

# ULTRA IN THE ATLANTIC

## Volume III

### GERMAN NAVAL COMMUNICATIONS INTELLIGENCE

An Edited Version of SRH-024

- Organization and Working of German Naval Communications Intelligence.
- Intelligence Disseminated to U-boats and the Sources Acknowledged in U-boat Traffic.
- German Intelligence on Allied Convoys in the Atlantic.
- Compromise of Naval Ciphers #3 and #4.
- "B-Dienst" Aboard U-boats.
- German-Japanese Cooperation in Communication Intelligence.
- German Fears of the Compromise of Their Naval Cipher.

Edited  
By  
Jeffrey K. Bray

# ULTRA IN THE ATLANTIC

VOLUME III

GERMAN NAVAL COMMUNICATION INTELLIGENCE

Edited by

Jeffrey K. Bray

Revised Edition Copyright © 1994 by Jeffrey K. Bray

ISBN: 0-89412-237-1

**Aegean Park Press**  
P.O. Box 2837  
Laguna Hills, CA 92654  
(714) 586-8811  
FAX (714) 586-8269

Manufactured in the United States of America



## Acknowledgments

This effort was originally intended to correct the quality of the copies that are currently on file at the National Archives and Records Administration in Washington, D.C. Throughout the process of retyping and editing the manuscript many individuals contributed to the overall success and the open disclosure of the "Battle of the Atlantic History."

Specifically I would like to thank Vice Admiral John M. McConnell, Director of the National Security Agency and his outstanding staff in the Freedom of Information Office; Mr. Bernard Calvacante and Mrs. Kathy Lloyd at the Operational Archives, Naval Historical Center; Mr. John Taylor and Mr. Barry Zerby at the Military Reference Branch, National Archive and Records Administration; Mr. Dennis Vetock at the U.S. Army Military History Institute; Mr. Grady Lewis and Mr. Irv Newman at the Naval Cryptologic Veteran's Association; Mrs. Alice Creighton at the Special Collections Division, Nimitz Library, U. S. Naval Academy; and Lt. Patrick Padgett and LN1 Steve Neal at the Staff Judge Advocate Office, Naval Security Group Command.

I would also like to thank Dr. Carl Boyd, at Old Dominion University, for his assistance and encouragement provided throughout the whole effort. The assistance provided by the many cryptologic veterans of the Second World War who have also given their time is greatly appreciated.

Every attempt has been made to correct any errors in the manuscript. The original copy was in draft form and never went into production. The intent has been made to keep the history in the same format as drafted. Several corrections are included and, in some instances, clarification is offered to benefit the reader's understanding. Any oversights are those of the editor.

## Preface

The Battle of the Atlantic series was an official internal history of the activities of Director of Naval Communications (OP-20-GI-A). The history comprised five volumes. In the original draft version appendices appeared in between individual chapters. This format can result in confusion and it interrupts the normal flow of the text. All of the appendices have been combined into a single group and comprise the contents of volume six.

Specifically, the contents of each volume are as follows:

- Volume I Allied Communication Intelligence and the Battle of the Atlantic
- Volume II U-Boat Operations
- Volume III German Naval Communication Intelligence
- Volume IV Technical Intelligence from Allied Communications Intelligence
- Volume V German Naval Grid and its Cipher
- Volume VI Appendices

Volume two of the U.S. Navy's "Battle of the Atlantic" history is a review of U-boat operations from a communications intelligence perspective. Volume three is a full disclosure edition of Special Research History-024 (SRH-024) of the Records of the National Security Agency (Record Group 457) presently held at the National Archives and Records Administration. While the actual authors have remained anonymous it is known that the draft version was proof read and annotated by, then Captain, Joseph N. Wenger.<sup>1</sup> The work was so closely guarded that even the senior officers assigned within the Atlantic Section were not aware of its development

---

<sup>1</sup>The annotations have been verified by the editor's interview with Admiral Wenger's son, Jeffrey Wenger, on 2 January 1994. Admiral Wenger was then the head of OP-20-G.

or existence.<sup>2</sup> It is most likely the product of Lieutenant John V. Connorton who was Captain Wenger's staff historian for OP-20-G and had access to the Atlantic Section's files.

