid unnecessary transmitting.

British Naval Code, General Table Area 1 (X 1). Time lag 4 days. (Enemy Intell. Report #52.)

2) 2216/7

OFFIZIER L

To: Bruns ((U-175))

Occupy next the sector west-northwest of ET 38 ((Freetown)).

~~TOP-SECRET-ULTRA~~

Presumably convoys leave there for ED 99 ((Trinidad)) in a 10 to 11 day rhythm. Next departure possible on 8 January. Passage points of a December convoy were:  
ES 3696 ((08.51 N. - 19.57 W.))  
ER 1515 ((09.27 N. - 35.03 W.))  
EP 1352 ((10.09 N. - 50.03 W.))  
Another convoy on 17 December was in latitude of ET 38 ((08.15 N. - 13.10 W. 'B')), course 295, speed 8.

Precise source unknown.

3) 1349/9

OFFICER O

To: Group FALKE

English passenger ship 'Capetown Castle' from AK 8224 ((53.33 N. - 33.25 W.)) to AL 6134 ((56.15 N. - 19.25 W.)) will pass the line presumably on 9 January. You may leave position in line only upon sighting the ship.

Precise source unknown.

4) 1156/25

OFFICER S

From: Comsubs

To: Reeder ((U-214))

1. Tanker convoy route is suspected from LP 49 over IZ 22 and 89 as well as IO 37 and IX 9690.

2. Straggler route probably runs over naval squares 4770 and 6910 of the large square west of disguised square FF as well as over FF 05 eastward.

Precise source unknown.

((Interpretation of positions:

LP 49 is probably ED 99 - 10.55 N.-30.50 W.  
IZ 22 is probably DS 72 - 20.50 N.-34.45 W.  
IO 37 is probably DG 87 - 27.10 N.-30.05 W.  
IX 9690 is DR 4690 - 30.27 N. - 20.06 W.  
FF 05 is probably DS 55 - 22.40 N.-32.05 W.  
(DR) 4770 - 21.27 N.-44.03 W. squares west of  
FF-probably DS  
(DR) 6910 - 22.03 N. - 36.51 W.))

~~TOP SECRET~~

FEBRUARY, 1943

1) 2312/10

OFFIZIER I

From: Comsubs  
To: All subs on Series 1

Position of apparent attack area of an American U-Boat was square PF-5854 on 9 Feb. ((PF-5854, no information.))

Precise source unknown. This case was studied in some detail but without results. The Germans presumably had reference to one of U.S. Submarines based on Rosneath, Scotland (Squadron 50) and the position must have been one of 3 possibilities off W. France. The logs of USS Shad, Herring, Barb, and Blackfish were examined but gave no leads that could be followed.

2) 1754/14

OFFIZIER W

From: Comsubs  
To: All subs on Series 3.

Group ROCHEM including Luis ((U-504)) on 16 Feb. 1200A be in reconnaissance line from JH 8285 to SJ 7785. Course 285. Day's run 150 nautical miles. Sequence: Bargsten ((U-521)), Markworth ((U-66)), Becker ((U-218)), Schwandtke ((U-43)). Other boats in sequence in which they set out from Cuygan ((U-118)). Eastbound convoy is expected beginning 17 Feb. Another little patrol line will be north of AI 64 ((er: north of you in AI 64)). ((Interpretation of positions: JH 8285 is probably CE 8285 - 36.45 N.-30.06 W. SJ 7785 is probably DG 2785 - 32.15 N.-30.06 W. AI 64 is probably CE 64 - 38.50 N. - 27.40 W.))

Precise source unknown.  
Convoy UGS 5.

3) 1731/18

OFFIZIER M

From: Comsubs  
To: All subs on series 4

Steamer Coulgorm left Freetown 12 Feb. for Saldanha Bay. Passage points: 00 27, GH 9570. Speed 9. Naval squares ((00 27 = area 24.11 S. - 00.33 W. GH 9570 = 29.15 S. - 10.33 E.))

Precise source unknown.

4) 2322/18

From: Consubs  
To: Group NEPTUN

Last disposition order rescinded.  
On 20 Feb. 0000((A)) be in new  
patrol line from DE 7438 to 5269.  
Westbound convoy is expected on the  
20th.  
((DE 7438 = AK 2438 = 59.45 N.-30.24 W.  
DE 5269 = AK 0269 = 56.45 N.-30.12 W.))

2330/18

To: Group RITTER

Order for period up to now cancelled.  
On Feb. 20th at 0800((A)) be in patrol  
line from sq. IZ 5299 to UK 9423.  
Westbound convoy expected.  
((IZ 5299 = AK 0299 = 56.27 N.-30.12W.  
UK 9423 = AK 9423 = 52.45 N.-30.05W.))

2349/18

Oelrich ((U-92)), Hoeltring ((U-604)),  
Walkerling ((U-91)) and Zurnuehlen  
((U-600)) will form Group KNAPPEN and  
occupy on 20 Feb. 0000((A)) patrol line  
from XI 9293 to 9684. Westbound convoy  
is expected on the 20th. Turn on Diana  
19 Feb. 0800((A)).  
((XI 9293 = AK 9293 = 53.03 N.-28.05 W.  
9684 = AK 9684 = 52.03 N.-27.25 W.))

5) 2310/27

#### OFFIZIER N

From: Consubs  
To: Group ROCHEN

Operation with 6 boats including Rashh  
((U-106)) is intended, on a westbound  
slow convoy, from 2 March on, in area  
naval square 90 of the large square  
west of HL. On 26 Feb. 2000((A))  
convoy was in GB 9979, course about  
260, speed 8.

Convoy ON 166, which lost 15  
ships to RITTER-KNAPPEN. It  
will be noted that these  
changes in patrol lines were  
made in less than 1/2 hour. It  
is difficult to account for  
this sudden redistribution of  
submarines (they had been ex-  
pecting an Eastbound convoy,  
HX 226) without assuming some  
good last minute intelligence.  
First ON 166 diversion (CINCWA  
Secr. 10013/17) could account  
for U/B disposition. Like the  
other Allied traffic concerning  
this convoy, it was sent in  
Combined Cipher #3, table S.  
(See SA 13-C).

FOC Gibraltar's daily situation  
report, 2000/26 Feb., in Com-  
bined Cipher #3, table S Area 1.  
Time lag 1 day. (Enemy Intell.  
Report #52). This case  
illustrates difficulties of  
compromise investigations.

TOP-SECRET-ULTRA

((Nav. Sq. 90 is DF 90, area  
28.03 N. - 36.03 W.  
RL is DG  
CB 9977 is DH 4979 = 29.27 N.-  
20.45 W.))

FOG's Gibraltar's dispatch was not available in Convoy and Routing's files. COMNAVEU also sent a convoy situation report for 2000A/26 Feb. which included GUS 4 (COMNAVEU Secr. 261639 to all US Commands concerned with etc.) but it was sent in ECM. It was not thought that ECM had been compromised.

MARCH, 1943

1) 1304/10

OFFIZIER Y

Keller ((U-130))  
Henke ((U-515))  
Emmermann ((U-172))  
Rueggeberg ((U-513))  
Rasch ((U-106))  
Sturm ((U-167))

Be in positions at 1000((A))  
12 March in reconnaissance line from Nav. Sq. ((CD)) 8381 ((36.51 N.-39.50 W.)) of the large sq. west of disguised Sq. FX ((CE)) to Nav. Sq. ((CD)) 2221 ((42.51 N. - 41.02 W.)) of the large Sq. west of disguised Sq. VV ((CE)). Course 270, speed of advance 5 knots. Do not arrive earlier than ordered. Radio silence except for ((or, until)) tactically significant reports. East-bound convoy expected beginning 12 March.

2) 1847/14

To: RAUBGRAF

Discontinue operations. Head for Sq. UF 49 ((BC 34 = area of 49.40 N.-42.15 W.)) at high speed.

CONVOY UGS 6, from which 3 ships were sunk in the action which resulted from this message. A gap in German traffic makes complete investigation impossible but it is believed that compromise of a routing dispatch in combined cipher #3 was involved, especially since these U/B's were diverted from a planned operation ("Seewolf").

These messages concern U/B formations for Convoy HX 229. At the conclusion of the

~~TOP SECRET-ULTRA~~



1920/14

To: Group RAUBGRAF in the order  
Bertelsmann ((U-603))  
Kapitsky ((U-615))  
Zurwahlen ((U-600))  
Schamong ((U-468))  
Strelow ((U-435))  
Walkerling ((U-91))  
Manseck ((U-758))  
Graef ((U-664))  
Uphoff ((U-84))

Take positions at 1200((A)) 15  
March in patrol line from Sq. DI  
1383 ((AJ 9883 = 51.15 N. - 42.05 W.))  
to KR 5081 ((BC 3581 = 49.27 N. -  
40.55 W.)). Object: To get hold  
of eastbound convoy to which further  
groups can later also be detailed.

3) 1119/18

OFFIZIER S

From: Comsubs  
To: Trinidad Subs

Convoy with speed of 13 was in Nav.  
Sq. DI 6222 on 13 March at ~~2000~~((A))  
((23.57 N. - 21.15 W.)). It is  
proceeding via EG 1145 ((18.09 N. -  
44.03 W.)), EF 4176 ((15.09 N. -  
52.03 W.)) and EE 7476 ((11.33 N. -  
60.09 W.)), at which point--accord-  
ing to dead reckoning--it should  
arrive about 21 March.

4) 2005/20

OFFIZIER D

From: Comsubs  
To: All subs on Series 1

A convoy steering course of 250 to  
270 is expected to be in YH 3625  
at ~~0900~~((A)) 21 March. Pich ((U-168))

operation Ger. Command called  
it the "greatest success yet  
achieved against a convoy".  
Both the original route and  
the diversion route recommended  
by Adnty. were sent in #3 "M"  
(CESY Secret 041704Z and C & R  
Secret 131602Z). While  
neither message was in OFFIZIER  
setting, the circumstances  
lead one to presume that  
cipher compromise was involved.  
(See SA 13-B, case 2).

Combined Cipher #3, Table S.  
Convoy TO-2. GCGS recorded  
two dispatches as sources:  
F.O. Gibraltar and FOC WAF  
reports, 2247A/10/3 and 1402/13/3  
Time lag 9½ - 5 days. (Enemy  
Intell. Report #52). Another  
candidate would be NOIC  
Gibraltar's Secret 2242A/10/3  
to USS Roper and Decatur,  
time lag 7 days 12½ hours,  
although NOIC Gibraltar's dis-  
patch does not account for con-  
voy position as given for  
2000A/13 (See SA 13-B, case 2).

\*Almost certainly based on  
Special Intelligence, of which  
the precise source was not

is to be there at the time mentioned, and to wait a few hours. If convoy is not found, sweep on small sags for the courses mentioned. On sighting convoy, without attacking, shadow for group Seestuefel. ((YH 3625 probably AK 2125 - 60.45 N. - 32.45 W.)). ((Presume same message as T.O.O. 2022/20/3 reported in ZIP/ZGU/24)).

confirmed." (ZIP/ZGU/24).  
The convoy was probably ON 173.

APRIL, 1943

1) 2259/11

OFFIZIER I

From: Comsubs  
To: All subs on series 3

Position of English steamer "Mandalay" on 9 April was approximately Nav. Sq. FK 60 ((area 09.45 S. - 26.39 W.)) and it is proceeding over FK 3290 ((06.45 S. - 26.21 W.)) and FK 4310 ((00.27 S. - 17.57 W.))

Precise source unknown. (Enemy Intell. Report #52.) Original routing dispatch (BO Baires Conf. 272245 March) was sent in F.S.SHIPCON Argentina Area 1543/1544A. It is not known whether this info. was subsequently relayed in combined cipher. (SA 13-B, case 3).

2) 1909/12 (1902/12/4 acc. ZGU/24)

OFFIZIER F

From: Comsubs  
To: All subs on Series 3.