The American "Battle of the Atlantic" history is not an all encompassing document. The series was written near the end of the war. The project was started around November 1944 and was not completed until shortly after V-J Day. Since the American history was completed as the war was ending it only uses sources available at the time in the offices of the Atlantic Section. However, unknown to many, the British at GC&CS were able to accomplish a more comprehensive study. A twenty-four volume naval history of communications intelligence in the Second World War was completed following the end of the war. The British series exclusively covers the naval conflict in the Atlantic and European theaters and a good portion it was the product of several American naval officers assigned to Bletchley Park.<sup>3</sup> The British effort was able to utilize all sources, Allied and Axis, in documenting the war from the perspective of communications intelligence and as such presents a more comprehensive study.

However, the American study provides a detailed view of the struggle for the Atlantic. The problems of Allied collaboration continuously plagued the communications intelligence effort. The increasing levels of intercepted message traffic, especially following the Normandy landings, placed a heavy strain on the whole apparatus. Nevertheless, as is demonstrated, the priority of eliminating the U-boat threat with this new form of special intelligence reconciled many differences.

---

<sup>2</sup>Editor's interviews with Willard "Van" O. Quine on 18 September 1993, Knight McMahan on 5 October 1993, and Allan Moltzen on 2 November 1993.

<sup>3</sup>Editor's interview with Knight McMahan on 5 October 1993.

## Introduction

The onset of war in Europe in the fall of 1939 caught the German navy off guard. It lacked sufficient numbers in surface vessels, submarines, and trained personnel to meet its immediate needs. To make up for these deficiencies the Naval High Command required timely and accurate intelligence on enemy naval operations. Like similar requirements of its adversaries, the German navy became dependent on communications intelligence to aid its war effort.

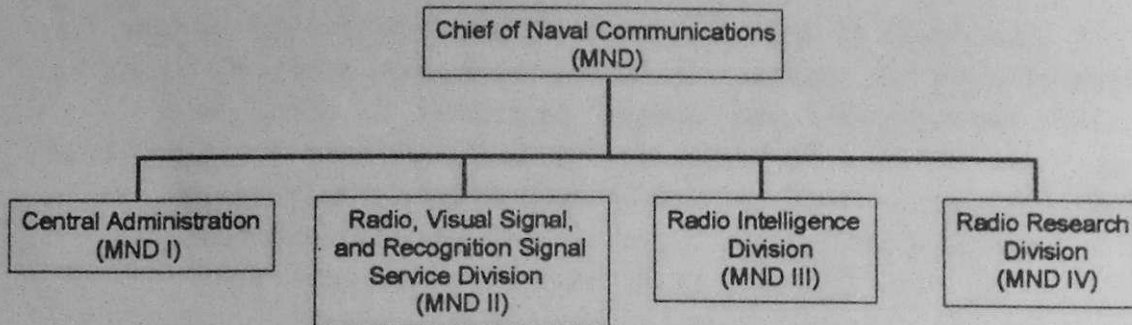
The German navy's intelligence service reflected the needs of the Naval High Command.<sup>1</sup> When the war started, all naval intelligence was coordinated by the Abteilung Marinemachrichtendienst (3/Skl) [Division of Naval Intelligence].<sup>2</sup> In January 1940 a naval command reorganization changed the designation of the Marinemachrichtendienst from the third division of the Seekriegsleitung (Skl) [Naval War Staff] to the second (2/Skl). This action recognized the establishment of a separate office for naval communications and communications intelligence. At the same time the Office of Naval Intelligence retained its designation as 3/Skl but its name was changed to Abteilung Nachrichtenauswertung. In a further progression the communications section was renamed Amtsgruppe Marinemachrichtendienst (2/Skl) [Office of Naval Communications] in June 1941. In March 1943, the operations division of U-boat Command was incorporated into the Naval War Staff. Due to its dominance in the German naval service it was designated 2/Skl and the Office of Naval Communications was re-designated as 4/Skl. It would retain this designation for the duration of the war.