Southbound convoy will be in Nav. Sq. EK 4850 ((13.39 N. - 18.33 W.)) on 13 April ~~0800~~((B)), speed about 7.5.

Precise source not confirmed. (ZIP/ZGU/24) Convoy was probably OS 45. (SA-19).

3) 1315/15

OFFIZIER A

From: Comsubs  
To: All subs on Series 3

Presumably a floating dock on 3 April at 2200((B)) in Nav. Sq. EP 4879

Combined Cipher #3, Table M.  
From dispatches sent on 3 April

((05.09 N. - 51.09 W.)) speed 2.  
On 11 April at 2200((B)) in FB 1566  
((01.03 N. - 42.27 W.)), course 085,  
speed 4.5, apparently going to Freetown.

and on 10 April (2011Z).  
(Enemy Intell. Report #52).

MAY, 1943

1) 1432/3

OFFIZIER N

Southbound convoy going via Freetown  
was by dead reckoning in about EK  
4590 ((14.15 N. - 18.15 W.)) on 2  
May at 0800((B)), speed about 7.5.  
Probably floating dock on 3 April  
at 2200((B)) in EP 4879 ((05.09 N. -  
51.09 W. - vicinity French Guiana  
Coast)), speed 2, on 11 April at  
2200((B)) in FB 1566 ((01.03 N. -  
42.27 W.)), course 085, speed 4.5,  
probably for Freetown. With a  
speed of 3.5 can be expected there  
beginning 4 May. All Nav. Sq.

The convoy was probably  
OS 46. (SA 19).

2) 2307/7

OFFIZIER O

To: ((Groups)) RHEIN and ELBE

An expected convoy was in LD 2684  
((BG 7684 = 43.57 N. - 48.25 W.))  
on 6 May 2330. Precise course not  
known, but approximately eastward,  
speed 9.3.

Combined Cipher #3, Table S,  
p. 14, 1.5W6 Secret 062130Z to  
CINCPAC. Time lag 23 hours,  
28 min. Convoy EK 237.  
(SA 13, case 1).

3) 0025/9

OFFIZIER K

To: Group RHEIN

The expected convoy, according to sure  
report, is further south and further  
ahead than assumed. A patrol line  
must therefore be drawn up by  
2000((B)) on 9 May extending from  
OG 2927 ((BD 7927 = 43.33 N. - 34.55 W.))  
to VA 9154 ((GE 4154 = 39.45 N. -  
35.02 W.)). Maintain radio silence.

Could have come from any one  
of several dispatches sent  
between 5 and 8 May in  
Table "S". (Cf. SA 13, case 2).

~~TOP-SECRET-ULTRA~~

4) 0952/11

OFFIZIER I  
To: ((Group)) BROSSER

Eastbound Clausen ((U-403)) convoy  
will be in Nav. Sq. 9552 ((44.21 N. -  
27.15 W.)) at 1600((B)) May 11.

5) (The following is inserted on  
basis of GCACS Enemy Intell. Report  
#52, although there is no record of  
such a message here:

?/11 "Unidentified steamship in  
tow on 9/5 in 36.19 N. - 32.32 W.")

6) 2241/19

OFFIZIER M

"Sidney Star" left Montevideo 12 May  
for the Clyde via Nav. Sq. FX 4391  
((08.39 S. - 30.57 W.)) and DS 4212  
((15.51 N. - 36.03 W.)); will arrive  
((Clyde)) 1 June. Speed 14.5.

7) 1654/20

OFFIZIER V

1. Steamer left Rio May 11, via  
14 S. - 26 W., 01 S. - 15 W.  
Speed 9.5; due in Freetown May 24.
2. Steamer left Rio May 13 via  
14 S. - 26 W., 01 S. - 16 W., speed  
8.5; due in Freetown May 26.

CINWA Secr. 090901Z May in  
Brit. Nav. Code #3, Auxiliary  
Vessel system SP 02358/44.  
Time lag 2 days. (SA 13, case 3).  
ZIP/ZGU/24 states that Combined  
Cipher #3, table S, area 1, was  
the source. Enemy Intell.  
Report #52 lists a dispatch  
FOO 0901/9/5 in Aux. Table  
Area 1 (I) as source.  
Convoy BX 237.

Combined Cipher #3, Table S,  
area 1, from 1034B/9/5/43.  
Time lag 1 1/2 days.

Routing dispatch was RO  
Montevideo Conf. 112105Z May  
sent in HCM 61. Diversion dis-  
patch was C & R Conf. RAMS  
152056Z in Ship pad 539. Info.  
repeated in Combined Cipher #3?  
(SA 13, case 7) Precise source  
unknown. (Enemy Intell. Rept.  
#52).

Steamers were SS MARIJA  
PETRINOVIC and EMPIRE ARUND  
respectively. Routing dispatches  
Rio Conf. 112324 and 122352 May,  
both to Con route and both in  
HCM Mk.II. 1533B. Enemy Intell.  
Report #52 attributes German  
info. to dispatches of 11 and  
13 May (not identified) in  
Combined Cipher #3, table M.

~~TOP-SECRET-ULTRA~~

8) 2214/21

OFFIZIER H

To: Group MOSEL

The expected convoy was in square UW 7682 ((BC 2682 - 49.27 N. - 43.45 W.)) on 20 May 1700((B)). It is to be in Square OG 6148 ((BD 1148 = 50.27 N. - 38.15 W.)) on 21 May 1700((B)), and is to head from there for square IJ 3581 ((AK 8581 = 52.09 N. - 33.25 W.)) speed 9 - 9.5.

Combined Cipher #3, Table S, area 1. Straggler R/V positions, Convoy EK 239. GINGONA BAMS 201310 in Incom SP 02406 pad 332 only dispatch containing this info. in C & R files. (See SA 13, case 4) Enemy Intell. Report #52 lists 171449Z and 201224 in #3, S, as containing same info.

9) 1252/22

OFFIZIER I

Position of large convoy bound for Freetown was plotted 22 May 0800((B)) approximately Nav. Sq. EK 1335 ((17.33 N. 17.21 W.))

Precise source not confirmed. (ZIP/ZOU/24). Convoy was probably OS 47. (SA 19).

10) 1252/23

OFFIZIER Q

Aux. Cruiser "Bulolo" was in Nav. Sq. ES 1720 ((08.33 N. - 27.33 W.)) on 4 May, on 15 and 18 May an un-recognized English unit on patrol.

Precise source unknown.

11) 1106/24/191

OFFIZIER B

Johannsen ((U-569)), Rendtel ((U-641)), Christophersen ((U-228)), Baltz ((U-603)), Bruening ((U-642)), Hunger ((U-336)), Kreck ((U-558)), Nagel ((U-666)), Hause ((U-211)), Strackmeier ((U-608)), Trojer ((U-221)), Marbach ((U-953)), Presel ((U-951)), Ziehm ((U-232)), Strelow ((U-435)), Reichenbach ((U-217)) head at once for Nav. Sq. 87 of the large Sq. west of TT ((area of GD 87 - 35.15 N. - 42.05 W.)). Square must be reached by May 31, 2000((B)).

Combined Cipher #3. COMING 211944Z to GESP and NOB Bermuda. Time lag 61 hrs. 22 mins. Flight 10. (SA 13, case 10).

Subs arriving with less than 50 cbm are to report posit and fuel on hand at once.

1832/29

OFFIZIER SOPHIE

To: Group TRUTZ

1. Action is planned against west-east convoy, expected in the ((patrol)) line from 1 June to 6 June. Speed 8 - 8.5.

2. Beginning 1 June, an eastbound convoy is expected approximately in area of Struckmeier's ((U-608)) position\* consisting of their attendant tankers protected by escorts...

\* Approx. 33 N. - 43 W.

12) 2032/27

OFFIZIER P

An American sub was in AK 5445 ((55.03 N., 35.15 W.)) on 24 May at 2100((B)) proceeding to its patrol area near AK 7657 ((52.15 N. - 36.25 W.)). Another American sub was on patrol on the 24th at 2100((B)) near AK 7182 ((53.03 N. - 39.15 W.)). Both subs are submerged during the day. All Nav. sq.

Combined Cipher #3. Table S, area 1. COMINCH Conf. 241705Z. US Submarine Notice. Time lag 3 days. (SA 13, case 6).

13) 1905/29

OFFIZIER C

A straggler from an eastbound convoy is proceeding over following positions: Nav. Sq. AJ 9355 ((53.15 N. - 40.45 W.)), AK 1895 ((55.27 N. - 34.00 W.))

Combined Cipher #3, Table M. CINCWA 272014Z (repeated in Admty. Liverpool 272015Z RAMS). Time lag 44 hrs., 50 mins. (See SA 13, case 5). Convoy HK 240.

14) 1456/30

**OFFICER W**

On 28 May English steamer "Lombardy" received order to deviate from present course and to head, via 03.25 S. 31.42 W., for 06.26 W. - 31.28 W.

Combined Cipher #3, Table M1  
Diversion, C & R RANS Conf.  
281502Z, was sent in OUTCON 434.  
GC & CS assumes this msg. must  
have been reenciphered in #3,  
M table, for Brazilian area.  
(Sa 13, case 9); Enemy Intell.  
Report #52.)

15) 1531/31

**OFFICER D**

On evening of 29 May an American sub was on patrol within 20 miles from Nav. Sq. AJ 6891 ((53.57 N. - 41.55 W.)) another one in Nav. Sq. ED 1321 ((50.57 N. - 34.55 W.)) submerged by day, on surface at night.

Combined Cipher #3, Table S.  
COMINCH Conf. 291613Z US sub  
notice. Time lag 45 hours,  
18 min. (SA 13, case 8).

16) 1917/31

**OFFICER X**

Position 31 May 0800 of convoy running to the South Atlantic by way of Freetown, was, according to dead reckoning, Nav. Sq. HK 7995 ((10.39 N. - 17.21 W.)) speed about 9.

Probably from Combined Cipher #3, table M, but not confirmed. (Enemy Intell. Report #54). Convoy was probably WS 30. (Sa 19).

**JUNE, 1941**

1) 1021/1

**OFFICER N**

To: Group TRUTZ

From today noon on, count also on westbound convoy when you sight it, operate on it.

Possibly from daily situation report in Combined Cipher #3. Convoy was GUS 7A, whose original route was sent in ECM 38 (CMSP Secret 240300Z). (See SA 13, case 10).

2) 1102/7

OFFIZIER I

According to dead reckoning, convoy bound for Freetown was approximately in Nav. Sq. BT 2640 ((09.09 N. - 15.15 W.)) at 0500 7 June.

Precise source not confirmed. (ZIP/ZGU/24). Convoy was probably OS 48. (SA 19).

3) 2159/7

OFFIZIER D

To: Kamecke ((U-119))

((Results)) so far: The British steamer "Alva", 1584 tons, has run into your minefield and sunk.

Combined Cipher #3, Table 8. CINCCMA Conf. 032323Z. Time lag 92½ hours. (SA 13-1, case 2).

4) 1202/8

OFFIZIER S

English passenger ship "Orion" on 5 June in Nav. Sq. GZ 7971 ((45.47 S. - 06.34 E.)), enroute from Durban to Freetown, ETA 13 June; speed about 20. A second steamer proceeding from Durban to Lagos; ETA 16 June; speed about 15.

Precise source unknown.

5) 1211/8

OFFIZIER W

From: Comsubs  
To: All subs on Series 4

On 5 June a convoy coming from Durban is expected in Capetown. Unknown steamer from Durban to Buenos Aires was in Nav. Sq. GR 5633 ((33.39 S. - 18.26 E.)) on 5 June 2200. Days run 156 miles.

Precise source unknown.

6) 1729/8

OFFIZIER F

American sub "Hake" on 5 June patrolling area of Nav. Sq. AX 7263

Combined Cipher #3, Table 8. Cominch Conf. 051606Z US sub Notice. Time lag 71½ hours. (SA 13-1, case 1).



((53.21 N. - 37.05 W.)); sub  
"Haddo" in Nav. Sq. 8787 ((51.03 N. -  
34.55 W.)).

2311/8

**OFFICER X**

U.S.A. submarine "Herring" was in Nav.  
Sq. AK 6588 ((54.39 N. - 28.45 W.))  
on 5 June; course not known; pre-  
ceding submerged by day.

Same. Time lag 77 hours.

7) 1557/10

**OFFICER W**

To: Kamecke ((U-119))

Steamer "Highland Count", Tonnage  
unknown, sunk in about Nav. Sq.  
MB 7583 ((44.03 N. - 63.05 W.)).  
? Presumably ran into your minefield.

No record of ship HIGHLAND  
COUNT. If error for SS HALMA,  
then probably from Combined  
Cipher #3, table S. NSHQ  
Conf. 040335Z to Admty.,  
info. GINGCHA and COMINCH.

.....

Combined Naval Cipher #5 introduced on  
10 June, 1943.

.....

8) 1319/25 (June)

**OFFICER D**

To: Staats ((U-508))

Four steamers received instructions  
on 10 to 14 June to proceed via Nav.  
Sq. FF 5138 ((00.33 S. - 08.21 W.))

Source unknown.  
(XIP/207252, Appendix III)

SEPTEMBER, 1943

1) 1946/1

**OFFICER Y**

To: Zimmermacher ((U-107))

The following American declared area  
has been announced: Sea area between  
37.08 N. and 37.38 N., 74.48 W. east-  
wards to the 200 meter line.

This case was investigated  
with the assistance of COMINCH  
but precise source was not  
found.

2) 1626/16

OFFIZIER P  
To: Group LEUTHEN

1. Operation on westbound convoys only from 21 Sept. on, convoy "ONS" is expected, from 23 September on, convoy "ON". Both westbound. Possibly late....

(Following the LEUTHEN operation on Convoys ONS 18 and ON 202, U/3 Command continued throughout Sept. and early October to arrange his groups on basis of convoy intelligence. These messages were not in OFFIZIER settings. They are too numerous to quote but are listed here for reference:

1115/22/9 to Barber ((U-220)), giving info. on eastbound convoy (80 142).

2336/23/9 to LEUTHEN, indicating plans for operation against eastbound convoy (NK 257).

1457/24/9, plans changed, operation to be against westbound convoy (ON 203)

1645/24/9 formation of ROSSBACH (for ON 203 operation)

1102/25/9 to ROSSBACH, concerning delay in convoy arrival.

1701/26/9 to ROSSBACH, further on convoy speeds & HFA. (ONS 19 now added).

2054/27/9 to ROSSBACH  
2055/28/9 to ROSSBACH  
2232/1/10 to ROSSBACH ).

Convoys ONS 18, ON 202.  
This German message led to reopening of compromise question with British, in view of convoy dispatches in Combined Cipher #5, table M. British concluded compromise of #5 not involved in this case.

Each of these cases was checked carefully. Although the results did not show clear signs of compromise, COMINCH and ADMTY. were currently informed of the fears which continued to be entertained. British believed German Convoy Intelligence could be accounted for by traffic analysis and low grade sources.

OCTOBER, 1943

1) 1855/2

OFFIZIER 3

To: Group ROSSBACH

1. You may definitely count on the arrival in patrol line of GNS convoy on or before 3 October; and on the arrival of ON convoy beginning 3 October. Hence continue sharp lookout.

2. Cautious enemy comments on the 'LEUTHER Convoy' confirm that the enemy has been dealt a telling blow.

As above.

Convoys were GNS 19 and ON 204.

2) 1742/8

OFFIZIER 2

To: Schrewe ((U-537))

8 October at noon, west bound convoy in AL 37 ((area 57.45 N. - 18.25 W.)); 9 October in AL 15 ((area of 58.40 N. - 25.35 W.)).  
Nav. Sq.

Source unknown.

Convoy was ON 205.

3) 2239/19

OFFIZIER 2

Eastbound convoy will be in FAX 97 ((51.27 N. - 30.15 W. 'B')) at noon 20 October. No operation; count on strong A/C. Take advantage of chances that are offered.

Combined Cipher #5, table 8.

Convoy HK 261.

G3 Sec. 181659 to CINCPAC.

Time lag 28 hours, 41 min.

(SA 13-5, case 1.

SCCS concurred.

4) 1205/22

OFFIZIER 2

1. Hangerhausen ((U-91)), Kille ((U-762)), Wenzel ((U-231)), Mahrholz ((U-309)), Struckmeyer ((U-608)), Dobbert ((U-969)), Witzendorff ((U-267)), Von Davidson ((U-281)), Peal ((U-413)), Roddenberg ((U-963)), Lanby ((U-437)),

Precise source unknown.

Convoy was HK 261.

~~TOP SECRET-ULTRA~~

Reich ((U-426)), Heller ((U-842)), Popp ((U-552)), Jaschke ((U-592)), Boehmer ((U-575)), Gaenge ((U-226), Von Lehsten ((U-373)), and Weber ((U-709)), will make up group SIEGFRIED, and will take positions in patrol line in this order on 24 October at 1200((A)) from Sq. Green TC 1928 ((probably AJ 9928 = 51.39 N.-40.45 W.)) to Sq. Green YY 5938 ((probably BG 3938 = 48.57 N. - 38.45 W.)).

2. Eastbound convoy is expected beginning 24 October, evening.
3. More will follow.

NOVEMBER, 1943

1) 2300/15

OFFIZIER I

To: Group EISENHART

1) Slow northeast bound convoy which is running approximately via Sq. green IV 69 ((area of BD 49 = 45.08 N.-34.45 W.)), 5350 ((BD 3350 = 50.33 N.-25.45 W.)) and Green AM 8610 ((AL 6610 = 55.21 N. - 17.15 W.)) is placed tonight by dead reckoning approximately in Green SP 45 ((BD 25 = 48.45 N.-31.45 W.)).

Combined Cipher #5, Table N. Partial recovery of CINCMA's diversion dispatch Secur. 100606Z to Escorts. Convoy SG 146. (SA 13-6, case 1).

2113/15

OFFIZIER II

To: Group EISENHART

2. Convoy referred to in Offizier msg. of 14 Nov. ((2300/14, quoted in part above)) is probably further south than has been assumed. Escorting A/C were located at noon today approximately in Green SP 02 ((BD 82, area of 45.09 N. - 31.45 W.)) and 03 ((BD 83, area of 45.09 N. - 30.15 W.)). Course of the convoy from this square apparently to Green LZ 91 ((AM 71, area of 53.15 N.-15.15 W.)). EK convoy steering NE is in the same area.

The EK convoy was EK 265. EK 265's diversion had also been sent in #5, "M". As far as known, however, this OFFIZIER did not involve further compromise. (SA 13-6, case 1).

MARCH, 1944

1) 1839/30

To: Herwartz ((U-843)).

Report upon crossing latitude  
of Sq. blue AB 88 ((#FS 38:  
area of 16.03 S. - 18.33 W.))

1. Fuel
2. Position at 1300A/30/3.
3. If, when, and where you were  
observed by enemy before that date.

APRIL, 1944

1) 2213/22

OFFICER H

To: Haenert ((U-550)) and  
Wittenberg ((U-856)).

Convoy and independents are  
travelling via Green Sq. NY  
8922 ((#CA 3922: 41.03 N. -  
68.30 W.)), then 8379 ((3379:  
42.03 N. - 68.46 W.)). Today  
they are in about green Sq. FQ 93  
((#CB 43: area of 39.45 N. - 64.54 W.  
'B')). Speed about 9.

AUGUST, 1944

1) 1802/10

OFFICER B

B-report: on 8/8 Commandant  
American Eastern Sea Frontier ordered  
8 allied merchant-ships to set  
navigation lights at night.

2) 1949/24

OFFICER X

Allied merchant shipping was warned  
on 15/8 of an obstruction in approx.  
#AB 7764 ((43.21 N. - 64.25 W.)).  
Our assumption: torpedoed steamer.  
If this is correct, U/B concerned  
report when opportunity occurs.

SP 2272/29.

Com 4th Fleet 291843Z RAMS  
to BYDS 2141, BYMS 221.  
(SA 13-10).

"Enemy submarine estimate for  
301200Z 1 southbound eastern  
half of area 01 degrees north  
25 degrees west."

SP 2388/682.

GESF 211941Z RAMS.  
(SA 13-11)

Time lag: 24 hours.

SP 2272/31.

GESF 082019Z. RAMS 2a  
Time lag, 44 hours.  
(SA 13-14 and Supplement).

SP 2272/32.

Adm. Halifax. Conf. RAMS  
151330Z.  
(SA 13-14).

~~TOP SECRET - U.S. EYE~~

SEPTEMBER, 1944

1) 2021/2

OFFIZIER F

On 1/9 Commander American Eastern Sea Frontier sent to 4 independents the order to proceed direct from 79.20 W. to Cape Cod Canal, then via Long Island Sound to Port of Destination, New York.

SP 2272/31.  
CESF Conf. 010511 to 3  
Brit. ships.  
Time lag, 37 hrs., 10 mins.  
(SA 13-14).

JANUARY, 1945

1) 2326/19

OFFIZIER M

Outbound convoy was to be in Nav. Sq. AM 9496 ((52.03 N. - 05.35 W.)) at 2200 today.

2) 1816/20

OFFIZIER I

According to B-report, R/V for stragglers of outbound convoy is at 2000/20/1 in Nav. Sq. XP 1257 ((50.27 N. - 09.25 W.)).

Precise source unknown.  
No reply received from British in answer to 20-G's query.  
Convoy probably OS 105/KMS 79.

COMPROMISE OF CSP 953.

Case of the Blockade Runner "Rio Grande",  
sunk by TF 41, 4 January, 1944.

On 8 - 9 December, 1943, Blockade Runners received the following instructions in "Alle" messages 60, 61, and 62.

"1. A/C or warships challenge merchantmen with 2 letters which change daily. Answer consists of 3-flag signal and international call sign. 3-flag signal changes about every 5 days. Details of changes not known for either call or answer. 3-flag signal also possible by blinker. A/C to be shown name plate outside of bridge. In connection with R/S exchange the ports of departure and of destination and dates are frequently requested.

2. Since there are no available data on secret call-signs (2-letter challenge, 3-flag signal answer) it is of course possible for the blockade-runners to imitate 2nd part of R/S procedure, however, the secret 3-flag signal must be intentionally hoisted in an unclear manner to be illegible. The challenge ~~NEJ~~ used up to now by warships is no longer practised, although it has not yet been officially recalled.

3. Use international call signs of assigned cover-ship. In case scuttling is unavoidable, when transmitting distress signal use enemy secret call sign assigned by W/T."

When the Rio Grande was intercepted she attempted to send an RRRR distress signal on 500 kcs., using the encoded call sign of the SS James Lykes. The suspicion of CSP 953's compromise which was voiced by Com 4th Fleet was confirmed by the Atlantic Section. An examination of CSP 953 indicated that the Germans must have had a rather old edition of this publication, for the challenge procedure ~~NEJ~~ was discontinued 1 November, 1942.

~~TOP SECRET ULTRA~~

APPENDIX B to CHAPTER IV.

CONFIRMED CASES OF ALLIED CIPHER COMPROMISE  
IN 1942. (This info. from GCCS Enemy Intell.  
Report #52, dated 18/6/43).