While the Office of Naval Communications constantly changed from command reorganization its internal designations remained essentially unchanged. Through the first half of the war the Office of Naval Communications was divided into four sections:

---

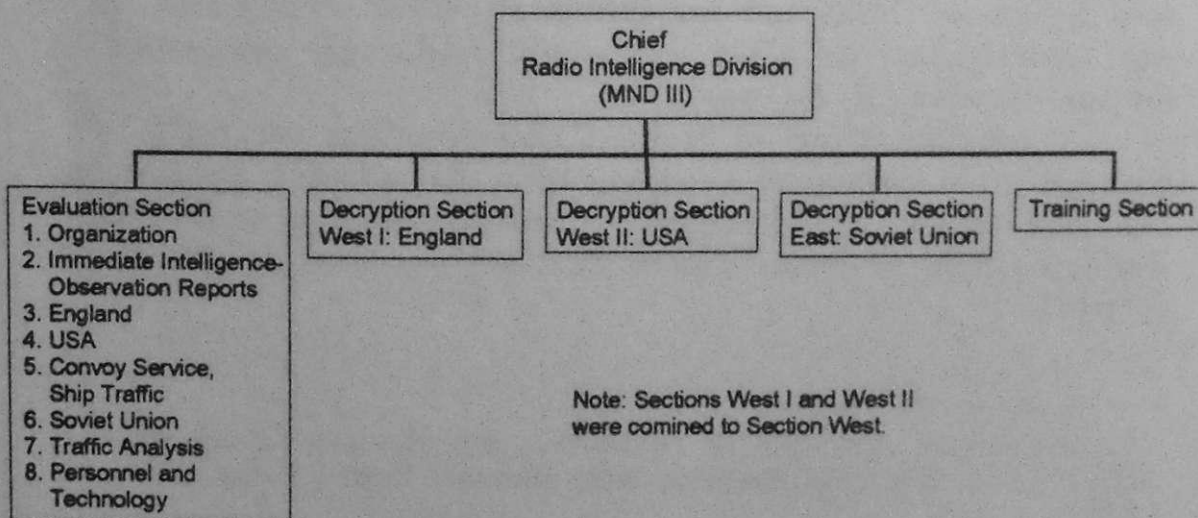
<sup>1</sup>Walter Lohmann and Hans H. Hildebrand, *Die Deutsche Kriegsmarine 1939-1945* 3 vols. (Bad Neuheim, West Germany: Podzun Verlag, 1964) 1: 3.32.

<sup>2</sup>The German word "Nachrichten" literally means information. However, in military terms it means also communications, signals, or intelligence. One must know its relationship to ensure which military meaning is inferred.



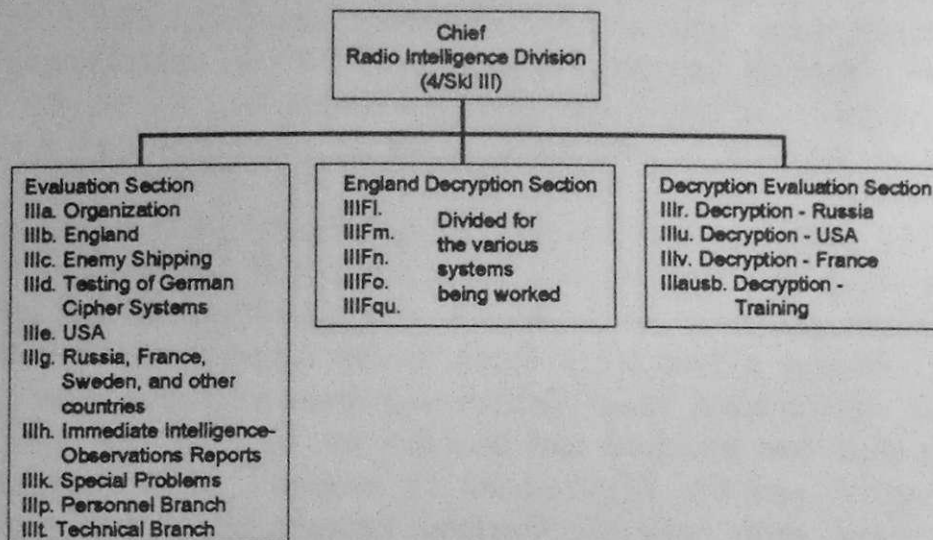
The need for more detailed research with Radar and associated countermeasures resulted in the division of radio research (MND IV) becoming its own section within the Naval War Staff, the Office of Radar Research (4/Skl), in June 1944. In September 1944, MND IV was reestablished with the responsibility for naval wire communications. When the Office of Naval Communications was re-designated 4/Skl all the subordinate divisions accordingly changed their designations from MND to Skl.