Nav. Cipher #3

<u>Allied Msg.</u>	<u>Contents</u>	<u>Ger. Ref.</u>	<u>System</u>	<u>Time Lag</u>
1121/8/7/42	Movements of Am. Merahips in N. Atl.	29/7/42	#3 "X"	20 days
0957A/20/9/42	Sinking of Norv. freighter "Olav Fortenes" in 45.50 N. 42.00 W.	24/9/42	#3 "X"	4 days
1802Z/21/9/42	Survivors of sinking of "Olav Fortenes"	24/9/42	#3 "S"	2 days
1753Z/5/10/42	Departure of Dutch S/M "L-15" from Freetown	13/10/42	#3 "X"	7 days
1135/7/10/42	from Freetown Edo. Departure of unit, prob. N.E.	20/10/42	#3 "X"	12 days
1758/11/12/42	N.A.S. attack against Bone, (Ital. & German foreknowledge of)	18/12/42	#3 "S"	7 days

Br. Nav. Cipher #4

1941A/12/8/42	Sinking of HMS Cairo	Captured document (Ital.)	#4 "C"	?
0949/15/8/42	Formation of Convoy A.P. 1	29/8/42	#4 "C"	14 days
1242/16/8/42	Unit from Kilindini via Simondstown to England	30/8/42	#4 "C"	13 days

TOP-SECRET-ULTRA



<u>Allied Msg.</u>	<u>Contents</u>	<u>Ger. Ref.</u>	<u>System</u>	<u>Time Lag</u>
0506/22/9/42	English S/S Haresfield overdue in Indian Ocean	?	#4 (A3)	14 days
0958/25/10/42	MCSO Capetown to Admty. ? quoted by Japanese on 1/12		#4 (A3)	37 days
0641/7/11/42	Eng. Transport left Archangel 7/11	13/11	#4 (A1)	6 days
2120/23/11/42	English S/M left Malta 25/11 for A/S duties CJ 7195	3/12 (also by Ital.)	#4 (C#)	10 days

British Naval Code

1359A/23/10/42	Br. trawlers on fixed patrol. Orkneys-Shetlands-Faroes-Iceland area	28/10/42	(X 1)	4 days
----------------	---	----------	-------	--------

Auxiliary Table Area 1 (I 1)

2330/11/11/42	Br. Warships (2) in area north of Petsamo	15/11/42		4 days
1/19/11/42	Br. "Bramhan" arriving Philippeville	3/12/42		14 days
1302A/26/11/42	Br. A/S trawler recv. info. on mines in area Melilla	2/12		6 days

~~TOP-SECRET-ULTRA~~

CHAPTER V

"B-DIENST" ON BOARD U-BOATS

.....

Table of Contents

1. U/B radio intercept teams, Fall, 1943.
2. Previous Warning in U/B Traffic.
3. U/B D/F Equipment.
4. Warning from Traffic of Beginning of U/B D/F on 2410 kcs.
5. U-664 (Graef).
6. Renewal of No. Atlantic Battle, Sept. - Nov., 1943.
7. LEUTHEM's Success, ONS 15 - ON 202.
8. ROSSBACH's Failure.
9. Comsubs turns to U/B Radio Intercept Teams.
10. B-Group performed well in SCHLIEFEN Operation, although attack failed.
11. Examination of U/B Command's Analysis.
12. Allied Precautions.
13. Allied Deception.
14. Special L/R air scouts for Convoy location, November, 1943.
15. Subsequent use of B-Dienst on board.
16. Standing War Order Comsubs Nr. 256 (captured document).

Chap.  
V

"B-Dienst" ON BOARD U-BOATS

1.

U-Boat Radio Intercept  
Teams, Fall 1943.

With the resumption of the North Atlantic convoy offensive in September, 1943, U/B's made a serious attempt to exploit convoy and A/C voice transmissions by means of B-Dienst personnel trained to take bearings on voice traffic (2410 kcs., 124.5 meters) and to correlate the plain language and codewords used in convoy communications. This activity came as no surprise to the Atlantic Section, for German interest in and experiments with U/B interception on 2410 kcs. were well advertised in past U/B traffic. For many details, including shore training and personnel, the Atlantic Section was indebted to OP 16 Z's interrogations of a B-Dienst party captured in August, 1943, (ex-U-664). During these interrogations, OP 16 Z frequently consulted the CO Atlantic Section. The results were made available just at the time when the German Navy was making its most concerted effort to home on convoys by intercepts at sea.

2.

Previous warning in  
U/B Traffic.

The first known instance of convoy voice interception by a U/B occurred in some of the earliest current traffic read by

TOP-SECRET-ULTRA

the Atlantic Section in December, 1942. U/B Group Panzer was expecting a north-east convoy (HX-217) by 5 December some 300 miles north of Flemish Cap. At about midnight on the 4th Steinaecker (U-524), a member of the group, reported hearing an English transmission on 124.5 meters in 51.27 N. - 47.35 W. Whether or not the shift in patrol line ordered two hours later was due to Steinaecker's report is not known. Steinaecker made first contact on the convoy at noon on the 6th. Nothing further on voice interception was seen until April, 1943, when four U/B's in Group Meise reported voice interceptions and signal strengths. Group Meise was patrolling the area north of Flemish Cap in anticipation of SC 126 and HX 233. It was evident that Comsubs sought to overcome the bad fog and weather conditions of 15-17 April and to establish contact by means of voice interceptions. The attempt failed completely. Convoys SC 126 and HX 233 were diverted far to the south of Meise, whose members apparently were intercepting transmissions from ONS 3 without realizing that they had the wrong convoy. A study of this operation was submitted to Cominch on 21 April with the conclusion that U/B's were not yet able to take bearings on a frequency as high as 2410 but might be in the near future.\*

\*This conclusion did not wholly agree with British findings, which interpreted the above operation as "indication of direction finding being used on this frequency wave (2410)".

3.  
U/B D/F Equipment.

2410 kcs is in the medium frequency band (300-3000 kcs). U/B beacon signals fell in the lower part of the M/F band and it was reasonable to assume that U/B D/F equipment would be extended to include the upper reaches of M/F, although the reliance on signal strengths for estimating the convoy's distance precluded such equipment in the Meise case. There is no indication that U/B's were ever able to take bearings on H/F (above 3000 kcs). The known development of U/B D/Fing went in the other direction with an attempt early in 1944 to take bearings on VL/F transmitters (VL/F = below 30 kcs), including those on the U.S. Coast, for navigation purposes.

4.  
Warning from traffic  
of beginning of U/B  
D/F on 2410 kcs.

Early in August 1943, it was discovered from traffic that eight code-groups were being added to the U/B Short Signal book for reporting bearings and signal strengths on convoy voice transmissions. A few days later U-664 was sunk, and B-Dienst personnel became available for interrogations.

5.  
U-664 (Graef).

According to P/W, an operator named Dobberstein left

~~TOP SECRET~~

St. Andries, the C.I. training station, in April 1943, for Brest, where he was assigned to U-664. While there is no trace of intercept activity in the traffic covering U-664's penultimate cruise, the period (May 1943) would fit in nicely with the known progression of German experiments on convoy voice interception. U-664 left Brest late in April and took part in Group Donau's unsuccessful attempt in May on Convoys SC 130 and EK 239. For U-664's final cruise there is again no record in traffic read of a functioning B-Dienst unit. There is, however, the interesting message (1936/16 August) which ordered U-664 not to use her SADIR receiver under any circumstances. Flotillas were also instructed to remove the equipment from U/B's being outfitted with it. The interrogation reports established that SADIR was part of the B-Dienst equipment aboard U-664, as well as standard equipment for intercepting A/C signals by shore B-Dienst stations. Special operators with such receivers as SADIR were probably to assist the U/B in its unequal struggle with the carrier task groups. While there is no certainty as to Command's plans for U-664's last cruise, it is interesting to note that Graef received orders (1909/25 July) to cruise out with Wilamowitz, a supply sub (U-459), sunk while outbound. Their destination was apparently the general refueling station west of the Azores.

Graef's association with Wilamowitz may have been accidental and is subject to other explanations, but it does suggest that Command was trying a new method for protecting his tankers. In both June and July refuelers (U-118 and U-457) had been sunk in their R/V areas by A/C from carrier task groups, and at the time of U-459's departure Command warned that a carrier force was in outer Biscay. In view of the recognized inadequacy of German Search Receivers during the summer of 1943 and the lack of any replacement at that time, it is reasonable to suppose that Command would have taken some extra precaution with his dwindling supply subs and have drawn on B-Dienst personnel and equipment to intercept A/C traffic for warning purposes.\* The Germans had temporarily abandoned convoy operations and hence had no opportunity to carry on with plans for intercepting convoy traffic for group attacks.

6.

Renewal of No. Atlantic  
Battle, Sept.-Nov., 1943.

From the reopening of the North Atlantic convoy battle in September to the withdrawal of the last patrol line from the Newfoundland area in November, seven large groups operated. The first three, Leuthen, Rossbach, and Schlieffen, were each provided with two B-Dienst U/Boats suitably disposed in line for

\*It is presumed that SADIR was withdrawn because of reradiation, the same trouble which afflicted GSR and led to so many changes in GSR policy and apparatus. It is worth mentioning here that in October, 1943, the Germans introduced A/A subs as protection for U-tankers.

taking cross bearings. The last four, SIEGFRIED, KOEHNER-JAHN, TIRPITZ, and EISENHART, had only one, Poel (U-413).

7.  
LEITHEM's Success,  
ONS 18, ON 202.

When Comsubs hailed Group LEITHEM on 23 September for its vindication of the U/B arm and its "proof of the new weapons" (2056/23/9), the B-Dienst groups were presumably congratulated along with everyone else. No preceding convoy operation had combined so many aids for the commanding officer. In addition to the acoustic torpedo, improved GSR, radar, radar counter-devices, and new tactics, B-Service not only followed the operation against ONS 18 and ON 202 very closely from shore, but also furnished information on the spot.

8.  
ROSSRACH's Failure.

Enthusiasm was short lived, for the next three west-bound convoys, ON 203, 204, and ONS 19, all slipped around the north end of the ROSSRACH line. Contacts had been made but the risks involved in transmitting to Control had discouraged U/B captains. Comsubs' reaction came quickly in the form of a Current Order (#4, 1035/1137/6/10). The location of the convoy was the "chief problem of the U/B warfare" and the responsibility rested on the U/B's themselves. Short signals for sighting

TOP SECRET-ULTRA



reports were to be held ready for immediate transmission. Not even the slightest hint of the convoy's whereabouts might be withheld from Control.

9.  
Comsub: turns to U/B  
radio intercept teams.

Despite assistance of German L/R reconnaissance A/C and shore D/F, Rossbach failed again with SC 143. On 11 October the B-Group in U-584 (Deecke) was requested to report its experiences, presumably as part of Command's attempt to analyze the failures and determine whether or not full use was being made of shipboard intercept possibilities. U-584's report was substantial and fairly detailed. Voice frequency had been heard over a radius of 200 miles. Convoy diversions had been detected. Information on the number of A/C's, the period of their coverage, and their radio frequency, as well as the general disposition of escort groups was submitted. Before the next operation began, Group Schlieffen's attention was especially called to the importance of voice interception. U-413 (Poel) and U-631 (Krueger) were singled out by name, for they were the two with B-men on board. (1150/15, 1852/16). The above sequence suggests that U/B operational Command was slower than Allied C.I. in attributing major importance to German intercept teams, for, in addition to emphasizing the need for caution in convoy and carrier voice transmissions, the Atlantic Section was at this time calling Cominch's

attention to the possibility of deception which could be practiced by B-parties with voice transmitters.

10.

B-Group performed well in Schlieffen operation, although attack failed.