The principle office for communications intelligence was the Division for Radio Intelligence (MND III/Skl III). This division, in 1942, consisted of five sections:<sup>3</sup>



<sup>3</sup>Heinz Bonatz, *Der Deutsche Marine-Funkaufklärung 1914-1945* (Darmstadt, West Germany: Wehr and Wissen, 1970), 98.

Sometime later sections West I and II were combined and simply called Decryption Section West. With the re-designation of the Office of Naval Communications to 4/SkI in March 1943 the radio intelligence section was also reorganized. Its composition was:<sup>4</sup>



Throughout the duration of the war the radio intelligence section was commonly known as the Beobachtung-Dienst (Observation Service) or B-Dienst. The decryption section was sometimes referred to as the Entzifferung-Dienst (Decryption Service) or E-Dienst. However, to most outside observers German naval communications intelligence and B-Dienst were synonymous.

When the war started the B-Dienst had a modest intelligence capability. It was located within the naval headquarters at Tirpitzufer 72-76 in Berlin. Approximately 90 people initially worked at the headquarters office. The B-Dienst also had 16 intercept sites manned by some 500 naval personnel. Each site was dedicated to observe the nearest enemy fleet. As the war progressed, the B-Dienst expanded to 44 intercept sites employing approximately 3,900 personnel. The Berlin office expanded to over 1,000 individuals.

The B-Dienst's successes against enemy cipher systems was initially sporadic. Prior experience included breaking several British, five French, four Russian, and three Danish

<sup>4</sup>Ibid., 99; Records of the National Security Agency, "The German Naval Signal Intelligence Service (Third Reich) 1944," SRH-379, Record Group 457, National Archives, Washington, D.C. (hereafter cited as NSA, RG 457, and its filing designations.)

systems.<sup>5</sup> However, the B-Dienst required more skilled personnel to break the systems employed at the start of the war. It quickly realized that qualified personnel were not easy to come by. Unlike the Allies, the Germans sought personnel from within the military and not from academia.<sup>6</sup> Prospective individuals were sought from called-up reservist who possessed foreign language experience. Prior businessmen with foreign experience and teachers turned out to be the most productive workers. Yet, these gains in personnel had brought little result.

The B-Dienst was reading some British naval codes and ciphers when the war started. An additional break came from the German raider *Atlantis* which was operating in the Indian Ocean. During a four week spree in the summer of 1940 the *Atlantis* encountered three British merchant vessels. The *City of Baghdad* was attacked and boarded on 10 July, the *Athelking* on 9 August, and the *Benarty* on 11 August.<sup>7</sup> The result from search these ships was the German capture of several merchant naval codes including the MERSIGS cipher which was used world-wide on the Broadcast to Allied Merchant Shipping (BAMS) system. The capture of such treasures allowed the B-Dienst to significantly improve its knowledge of Allied naval communications systems. By the end of summer 1940, the B-Dienst was reading up to 2,000 messages, from all sources, each month.