Group Schlieffen's operation against ONS 20 and ON 206, 16-18 October, marked the climax of German efforts with B-Dienst in the Atlantic. A premature sighting of ON 206 confused the beginning of the attack, for Comsub apparently assumed the convoy to be ONS 20, the one he seemed to know more about. The B-Dienst U/B's were called upon to clarify the situation, but Comsub's initial confusion continued to show up in his misinterpretation of their data. The sinking of Krueger on the night of the 16th placed the full burden of B-Service on Peel's U/B. A careful analysis of the operation indicated, however, that Peel's group performed well and that the operation's failure was due in part to faulty correlation of information at home. Command did make use of Peel's bearings in directing the attack but could not form a clear picture from the various types of reports which all U/B's submitted. At a critical moment, for example, there was considerable hesitation in trying to decide between a radio bearing reported by Peel and a conflicting hydrophone bearing sent in by Hungershausen (U-91). After the operation had been

TOP-SECRET-ULTRA

discontinued, Poel's B-men were requested to report. Somewhat on the defensive, they explained that through lack of experience they could not always distinguish immediately between convoy and remote escort groups. On the 20th Comsubs summarized the problem as follows:

"Wrong data concerning location of convoy have originated in at least some cases from the circumstance that during a convoy operation subs have taken medium frequency bearings on A/C or escort groups which are at a distance from the convoy. As long as subs are far from convoy, a bearing on escort groups is a valuable clue to the convoy's position (for example, noon of the 16th). During sweep and pursuit, on the other hand (noon of the 17th), bearings on remote groups are misleading. In the future, therefore, when reporting bearings, report also the object on which bearings are taken, insofar as this is known. Procedure regulations will follow." 0716/20.

11.

Examination of U/B Command's  
Analysis.

Poel's bearing, noon 16th, had been an accurate one on ON 206, then approximately 190 miles NNE of U-413 and on a diversion course to the NW. It was disregarded in disposition orders, apparently because it did not agree with preceding sighting reports which had been correlated with ONS 20's plot, and it was thus probably interpreted as coming from a remote escort group. About noon of the 17th, Poel reported a radio bearing of approximately  $10^{\circ}$  T and, from the same position, Hungershausen reported hydrophone bearings of  $170-250^{\circ}$  T. Comsubs did not attempt a clarification for five hours. It is believed here that

both U/B's were probably right but that Poel's bearing was on ONS 20, then about to alter from a NW to a SW course, and that Hungershausen had heard stragglers or rear escort of ON 206, then clearing the infested area on a SW course. When Comsub's clarification finally came, it rejected Hungershausen's evidence altogether. Using Peel's bearings Command drew the wrong conclusion and sent his boats on a sweep to the NW. Meanwhile Convoy ONS 20 was cutting in behind the U/B's on a SW course. Comsub's consistent exclusion of ON 206 from consideration, despite his general awareness that the convoy would be in that area, was probably a major factor in the failure.

12.  
Allied Precautions.

Although the U/B arm failed to reestablish itself in the open Atlantic during the group operations of October, 1943, the threat of radio intercept parties was appreciated and efforts were increased to deprive the enemy of any support he might derive from this source in the struggle for advantage. Cinclant disseminated warnings to Atlantic forces and CINCPAC sent instructions and defined states or degrees of radio silence to be enjoined according to the situation. Early in November EINCWA reported two cases in which U/B's "used R/T in apparent effort to obtain D/F bearing of reply. Correct convoy call sign and phonetic alphabet employed". (Comnavop Secret 051651 November, 1943).

Operators were warned "against answering transmissions made with incorrect procedure or with foreign accents". Other cases of presumed deception by U/B intercept parties were reported, but no one of them was ever confirmed by Atlantic U/B traffic.

13.  
Allied Deception.

The Allies, on the other hand, did practise deception as a counter-measure. As early as 2 November CINCWA drew up a proposal for detaching a group or single ship to simulate convoy R/T traffic. In mid-December, an attempt was made to carry out this counter-measure for the confusion of Group Coronel, then in area 55 N. - 25 W.

14.  
Special L/R air scouts for  
convoy location, November,  
1943.

Following the failures of October and early November, Comsubs announced on 13 November, 1943, that, effective at once, reliance would be placed on special L/R air scouts (JU-290) for the location of convoys and the homing of U/B's. U/B groups were drawn in from the mid-Atlantic and concentrated in the Western approaches within the range of GAF reconnaissance. No blame could attach itself to B-Dienst on board, for the difficulties of U/B operations were too fundamental to be overcome by a device

which was tried on a limited scale and which at best pre-supposed some degree of mobility for the U/B. On the occasion of this general shift in tactics, Comsubs gave the standard explanation to his men:

"Founded assumption is that enemy air reconnaissance, using location methods which in part we have not yet been able to pick up, has contacted our line arrangements and has gone around us."  
(1903/13/11/43).

15.

Subsequent use of B-Dienst  
on Board.

The U/B radio intercept project seems gradually to have been abandoned, at least in the Atlantic, for as U/B groups came in closer to the convoy gathering and dispersing points radio bearings were more often confusing than not. Certainly Comsubs paid more attention to the reconnaissance A/C. A few U/B's on inshore operations around the British Isles continued to carry B-groups. One of these, Albrecht (U-386), claimed that R/T interception\* warned him of an impending search for his boat during an operation off North Ireland in January 1944. During 1944, U/B radio interception was confined largely to Arctic waters, where in fact it is still being used to a considerable extent.

\*Some R/T interception by U/B's could have been on VH/F (above 30 mcs) since this equipment (LO 1<sup>st</sup> UK 39) was reintroduced for operational cruises during the winter of 1943-1944. During the remainder of the war, shipboard interception was largely confined to Arctic waters.

~~TOP SECRET-ULTRA~~

16.  
Standing War Order Comsubs  
No. 256 (captured document).

Standing War Order No. 256, "Observation of Enemy Convoy Voice Traffic", was issued in October, 1943. It warned U/B operators that they must distinguish between ground and sky waves, disregarding the latter, and that they must make certain of the bearing's sense by checking with several bearings before reporting. (Poel's group did report one reciprocal bearing in the Schlieffen operation but it came after the operation had already fizzled). German equipment was said to D/F ground waves accurately over a range of 50 to 100 km. The digest on convoy communications procedure included types of traffic and originators, together with methods for identifying the convoy and originators and methods for determining the sea area, direction, and speed of the convoy. 52 codewords were listed with convoy designators and call letters of the radio guard ships. Of the 101 convoys identified with codewords there were 3 GUS, 4 UGS, 4 FT, 4 TF, 1 TH, and 2 HT convoys. Although St. W.O. #256 contained nothing of a startling nature it bore adequate witness to the care with which German Communications people had worked on voice interception. Had the German Navy been able to master the overall problems of a mid-Atlantic U/B offensive, it is probable that St. W.O. 256 would have been a modest introduction to U/B radio interception at sea rather than an unintended, final summary.

CHAPTER VI.

GERMAN-JAPANESE COOPERATION IN  
COMMUNICATION INTELLIGENCE.

\*\*\*\*\*

Table of Contents

Chap.  
VI

1. Introduction: Little evidence of effective exchange.
2. Early proposals, 1942. German successes with British systems to be exchanged for Japanese assistance with USN systems.
3. Tokyo's silence.
4. The Joint Communications Agreement.
5. German C.I. relayed to Tokyo via GHA, Aug. - Sept., 1942.
6. Cipher Material for Shipment to Japan, November, 1942. Indication of German Progress, November 1942. Merchant signals.
7. Neglect of "Clause 7" and the JMA's Complaint of December 1943.
8. Possible Explanation of Neglect Clause 7 in 1943.
9. Cooperation, 1944.
10. An Exchange on Crypto-problem, May 1944.
11. The Situation in General Combined Intelligence, May 1944.
12. Weakness of German Intelligence, Summer 1944.
13. Concrete Liaison July, 1944. Description of German Cryptanalytic Activity.
14. German Requests.

~~TOP SECRET U.S. EYES ONLY~~



15. Japanese Compliance.
16. The JMA's Plans and Instructions. Japanese Proposals.
17. Contents of Material (Traffic Analysis) offered by Germany in 1944. Very similar to that offered in 1942.
18. Material requested by Tokio via dispatch.
19. Critical situation, Fall 1944.

GERMAN-JAPANESE COOPERATION IN  
COMMUNICATION INTELLIGENCE.

(Based on info. available as of 8 Dec. '44).

1.

Introduction: Little evidence  
of effective exchange.

While information on German-Japanese cooperation in C.I. is still incomplete, it seems evident that effective exchange has never been established, despite the endeavors of the Japanese Naval Attache and the apparent willingness of the German Navy to share its material. On the whole the past history of German-Japanese cooperation in C.I. seems to be an account of professions and intentions, without any evidence of combined efforts in attacking high grade naval ciphers or of an exchange of ultra information from such ciphers. The Germans have talked darkly about their successes with such ciphers but there is no record here that the Japanese have even done that much. This conclusion is based largely on the earlier Japanese-Naval Attache traffic which became available in 1944, and on the few days of German Naval Attache traffic which have been read for 1942 - 1943.\* The more recent dispatches of the Ger. Nav. Att. (including the Offisier messages) which have been read since the fall of 1944 lack any reference to joint cryptanalytic work. The summary given immediately below lists only those identifiable

\* See note at end of Chapter.

items which have been mentioned in available traffic as either exchanged or ready for exchange, but does not list the "operational intelligence" reports which have been seen in increasing numbers since the summer of 1944. Some of these may contain elements from C.I., as indeed was claimed for a German report of December, 1943 (see para. 7 below), but it is not possible to give a detailed derivation for them.

Germany to Japan Exchanges.

(a) EAHS intercepts (Indian Ocean).

Via dispatch to GHA, Tokio. Instances available from 1942, 1943, and 1944.

Comment: Presumably passed for correlation with Axis submarine activity in Indian Ocean. German information on current locations of Jap subs was apparently very limited, at least prior to establishment of U/B base at Penang. In July, 1943, for example, JHA stated that German Navy had many R.I. reports of M/V's sending out submarine warnings in Arabian Sea, Oman Bay, and off the coast of Aden. The Germans presumed this was due to Japanese submarines and asked the JHA to check. At this very time the German Monsoon U/B's were departing Western France for Indian Ocean operations and the establishment of the base at Penang.

(b) General information on British D/F via JHA dispatch, July, 1944.

Comment: Germany recognized the "amazing progress" which England had made. Radio transmissions of over 10 seconds were certain

to be D/F'd with effective and reliable results in Indian Ocean as well as in Atlantic. It is interesting to note that in another dispatch of the same day (10 July) the JNA accounted for the loss of the Satsuki #2 as follows: "... she was first located by D/F..."

(c) Traffic Analysis.

British Naval frequencies ) ready for ship-  
British call signs and call sign ) sent, Nov. 1942.  
construction.

The same with addition of similar ) To be shipped  
information on U.S.N. and outline ) August, 1944.  
of joint British and American ) Not sent.  
Naval Communications. )  
(principally for Atlantic and Med. )  
This material was requested by ) Sent by dispatch  
dispatch in view of transportation ) fall, 1944 (?).  
difficulties. )

(d) Captured Documents.

"Merchant Navy Code" ) Included in material  
 ) ready in November, 1942.

(e) Merchant signal Recoveries, 1942. ) Included in material  
 ) ready in November, 1942  
 ) with promise to include  
 ) any subsequent recoveries.

(f) Presumably from decryption, exact source not known.

Via dispatch to GHA, 9 September, 1942. M/V movements;  
Allied escort E/V (?) in Indian Ocean.

Japan to Germany Exchanges.

(a) BAMS intercepts.

Via GHA. 1944.

(b) Allied A/S A/C Reports (?)

Via GHA. One instance known, July, 1944, and this may have been a RAMS. There was also the Operation Transom deception message which the Japanese reported on request.

(c) Allied submarine positions and ship movements.

(Sources not given but D/P is presumably one source). The submarine positions have been seen in increasing quantities in German Far Eastern communications with growing U/B activity in Japanese waters.

(d) Decryption.

Via GHA dispatch 26 October, 1944. Only instance seen here. Japanese C.I. deciphered a message 'from New Delhi to agents (probably in Penang) containing request for information on German U/B armament and speeds'.

2.

Early proposals, 1942.  
German successes with British systems to be exchanged for Japanese assistance with USN systems.

As early as January, 1942, the JNA was reporting very favorably on German progress in decryption and was urging joint research in cryptanalytical work. He was confident that the Germans would solve the problem, "even though they have troubles in the methods to be used in attacking the fundamentals". There was also a "change" which would "give some trouble in breaking the systems", but the Germans had already achieved some finished results. "They have been working at it very cleverly and have recently broken into the English Navy systems with some success, and have gotten some clues to

~~SECRET~~ ULTRA

solving the US Navy systems." Lacking adequate data on USN systems, the Germans hoped to meet this need through joint research with the Japanese. The JNA proposed that intercepts of what the Japanese regarded as the principal USN systems . . . be forwarded via the ONA to Germany, where "the Germans will endeavor to break them". It is clear that the JNA approved of the proposal, at least as a temporary measure, "although you ((Tokyo)) may be considering other plans..."

3.  
Tokyo's silence.

The reply from Tokyo is not available. If any was sent at all, it was surely non-committal, for in April, 1942, the JNA brought the subject up again. It was apparently necessary to remind Tokyo that "The cryptanalytic section of the German Navy is organized on an extremely large scale, and seems to be obtaining fairly good results". For the third time Tokyo was informed that the Germans desired cooperative investigations, "from the standpoint of joint operations", and were willing to turn over their decryption methods, "especially those on USN systems". The JNA had planned to assign a Lt. Comdr. Mishina to joint work with the Germans in these matters but this officer had been transferred and no qualified person was now available. The Attache respectfully inquired of his

superiors whether they might be disposed to send a specialist on the submarine which was about to leave for Germany, (presumably I-30). It is unlikely that the I-30 carried such a specialist to Europe, but on her return trip to the Orient she did carry secret documents and a shipment of German enigma cipher machines, some of which were unloaded in Singapore before the sub struck a mine and sank.

4.  
The Joint Communications  
Agreement.

In June, 1942, Vice-Admiral Nomura reported the clauses of the "German-Japanese Naval War Communication Agreement" which had just been concluded with Vice Admiral Maertens, then Chief of German Naval Communications. The 7th clause provided that:

"The Japanese and German Navies will collaborate in regard to radio intelligence."

5.  
German C.I. relayed to  
Tokyo via GHA, Aug. -  
Sept., 1942.

The few days of German Naval Attache traffic which have been read for 1942 suggest that Germany made a show of compliance with "Clause 7". The German Naval Attache received

intercepts of U/B sightings broadcast (BANS) for the Indian Ocean area, and on 9 September he received what appeared to be results of German decryption, giving the movements, passage points, and speeds of the following ships in the Indian Ocean: "Helen Moller", "Catrine", "British Sovereign", USA transports "Gremer" and "Maatsuyker" (sic), and the Australian "Manunda". In addition, the GHA was informed that at 0600/5 September an Allied unit was to relieve another unit in 23.15 S. - 90.10 E., (about 1440 miles N.W. of Perth). The above items bore "B" serial numbers and were probably taken from the current German C.I. Bulletins. It is unfortunate that evidence available is not sufficient for judging the extent of German C.I. information which reached the GHA in the above manner.

6.

Cipher Material for Shipment to Japan, Nov., 1942. Indication of German Progress, Nov., 1942. Merchant signals.

A message of 26 November, 1942, from the JMA stated that in response to Tokyo's request the Germans had turned over certain material on the British Merchant shipping code and had promised to "organize any recoveries made hereafter and deliver them by the time the submarine is ready to leave."

(\*The submarines referred to may have been one of the German submarines which sailed for the Indian Ocean early in 1943, either U-180 which departed Kiel, 8 February, 1943 to R/V with the I-29 in April, or the U-511 which departed Lorient 10 May, 1943, carrying Adm. Nomura home.)



Matters urgently needed by the Japanese were to be forwarded by dispatch upon request.

Contents of the material then available:

- (a) 200 pages of British Naval frequencies and call-signs of every sort, including main points of call-sign construction, "but apparently practically no specific call signs for vessels are included".
- (b) "Merchant Navy Code".

The Germans held an original of the document itself and were supplying photographic copies to the Japanese. (This publication was the earlier form of Mersigs). The British had changed the key words and the substitution table on 15 March, 1942, but the basic code appeared to be the same and the Germans were gradually accumulating the number of messages needed to recover the new key words and substitution table. As of November, they had recovered only about 20 of the new key word groups.

7.  
Neglect of "Clause 7"  
and the JMA's Complaint  
of December, 1943.

The JMA traffic for 1943 which has been seen in the

Atlantic Section is singularly lacking in any references to the project for cooperation in radio intelligence. It is evident from the JNA's complaint in December, 1943, that the whole business had fallen into neglect, at least as far as Japanese assistance was concerned. To what extent the Germans had continued to send cryptographic material is not known,\* but they had at least given the Japanese some operational information gained from radio intelligence, for it was an instance of this that occasioned the JNA's complaint. German radio intelligence had warned Japan via the Ger. Nav. Att. in Tokyo that the Americans were preparing to challenge the increasing activity of Japanese ships and convoys in the northern New Guinea area. The situation was compared to that which immediately preceded the Battle of the Solomons. The JNA shared the German fear that a sudden change was imminent and introduced his plea for cooperation by pointing out the obvious: "If, at this time we could learn the plans of the enemy or the movements of his vessels, it would help us considerably in planning our own operations." The Germans, he declared, fully appreciated the importance of crypto-intelligence, but, although doing their best with limited personnel, they were handicapped by lack of material. "By mutual

\*There seems to have been at least one exchange in 1943. See para. 16 below.

exchange of material between the Japanese and German navies, it is hoped that there will be a gradual development of crypt-analytical intelligence. Even when it is difficult to get concrete decrypted material, analyses should be possible." The Germans had evidently put the JNA in an embarrassing position, if one may judge from the following paragraph which summarized his own reactions:

"With regard to our cooperating in this matter, although it was our intention to exchange information frequently, these exchanges have been reports on the general war situation. At a time when one feels more than ever the necessity for mutual alliance and cooperation between Germany and Japan, the best plan for Japan is not to change the obligations set forth in the communications agreement. It is an important matter from the point of view of joint operations. In addition to considering this matter anew, I humbly urge that we do all we can to realize cooperation in this matter. (Where nothing else is possible, we can at least exchange information about this problem)."

A further statement is ambiguous, but seems to imply that the JNA recognized how little material of operational value the Germans could actually furnish the Imperial Navy at that time. \*\*

5.  
Possible explanation of  
Neglect Clause 7 in 1943.

In view of Germany's initial determination not to share her technical advancements with the Japanese, notably the T-V acoustic torpedo, it is quite possible that she had not been

\*\* See Note at end of Chapter.

completely honest with Japan in matters of radio intelligence. It will have been noted that the material being prepared for shipment to Japan in November, 1942, did not include Naval ciphers or codes, at least no mention was made of anything but Merchant Ship Code. Yet the British recorded cases in 1942 of German success with Naval cypher #3. (The source of British information was not U/B traffic.) Certainly U/B traffic up to the summer of 1943 showed an impressive total of German decryptions in Naval Cipher #3, and some success with Naval cipher #5 was obtained in the fall of 1943. It is conceivable that the Germans might have shown these to the JNA and have convinced them that they were of operational value to the Germans only, but it seems more likely that for security reasons the Germans kept these things to themselves and did not press for cooperation until things began to go badly for them. Such an explanation could, of course, work equally well from Tokyo to Berlin and mean that the reluctance of the Japanese to share with the Germans was based on reasons of security. Certainly the professions of mutual aid revived and became increasingly vigorous as Axis fortunes waned in 1944.

9.  
Cooperation, 1944.

The first actual statement from Tokyo on C.I. cooperation ever seen in the Atlantic Section bore the date 3 February, 1944.

~~TOP SECRET U.S. EYES ONLY~~

"With regard to Japanese-German Naval collaboration in the matter of radio-intelligence, we intend to make it our policy henceforth to cooperate in as positive a manner as possible; but the situation at present is that as yet little of the material we have on hand is worth offering to the Germans. At present, every time special information that seems important is derived from radio-intelligence reports, it is communicated to the German Attache in Tokyo...."

(Remainder of this message was not intercepted.)

As far as is known here, and especially subsequent to 3 February, this cooperation has been largely confined to the relay of submarine sighting and attack reports in the Indian Ocean and to the relay of Allied submarine locations in East Indian waters. While information is admittedly scant, the following case from May 1944 may be characteristic of actual German-Japanese cooperation.

10.

An Exchange on Crypto-  
problem, May 1944.

On 16 May 1944, the Germans intercepted an A/C sighting report of a naval task force which had been relayed by Colombo, and sought to exploit it with the assistance of the Japanese cryptanalysts.

18 May: German Navy requested via JNA any information which could be used in connection with the intercept.

25 May: Tokyo replied but could not help. The Japanese had likewise picked up the sighting report. They

assumed that the A/C had mistaken an Allied for an enemy task force, although it was also deemed possible that the report had been a deception message.

Comment: The sighting report was part of a deception plan for Operation "Trancon" and was sent in self-evident code.

11.

The situation in general combined Intelligence, May, 1944.

Meanwhile, on 20 May, the JNA raised the whole subject of general combined intelligence, and in so doing provided the following summary of the situation as of that date.

- (a) The Japanese maintained liaison in operational intelligence.
- (b) "German Navy and Air Force are now offering the Intelligence reports that had not previously been given to the Japanese."
- (c) The Germans were "having trouble getting current intelligence and the operations sections of all the services pay close attention to the Japanese intelligence reports".
- (d) The Japanese had, however, sent little useful information and the Germans were dissatisfied. Germany did not understand why Japan did not furnish special material.

for example, from prisoners of war and from their  
Attache in Russia.

(e) Tokyo was requested to send weekly:

"Our intelligence reports."  
"Lessons learned in air and naval battles with the  
English and Americans."  
"Weekly War Reports" from the Navy.  
The Japanese Army weekly war reports were already  
being received.

12.  
Weakness of German  
Intelligence, Summer, 1944.

That the Germans were having trouble in getting current intelligence late in May, 1944, was well demonstrated by the Allied Landings in Normandy and the subsequent campaign. According to the reports which the JNA and Ambassador Oshima were receiving from German Headquarters and relaying to Tokyo, the Germans were not only surprised by the landing but continuously and grossly underestimated the number of troops which gathered in Normandy during June and July. At the time of the breakthrough at St. Lo, the Japanese representatives in Germany were informed that "Patton's Army" was still in England, whence he had threatened an invasion of Dieppe throughout July.

13.  
Concrete Liaison July,  
1944. Description of  
German Cryptanalytic  
Activity.

~~TOP SECRET~~

Following a very friendly interview with Rear Admiral Stummel, Chief of Naval Communications, the JNA declared on 10 July that he had begun concrete liaison with the head of Naval Communications Intelligence, who at once agreed to place Japanese in the German C.I. organization. Furthermore, the Germans would make up a shipment of all types of C.I. material now on hand for forwarding on the Japanese submarine which was soon to reach Lorient. Meanwhile, however, it was requested that the Japanese indicate just what problems were of especial interest to them. During this visit the JNA learned the following about the German organization:

Two main sections: Evaluation  
Cryptanalysis  
Total personnel: about 800

German difficulties were blamed on Italy's betrayal, which had increased Allied security measures.

"English and American countermeasures are very vigilant (secure), especially since Italy's 'Stab in the back' of last year when the communications intelligence situation was realized by the enemy." At present, although they are bending every effort, the results are not satisfactory. It is said that this is especially true where American communications are concerned."

14.  
German Requests.

The Germans in turn made certain demands upon the Japanese, of which the last is somewhat surprising:



- (a) "All types of British and American material, including captured documents."
- (b) "Absolutely all available information on the dispositions of the British and American Fleets."
- (c) "They would also like to have the forms of all types of Japanese Naval traffic so that they can distinguish them from British and American traffic."

15.  
Japanese Compliance.

Tokyo complied with this last request on 26 July sending a brief description of "the external forms of Japanese Naval Communications" in terms of the different types of call-signs and the different types of textual grouping.