The B-Dienst also recognized the importance of establishing foreign contacts in communications intelligence. It established ties prior to the war with Italy, Finland, Japan, Sweden, Spain, Portugal, Hungary, Bulgaria, and Turkey.<sup>8</sup> Especially close ties were formed with Italy, Finland, and Japan. The Italians had been studying British naval communications in the Mediterranean. The Finns had a particular interest in Russian naval traffic in the Baltic. Japan, soon to be a member

---

<sup>5</sup>David Kahn, *Hitler's Spies* (New York: Macmillan, 1978), 216.

<sup>6</sup>Wladyslaw Kozaczuk, *Enigma: How the German Machine Cipher was Broken, and How it was Read by the Allies in World War Two*, trans. and ed. Christopher Kasparck (Frederick, MD: University Publications of America, 1984), 36.

<sup>7</sup>Steven W. Roskill, *The War at Sea 1939-1945* 3, vols. in 4 (London: Her Majesty's Stationary Office, 1954-1961) 1:281; David Kahn, *The Codebreakers: The Story of Secret Writing* (New York: Macmillan, 1967), 465-66.

<sup>8</sup>Kozaczuk, 39.

of the Tripartite Pact, also shared similar interests in communications intelligence.

The Italians possessed a naval code breaking section within its naval organization. Section B of the Servizio Informazione Segreto (SIS) [Office of Naval Intelligence] was the section directly responsible for analyzing naval communications.<sup>9</sup> It had experienced some success against British, French, and Yugoslav systems.<sup>10</sup> The organization of Section B was less than desired and failed to have any form of centralized control. It did not have any resemblance to a coordinated filing system, lacked an adequate cross-reference system, and was severely understaffed.<sup>11</sup> The B-Dienst had collaborated with Section B from time to time but viewed it with suspicion.

The relationship between the B-Dienst and Section B lacked sure-footed stability. The German navy had displayed dismay over the lack of security with Italian codes and ciphers.<sup>12</sup> Indeed, the Italian general fleet codebook was being broken by the British.<sup>13</sup> The British success with the Italian system led to the destruction or capture of ten submarines. It was feared by the Italians, and the Germans, that this dramatic loss rate with Italian submarines may be due to the compromise of their communications.

In early June 1940 the Italians sent out their submarines to conduct area reconnaissance missions in anticipation of entry into the war. The *Galileo Galilei* had been operating in the Red Sea area in less than desirable conditions. Air conditioning systems on the submarine could not reduce the excessive heat levels inside. Cases of heatstroke and chlorine gas poisoning were common. The *Galileo Galilei* was caught on the surface by the anti-submarine trawler HMS *Moonstone* on the 19th of June. The ensuing attack resulted in the death of most of the officers and crew on the submarine. The surviving members

---

<sup>9</sup>Kahn, *Codebreakers*, 468.

<sup>10</sup>MacGregor Knox, *Fascist Italy Assesses its Enemies, 1935-1940*, in Ernest R. May, ed., *Knowing One's Enemies* (Princeton: Princeton University Press, 1984), 351.

<sup>11</sup>*Ibid.*, 352.

<sup>12</sup>John W. M. Chapman, ed. and trans., *The Price of Admiralty: The War Diary of the German Naval Attaché in Japan, 1939-1943*, 4 vols. in 3 (Ripe, East Sussex: Saltire Press, 1982-1989) 4:xl.

<sup>13</sup>F. H. Hinsley et al, *British Intelligence in the Second World War*, 5 vols. (New York: Cambridge University Press, 1979-90) 1:209.

then became incapacitated by gas poisoning. The drifting submarine was boarded and searched. Found amongst the numerous papers were the sailing orders of four other submarines and a limited amount of cipher material.<sup>14</sup> As a result of learning of this incident the Italian navy instituted a major cipher change on 17 July.<sup>15</sup>

By the end of summer 1940, the B-Dienst had made significant gains against British naval systems. However, on 20 August the British instituted a world-wide code and cipher change. The German Naval High Command was dumbfounded by the sudden blackout.<sup>16</sup> The Germans were at a loss for words as to the reason for the sudden change. After all, the British had used the old system for almost a whole year of the war. It was estimated that it would take six weeks to show any significant progress against the new British systems. The suspicions of the German navy turned to Italy as the possible source of compromise. The B-Dienst sent an investigative commission to Rome in October 1940 to evaluate the security of the Italian naval communication systems.

The commission arrived in Rome and immediately began assessing the Italian naval communications systems. The head of the delegation was the Chief of the German Naval Communications, Captain Ludwig Stummel. His counterpart, Captain Vicedomini, welcomed the inspection and acknowledged that there were some deficiencies in the current systems.<sup>17</sup> Further, he was more than willing to incorporate German ENIGMA cipher machines into several critical Italian naval circuits. The head of the German naval delegation in

---

<sup>14</sup>An Italian account of this incident denies the fact that any cipher material was seized. The official British intelligence history states that cipher material was present. Marc' Antonio Bragadin, *The Italian Navy in World War II*, trans. Gale Hoffman (Annapolis: United States Naval Institute, 1957), 23; Hinsley, 1:209.

<sup>15</sup>The main Italian fleet communications would remain secure with the exception of several brief intervals in the middle of 1941. Bragadin, 23; Hinsley, 1:210.

<sup>16</sup>"This is the most serious blow to our radio intelligence since the outbreak of war. Radio monitoring and deciphering activities had been greatly facilitated by the capture of numerous enemy documents, which afforded at times an almost complete insight into enemy radio service." War Diary of the German Naval War Staff (Operations Division), Volume 12, Part A (August 1940), 173. German Sources, Operational Archives/Naval Historical Center (OA/NHC), Washington, D.C. (hereafter cited as War Diary.)

<sup>17</sup>Chapman, 4:xl.

Italy, Rear Admiral Eberhard Weichold, had stressed that Italian and German cipher systems should continue to be segregated.<sup>18</sup> Stummel apparently was not convinced and a series of cooperative measures were recommended. Despite the confidence displayed by the head of German Naval Communications, the overall viewpoint of German naval officers was that the Italians were a security risk.<sup>19</sup>

The Germans quickly went to work trying to recover from the British blackout. Within seven weeks of the change they had recovered some 1,900 code groups of the new naval code, which the Germans code named *München*.<sup>20</sup> By January 1st, the recovery totaled over 2,600 code groups. The B-Dienst continued the work despite several British modifications to the *München* system. When the Americans entered the war a new four digit Anglo-American code was discovered. The Germans designated this new system *Frankfurt* and soon realized that it was associated with convoy message traffic.<sup>21</sup>

The B-Dienst reconized the importance of the *Frankfurt* system and directed more resources to handle it. *Frankfurt* was, in fact, the new Allied Combined Cipher #3. American use of the system dramatically increased the volume of traffic which in turn increased its vulnerability to attack. The B-Dienst took people off other projects and concentrated its efforts on *Frankfurt*. By spring 1943 the B-Dienst was operating at peak efficiency. In addition to breaking individual convoy messages it was also breaking the Admiralty's U-boat Situation Report which was encrypted in this system.<sup>22</sup>

---

<sup>18</sup>John W. M. Chapman, "Tricycle Revisited: Collaboration among the Secret Intelligence Services of the Axis States, 1940-1941," *Intelligence and National Security* 7:3 (July 1992):283.

<sup>19</sup>The Italian connection remains a mystery. Many Italian communications intelligence facilities and personnel had been captured by the time of the Italian capitulation in September 1943. Any cooperative steps taken by the Italians for the benefit of the Allies still remain classified. However, it has been suggested that the Allied recovery of the eighth wheel of the naval ENIGMA may have come from the Italians. *Ibid.*

<sup>20</sup>Heinz Bonatz, *Seekrieg im Äther* (Herford, West Germany: E.S. Mittler and Sons, 1981), 31; Kahn, *Hitler's Spies*, 218.

<sup>21</sup>Bonatz, *Seekrieg*, 33-36.