16.  
The JNA's Plans and  
Instructions. Japanese Proposals.

As part of his immediate program for cooperation the JNA planned to assign his special secretary to duty with the German organization, "after the code-clerk on the Momi arrives". Before going further, however, he apparently wanted "to know as soon as possible the views and desires of the central authorities concerning this matter". The Momi (I-52) with its code-clerk never made port, but the central authorities did communicate their views.

Two and one half years after the first known discussions of Clause 7 the JNA was being told that "We desire that you negotiate as fully as possible with the Germans in this matter". The Japanese proposed the following steps:

- (a) The assignment of Japanese research specialists to the German organization, in order to effect technical liaison. Four to be sent from Japan by next submarine transport, two reserve officers and two non-coms, prepared to stay in Germany for approximately one year. In the interim qualified special clerks now attached to the JNA's office will be assigned.
- (b) "If occasion warrants", German specialists to be employed in joint research in Japan.
- (c) Exchange of Material:
  - (i) Material offered by the Germans to be sent on the Homi's return trip.
  - (ii) Material offered by the Japanese to be sent by German vessel or by next Japanese cargo submarine.
  - (iii) "For the immediate present we will exchange material gathered since the last time (August of last year)."

Comment: If the above statement means a mutual exchange, it may refer to the I-8 ("Flieder") which arrived West France

late in August, 1943, and to the U-511 (Satsuki #1, Ro-500) which reached Japanese waters in August. It is not known here that these submarines did carry such material. There are no known departures of submarines in either direction during the month of August which might fit the above.

17.

Contents of Material (Traffic Analysis) offered by Germany in 1944. Very similar to that offered in 1942.

On 25 August, 1944, the JNA reported that he had received the material which had been destined for the Momi's return trip and that he would forward it by the next appropriate transportation.\* The Imperial Navy could judge from the list of contents what was of immediate necessity, extracts of which could be sent by dispatch.

Contents:

- (a) British Navy: Call-signs (shore stations, ships, convoys), frequencies, communication circuits, areas, abbreviations, British and American merchant ship call signs, outline of British and American Naval (joint) communications.
- (b) American Navy: As above. Also "American Army field radio cipher machine (it cannot be heard by ear)".

\*The large consignment (70) of German enigma machines and all non-crypto material destined for the I-52 were destroyed at Lorient in September.

The above material applied principally to the Atlantic and Mediterranean areas; information on Indian and Pacific Ocean areas was not abundant.

18.

Material requested by  
Tokio via dispatch.

On 31 August Tokyo requested that the following be sent by dispatch:

- (a) On the British: Call signs for ships and escorted convoys and the basis of their deduction. Various types of abbreviations. Outline of communications used between the British and American Navies, including call signs, code identification, frequencies, procedure, etc.
- (b) On the American Navy: Structure of the "XU numeral-letter" call sign system, and period of its use. Basic material necessary for traffic analysis. (i.e. Material which has appeared in the past where there has been a connection between operations and communications conditions.

19.

Critical situation,  
Fall, 1944.

One assumes that efforts toward cooperation have increased

since the summer of 1944 with the dangerous situations in which both Germany and Japan find themselves. It is evident, however, that the situation itself tends to defeat these efforts, for exchange other than by dispatch has been practically impossible. The report of an interview between Vice Adm. Abe and Admiral Meisel on 30 October sounds characteristic of the Axis plight. Adm. Meisel pointed out that:

"It is extremely important to Germany, fighting a defensive battle, to fix the time and place of enemy attacks. Especially at this time, when there is a great possibility of enemy landings in Norway, the Germans are uncertain as to the place selected."

"In view of the brilliant successes of the Japanese Navy" in repelling the October thrusts of the U.S. Navy, Admiral Meisel asked whether the Japanese had used special long range reconnaissance planes "or did it have any other special help?" "Other special help" surely includes C.I. Vice Admiral Abe replied diplomatically and referred the matter of "lessons gained from the battle" to Tokyo.

The persistent "shelving" by the Japanese of German requests for information which was of the utmost importance as the situation became more desperate, and their long-standing neglect of Clause 7 had begotten a similar attitude on the part of the Germans by March of this year. Vice Adm. Abe urged Tokyo to release more operational information and estimates of enemy plans together with Japanese counterplans. He complained that the lack of such information was making effective liaison virtually impossible, that conferences with

German officials were difficult to arrange and when arranged, he received the same "diplomatic" treatment which it had formerly been his habit to administer.

By comparison with the German attitude indicated above there is some inconsistency in the message to the German Naval Attache, transmitted the day before the JMA's report to Tokyo. The consent contained therein for the formation of a German Armed Forces communication intelligence liaison with the Japanese General Staff may have been inspired by the hope that more practical results could be obtained by cooperation in Japan than via the existing communication system.

H.B.

The following additional information was made available through traffic read subsequent to the writing of this chapter.

\* A report from the German Naval Attache in September 1942 (only part of which was intercepted) implies that the Japanese were more concerned at that time with the possible compromise of their own ciphers than with decryption of enemy ciphers.

"At desire of Japanese Navy prolonged conference was held 29 August on basic communication questions: documents captured at Hanking showing disposition of Jap fleet have apparently aroused the impression that their own communication service is inadequately secure. Japanese communication practice is modeled on English and American. Crystal controlled transmitters. Cipher procedure only by hand substitution. Radio, cipher and technical personnel separate; each understands only part of the field. Control station procedure unknown." (PPA 91, 2 Sept. #469).

\*\* More than a year later, in March 1945, even the reports on the general war situation mentioned above were being sent to the Germans in a form which indicated only a perfunctory consideration for cooperation. In an exchange of information reviewing the general war situation between the German Naval Staff (Rear Adm. Wagner) and the Japanese Naval Staff, the Japanese gave "information on the Greater East Asia Area situation and general conditions, based on weekly intelligence reports of the army". The lack of current and specific information from Tokyo again placed the JNA in an embarrassing position for, in response to questions concerning Japanese subs in the Singapore area, he was forced to refer to a German Intelligence report on sub operations.

Hence his request, included in the report, that the Japanese Naval Staff "arrange immediately to furnish the reports on the war situation in Greater East Asia and the general situation requested in "H" Serial #299" as well as information regarding the present and future policy in regard to sub operations in the Indian and Pacific Oceans. (JNA #049, 03/080900/45).



REFERENCES

Paragraph 1

JNA #675, 07/06 1830/43  
JNA #209, 07/102000/44

2

JNA #087, 01/24/42

3

JNA #313, 04/071800/42

4

JNA #277, 03/271200/42  
JNA #511, 06/151200/42

5

1520/21/8/42, Diplogerma  
9/9/42, #75-78

6

JNA #546, 11/26---/42

7

JNA #150, 12/211230/43

9

JNA #386, 02/031600/44

10

JNA #943, 05/182000/44  
05/252330/44

11

JNA #970, 0520 2000/44

13, 14

JNA #197, 1130/10/7/44

15

JNA #750, 2150/26/7/44

16

JNA #751, 2100/26/7/44

17

JNA #355, 2200/25/8/44

18

JNA #825, ---/31/8/44

19

JNA #649, 1000/4 Nov. '44  
JNA #035, 03/011950/45  
PPB 31, 2 March, 1945.

CHAPTER VII.

GERMAN FEARS OF THE COMPROMISE  
OF THEIR NAVAL CIPHER

• • • • •

Table of Contents

1. German precautions have been against physical compromise.
2. Allied radar blamed for U/B losses.
3. Minor scare, August 1943.
4. U/B P/W warning, September 1943.
5. Possible rumors in Fleet.
6. Sinking of "Schliemann" and "BRAKE", Indian Ocean. Cipher crisis, 12 March 1944.
7. Sinking of U-IT-22.
8. Examination of U/B R/V's, September 1943 - March 1944.
9. Cipher changes introduced at once.
10. These changes not effective against cryptanalytic attack.
11. Confidence in U/B cipher.
12. Case of Herwarts, 30 March 1944, as example of enemy's problem. Allied D/F Net.
13. U/B Special Ciphers.

Chap. VII
--------------

## GERMAN FEARS OF THE COMPROMISE OF THEIR NAVAL CIPHER

### 1.

German Precautions have  
been against Physical  
Compromise.

German Admiralty's ignorance of, or knowledge of, the extent to which their ciphers were being read has been one of the vital concerns of the Atlantic C.I. Section. This concern has been, of course, fully shared by Cominch. After each direct offensive use of decryption intelligence, principally in attacks on E/V's at sea, German traffic has been scrutinized for any evidence that serious misgivings were aroused. While no information is available on German research, it is known from traffic that fears of compromise were entertained, particularly in the spring of 1944, and that precautions were introduced in the form of very special message settings until certain major changes could be made effective. The German analysis of cipher weaknesses was apparently incomplete and erroneous, for the countermeasures adopted during 1943-1944 seem designed to defeat physical compromise rather than the Allied cryptanalytic attack.

### 2.

Allied Radar blamed  
for U/B Losses.

Other than a statement in U/B traffic of January,

~~TOP-SECRET-ULTRA~~

1943, that British Naval units had been assigned to patrol Neumann's (U-117) refueling R/V area, there was little in the early traffic read to suggest the possibility of undue German concern for the security of their cipher. And the case of Neumann was more serious as compromise of a British cipher. By May, 1943, sufficient A/S forces were available in the Atlantic to begin a general offensive sweep and from this time on decryption intelligence was steadily used in tracking down and destroying U/B's. Nevertheless a general cipher alarm was not sounded in traffic for nearly a year. Cipher changes were introduced on occasions but these were routine measures. The combination of Allied superiority in radar with the wide coverage of Atlantic A/S A/C patrols, both land based and carrier borne, probably diverted attention from communications security. Whatever the speculations at headquarters, the decline in U/B successes was officially explained by the advances in Allied radar. This explanation was repeatedly offered to the U/B's at sea, with interim orders on conduct and with liberal promises of countermeasures.

3.  
Minor scare,  
August, 1943.

In addition to the serious disruption of U/B plans by

~~TOP SECRET U.S.A.~~

sinkings at successive mid-Atlantic refueling R/V's in June, July, and August (by August the existing fleet of supply U/B's had been practically destroyed), fully half of the U/B's which did reach distant operational areas in Caribbean and Brazilian waters in the summer of 1943 failed to return. In August, 1943, the harassing of U/B attempts to make emergency R/V's off Brazil brought a reaction from Comsubs that made the Atlantic Section anxious. The R/V's had been necessitated by a surprise A/C attack on U-604 (Hoeltring) which left the U/B and its crew in serious difficulty. U-185 (Maus) was ordered to the rescue after U-591 (Ziesner) failed to respond to requests. (U-591 had already gone down.) On 1 August, Maus radioed that he would meet Hoeltring in 09.45 S. - 29.21 W. at 1400E on the 23rd. Although difficulty was experienced with traffic during this period and keys not always currently recovered, this particular message was read before the end of the same day. On the 4th, German B-Service gave Comsubs his first knowledge that something had gone wrong.

"B-Service reports: U/B motionless on surface in area 09.45 S. - 30.15 W. If R/V has taken place Maus and Hoeltring are to report position." (Note: The P/L dispatch which had been intercepted actually read "still on surface").

0058/4

The R/V had not been effected due to successive interruptions from A/C. New assignments were made and a third U/B, U-172 (Eamermann), was brought into the rescue. On the 11th the three subs got together but another A/C intervened before Eamermann

~~TOP SECRET - MINTON~~

could assist Maus with the crew of the scuttled U-604. On the 12th Comsubs instructed Hamermann to

"suggest R/V with Maus further to the north for the evening of the 12th using Enigma Offizier and disguised grid squares. Carry out trans-shipment of half of Hoeltring's complement as early as possible". (0012/12).

That Hamermann should have been specifically instructed to use Offizier settings was clearly a measure of security. The reading of Hamermann's R/V proposal was delayed for eight days. Suffice it to say, Maus was sunk on his way home at the Kuppisch (U-547) refueling R/V, whose location was known through decryption three days before its scheduled time.