<sup>22</sup>Patrick Beesly, *Very Special Intelligence: The Story of the Admiralty's Operational Intelligence Center, 1937-1945* (Garden City, NY: Doubleday, 1978), 167.

Decrypts of *Frankfurt* were passed on to U-boat Command, the main consumer of the radio intelligence, as rapidly as possible.

The German dissemination of B-Dienst intelligence brought its eventual downfall. The B-Dienst had a variety of methods for reporting its radio intelligence findings. If the matter was time critical a telephone call was made to U-boat Command. At a lower priority, a teleprinter link was used to send B-Dienst message reports. Finally, the B-Dienst produced a weekly bulletin covering world-wide radio intelligence.<sup>23</sup> The Germans, like the Allies, were equally sensitive about protecting this valuable source of intelligence. At the bottom of each weekly summary came the following warning:

"Radio evaluation requires the strictest secrecy! Every form of reproduction and extraction is forbidden. B-reports may be disseminated only in cases of emergency and then in paraphrase and without reference to source."<sup>24</sup>

In comparison, the American security guidelines for radio intelligence were strikingly similar:

"The utmost secrecy shall be used in dealing with decryption intelligence. Every effort must be made to avoid indicating any connection between the source of intelligence and the outcome of operations."<sup>25</sup>

Despite the German warnings the requirements for communications intelligence security were not rigidly enforced.

The lack of proper security measures for German naval communications intelligence compromised the source. When U-boat Command directed submarines to an expected convoy it

---

<sup>23</sup>These are on file at the National Archives, Washington, D.C. NSA, RG 457, "German Navy Reports on Intercepted Radio Messages (B./X.B. Berichte), 8 September 1939-23 March 1945," SRS-548, SRS-1166, and SRS 1870.

<sup>24</sup>Ibid.; NSA, RG 457, SRMN-051A, "OP-20-GI Memoranda to COMINCH F-21 on German U-boat Activities October 1943 - May 1945," 13.

<sup>25</sup>Records of the Secretary of the Navy/Chief of Naval Operations (SC), CNO to Commander in Chief, U.S. Atlantic Fleet, serial 0325520, dated 20 June 1942, Folder A6-2/A8, Box 287 (A6-2--A6-2(12)), Record Group 80, National Archives, Washington, D.C. (hereafter cited as SECNAV/CNO (SC), RG 80, with filing designations.)

would often attribute the source as being B-service or B-report. Naturally, the Germans had full confidence in their own cipher systems and apparently felt secure with these open statements. However, had the security guidelines been enforced by the B-Dienst any potential for compromise would have been minimized. As a result of this lack of security the Allies became aware that their own cipher security was compromised.

American suspicions of cipher compromise began to rise in early 1943. The successful U-boat attacks on the convoy ON 166 in February brought out this suspicion. Several last minute shifts of the U-boats seemed to be more than coincidental to the watch officers of OP-20-GI-A (Atlantic Section).<sup>26</sup> This concern was passed on to the submarine tracking room of the Commander in Chief, U.S. Fleet (COMINCH). Over the following four months the evidence began to mount that the Combined Cipher #3 had been broken by the Germans. In March, an Atlantic Section watch officer studied a U-boat decrypt and realized that it must have been a German report of a convoy routing message. The problem was how to verify the source of the compromise.

The Atlantic Section of OP-20-G quickly took the initiative in investigating the source of the cipher compromise. A following convoy, HX 229, also appeared to be compromised. The watch officer who made the discovery, Lieutenant Knight McMahan, was assigned to investigate.<sup>27</sup> While McMahan held one of the Navy's highest security clearances he was initially denied access to COMINCH's Convoy and Routing Division files.<sup>28</sup> A dilemma faced McMahan, the security requirement demanded that he establish his need to know. However, he was not authorized to disclose his reasons for searching the files.<sup>29</sup> Access was finally granted after some inter-office diplomacy was implemented. He quickly found the files relating to the convoy HX 229 and discovered the connection between the U-boat traffic and the convoy routing messages. After gathering the facts, McMahan briefed his Officer in

---

<sup>26</sup>Editor's interview with Knight McMahan on 17 November 1993.