4.  
U/E P/W warning,  
September, 1943.

A further suggestion concerning German reactions to the ever-present A/S forces came in September, 1943, from a code message\* within a letter written by P/W Hans Werner Kraus, ex. C.O. of U-199. "July 8 Bomber Rio Betrayal in Radio Control since message content meeting point known." Although the implications of compromise seem fairly clear, the message is obscure in detail. Kraus had been sunk on 31 July off Rio de Janeiro at time when he was trying to arrange a R/V with Guggenberger (U-513), who had already been sunk.

\*Code messages from Ps/W were furnished by OP 16 Z.

~~TOP SECRET - GERMANY~~

5.  
Possible rumors  
in Fleet.

The decision early in 1944 to supply U/B base Penang with cipher data was accompanied by a warning of responsibility for security: "Breaking into the cipher aids would mean the greatest danger for the U/B war." (1539/10/2). Such a statement was not exceptional in itself, but it was noted with unusual interest here because of the increasing number of molested R/V's. Furthermore, talk of cipher compromise was apparently making the rounds among U/B crews. A prisoner (Ex - U-231, C.O. Wenzel) informed OP 16 & interrogators in February that German Command feared cipher compromise" as a result of the destroyer losses in the Biscay battle of December. (These were the destroyers involved as escort for "Alsterufer".) The prisoner's statements were false on several points that could be checked against traffic. He implied, for example, that after the destroyer battle, German Command had instituted a sudden cipher change, and that U-231 had been forced to use the Reserve Hand cipher until the matter of the new keys was explained. No such traffic was intercepted. The P/W story was possibly indicative, however, of rumors and gossip in the fleet. The distress of the U/B arm would naturally have stimulated every sort of tale. In August, 1944, P/W coded

\* Presumably physical compromise.

~~TOP-SECRET-ULTRA~~

messages protested that everything was known to the enemy and that there was treason in the highest places.

6.

Sinking of "Schliemann"  
and "Brake", Indian Ocean.  
Cipher Crisis, 12 March,  
1944.

The only cipher crisis actually known through U/B traffic occurred in March, 1944, as a result of the "Brake's" sinking. The "Brake's" loss came just one month after that of "Charlotte Schliemann" and completely upset the refueling plans so necessary for combined operational and freight runs between Japanese waters and the homeland. Junker, U-532, returning after many months in the Indian Ocean, had been the last to see the "Charlotte Schliemann". When, after a month of waiting, he saw the "Brake" go down before he had been completely provisioned, exasperation alone could have prompted his report to Comsubs: "Presumably provisionings have been systematically compromised". (1809/12/3/44.)\*

7.

Sinking of U-IT-22.

To make matters worse, German Admiralty had that very morning received warning from B-Service that the Spahr-Wunderlich R/V, 450 miles south of Capetown, was being tampered with.

\*See note at end of chapter.



Spahr (U-178) had been successfully refueled by "Schliemann" before her sinking and was to receive certain materials, including radar search receivers, from U-IT-22 (Wunderlich), an ex-Italian sub carrying cargo to the Orient. By evening of the 12th Comsubs had reason to believe that the U-IT-22 was no more, for Spahr on surfacing reported a large oil slick where Wunderlich should have been. Within 48 hours emergency cipher arrangements were being transmitted to U/B's.

8.  
Examination of U/B R/V's:  
September 1943 - March,  
1944.

The R/V disturbances which occasioned this crisis were of course due to decryption. In an attempt to appreciate the problem as it might conceivably confront German Admiralty, the Atlantic Section<sup>of Op-20-G</sup> examined the R/V traffic record for the period September, 1943, to March, 1944, inclusive. Participating U/B's reported the presence of Allied forces in 21 of the 48 major R/V's actually held during this period. The attendance of Allied units at German meetings seemed sufficiently irregular to make any strong generalizations unlikely, especially since the Germans were prepared to believe in the ubiquity of Allied patrols - except possibly in the southern Indian Ocean. Had it not been for the peculiar circumstances surrounding the loss of

two such important ships as "Schliesmann" and "Brake" within so short a period of time and in such a remote area, fears of compromise might have remained dormant or might have been rendered inactive by force of other possible explanations.

9.  
Cipher Changes Introduced at once.

It must have seemed that there was no place in the oceans where the German Navy could R/V with assurance. To meet this intolerable situation German Admiralty introduced an awkward cipher procedure making use of the names of crew members identified by their service numbers. The first of these special settings, called "Maske", was sent on 14 March to Stude, (U-455), a refueler, and the three subs who were to refuel from him. At the same time their R/V position which had been ordered in a regular officer message of 10 March was cancelled. The new R/V was to be assigned in a "Maske" message, which in consequence could be read by the C.O.'s of those four subs and those four only. On 16 March a similar procedure ("Schatten") was followed for a U/B R/V in the Indian Ocean. In all, eight such special settings were sent out to various groups of U/B's during the next four weeks until all U/B's at sea had been reached. Aside from changing R/V positions, the purpose of the special settings was the safe dissemination of a new keyword order ("Bellatrix alpha") for the enigma machine.

10.\*

These changes not effective  
against cryptanalytic attack.

Inasmuch as the special settings and the "Bellatrix  
alpha" procedure did not seem designed to defeat a cryptanalytic  
attack, it was believed that German Admiralty was primarily  
concerned with leakage of information from one or more of the  
following sources:

- a) Physical compromise of U/B enigma with regular  
and officer settings.
- b) Officer Ps/W being interrogated immediately upon  
capture and revealing information about rendezvous.
- c) Enlisted personnel having access to officer  
settings, "Bellatrix" system, and officer information  
with the attendant danger of (b) above.\*\*

Support for this view seemed implied in such statements to U/B  
C.O.'s as the following: "Strictest secrecy. Only officers to  
have access to information. No exceptions." A British appreciation  
of the situation, based on German traffic not available here,  
pointed out that certain German Naval authorities in occupied  
areas were known to be increasingly anxious about physical compromise

\*Reference for para. 10: See Memo from Comdr. Roeder to G-1  
of 23 March, 1944.

\*\*Ps/W had in fact accurately discussed the Bellatrix procedure.  
The information was not really necessary for the Allied  
cryptanalytic attack and made the Atlantic C.I. people worry  
about their own security problems primarily for fear that  
word of these interrogation results might get back to the  
enemy.

~~TOP SECRET-ULTRA~~

and were endeavoring to enforce the most rigid security measures.

"German Naval Authorities in the Adriatic and Aegean are becoming increasingly security conscious. They are afraid of leakages of all sorts, and above all of skilled interpretation of their activities by persons in Allied service. These suspicions, which were strengthened by the decode of Jugo-slav partisan traffic informing Allied authorities of the move of Admiral Adriatic to Abbazia, will be further fortified by the sinking of the "Dietrichsen". Although at the present time German Naval authorities are following a false track their noses are so very keen that anything untoward might put them on the true scent with dangerous repercussions."

11.

Confidence in U/B Cipher.

On the whole German confidence in the U/B cipher seems to have been consistently strong. The March alarm died down. New editions of certain cipher publications were put into effect but no radical changes were made, unless the U/B special ciphers can be regarded as such. (See para. 13 below.)

12.

Case of Herwartz, 30  
March, 1944, as example  
of enemy's problem. Allied  
D/F net.

That the Germans were using their own C.I. results in an examination of the security problem was evident from an exchange of messages with Herwartz (U-543) during the period of the cipher alarm. Herwartz had been provisioned at the "Maske"

~~TOP SECRET ULTRA~~

R/V and was proceeding into the South Atlantic enroute Indian Ocean. Two members of the refueling party (Leupold U-1059 and Brans U-801) had been sunk in the R/V area and by 0815/30 Comsubs was requesting immediate reports of position. At 1839/30 he asked Herwartz to report his position as of 1300/30 and to state "if, when, and where you were observed by enemy before that date". It was clear that German C.I. had decrypted a submarine estimate for 1200Z/30 (1300 Ger. Time) sent by Com. 4th Fleet in SP 2272 (29). Unfortunately the estimate had been taken from a Cominch situation report based on special intelligence and considerable concern was felt lest this slip should further stimulate German apprehension. Herwartz's reply (2221/3 April) showed that the submarine estimate had been very accurate and that it could not possibly be accounted for by any sightings of which he was aware. He was not conscious of having been observed at any time by Allied forces but thought it worthwhile to add sightings by neutrals on 6 and 12 March (Spanish and Portuguese). German attention was surely directed to Herwartz's message of 2149/24 March, which was indeed the source of the sub estimate, reckoning from the position Herwartz himself gave for the time of transmission. The Germans had to consider, however, that the sub plot lay mid way between Brazil and West Africa and could have been arrived at from a good D/F on the 2149/24 transmission. Comsubs had frequently warned his

TOP-SECRET-ULTRA

U/B's of Allied skill in D/Fing and presumably could not in this case eliminate D/F as the source of Allied information.

13.  
U/B Special Cipher.

The closing months of the war brought a new challenge to Allied cryptanalysts in the form of special ciphers peculiar to each U/B. Knowledge that U/B's were being equipped with individual ciphers was not at hand until 6 June, when the sabotage of interior land lines forced traffic between BdU and flotillas into emergency radio channels. As far as known, these special ciphers were not actually used until November 1944. Special ciphers were used increasingly during late December 1944 and January 1945, but at no time eliminated the continuing reliance on the enigma general and offizier.

It was believed at the time that the introduction of individual ciphers was an outgrowth of the forebodings which followed the "Brake's" loss in March 1944 and that they represented a further safeguard against physical compromise, an eventuality whose likelihood would increase with an invasion of the Continent.

Two special ciphers were finally broken in April 1945 as the result of re-encipherments in the regular naval cipher. It was discovered that the breaking of each special cipher was equivalent in difficulty to breaking a new month of normal enigma traffic.

14.  
Increasing Fear of Physical Compromise.

Fear of physical compromise naturally increased as U/B's undertook shallow-water campaigns while the land front went to pieces. In September 1944, a Russian attempt to salvage the U-250 (Schmidt) made probable the compromise of secret and most secret memoranda on board. It was necessary to issue warnings to all U/B's that

- "Loss of U/B's in shallow waters gives the enemy the possibility of diving for cipher material and data.
- 1) Make sure that cipher data are so kept that water can actually come into contact with the red print.
  - 2) When enigma cipher machine is not being used, disconnect the stackers, take out the wheels and disarrange them. Keep everything concealed in separate places. See further St.V.O. Nr. 246.
  - 3) See to it that keyword orders are known to three officers only.....
  - 5) Lack of attention ((to these points)) may have unforeseeable results for the U/B war."  
(Offizier 2107/2237/28/12/44).

In addition to diving, the Germans feared boarding parties.

"So great is the enemy's interest in new devices, enigma cipher machines and cipher aids of U/B's, that he attempts in every possible way to board U/B's....."  
(2108/9/1/45)

On the eve of surrender,

"A U/B was ... attacked off the Norwegian coast by gunfire from 2 English S-boats which were first thought to be our own R-boats... Attempt was made to ram the U/B and board it, presumably in order to capture classified material. (Exper.Mag.#236, 1255/27 April 1945).

In April the compromise of the Reserve Hand Procedure for U/B's was announced, presumably as a result of shore station losses.

At last, on 8 May, it was announced that U/B cipher

keys had been handed over to the enemy. There was still no evidence in Naval traffic that the Germans had believed a cryptanalytic compromise possible.

**H. L.**

From German Naval Attache traffic for Spring 1944 it is now known that Command conducted an exhaustive investigation of the Schliemann-Brake sinkings. The resulting analysis of their own transmissions in the E/V area, together with observations by radio personnel of receiver radiation and the known efficiency of Allied radar, apparently led to the conclusion (or implication) that the Allies could have located the ships by D/F and analysis alone. (PPA 63, 25 April 1944).

~~TOP SECRET-ULTRA~~