<sup>27</sup>Ibid.

<sup>28</sup>The Atlantic Section was never on the distribution for convoy and routing messages. Thus, the only plot of convoy movements that could be made was that from U-boat contact reports.

<sup>29</sup>No one in the Convoy and Routing Division was in on the ULTRA picture and McMahan could not disclose it to them.

Charge, Lieutenant Commander Bernard F. "Dutch" Roeder; the Director of Naval Communications, Captain Carl F. Holden; and the Director of Naval Intelligence, Rear Admiral Harold C. Train. An immediate series of messages were exchanged between the Royal Navy, the Government Code and Cipher School, and the U.S. Navy.

The officers of OP-20-G were startled by the British response to the American's concerns. Several days following McMahan's briefing Lieutenant Commander Roeder was called to the office of Commander Joseph N. Wenger. He was informed that the British had suspected a cipher compromise for quite some time. Further, they had reported it to the Americans in late 1942 at the policy level only.<sup>30</sup> Roeder was furious and displayed the typical bitter feeling that many of the officers were feeling at the time towards their British contemporaries.<sup>31</sup> The British finally introduced Combined Cipher #5 in June 1943 thus ending the success of the German B-Dienst.<sup>32</sup> The Germans did try to break the new cipher but only achieved sporadic success. The B-Dienst would never have the same level of success that it experience with Combined Cipher #3.

Another factor also influenced the demise of the B-Dienst. The Allied invasion of Sicily in July 1943 would further compromise the operations of the B-Dienst. The B-Dienst had an intercept station located below the Straits of Messina at the city of Taormina.<sup>33</sup> The regional headquarters of the Italian navy was on the opposite side of the island just outside the city of Agrigento. Allied action at these two cities would directly affect the B-Dienst. Agrigento fell to American forces on 16

---

<sup>30</sup>Editor's interview with Knight McMahan on 17 November 1993.

<sup>31</sup>For more on the British-American collaboration problems see Jeffrey K. Bray, ed. *Ultra in the Atlantic*, 6 vols. (Laguna Hills, CA: Aegean Park Press, 1994) 2:xii-xxv.

<sup>32</sup>Hinsley, 2:636. It is surprising that the official British intelligence history on cipher security fails to mention the American influence on the change to Combined Cipher #5. Some of the officers in the Atlantic Section felt the British actions in this matter were criminal. This was during the period of the largest merchant shipping losses ever experience at the time in the Atlantic. Had the American naval communications intelligence personnel been directly alerted the excessive loss of life and material could have been minimized.

<sup>33</sup>Bonatz, *Die Deutsche Marine*, 102.

July and was immediately occupied by reconnaissance teams.<sup>34</sup> A contingent of American naval intelligence officers searched the city and discovered the regional naval headquarters just outside of the town. The team immediately noticed that the building had been evacuated in a hurry and that all documents had remained as they were left, the building had not been looted.<sup>35</sup> Three safes were discovered in addition to the documents left behind. The safes were forced open and an inventory of the contents revealed "some of the most secret codebooks of the Italian armed forces."<sup>36</sup> The material was boxed up and taken to Malta by ship and then handed over to the British naval intelligence officer. From Malta the documents were immediately flown to London to be processed.

The Sicilian city of Taormina was the headquarters of Field Marshal Albert Kesselring, the Commander in Chief, German Armed Forces, South. The town was also the location of the B-Dienst's Italian intercept site. Taormina was occupied by British forces on 14 August but it remains unknown if the communications intelligence site was captured intact.<sup>37</sup> It is known that a supposedly mobile intercept unit was damaged at Messina, just to the north of Taormina.<sup>38</sup> A German codebook and several notebooks on British and American codes and ciphers were seized following the raid. With the loss of Taormina the B-Dienst moved its operations to Genzamo just south of Rome.<sup>39</sup>

In the weeks that followed actions in Italy turned against the Germans. An Italian intercept station on the island of Capri was captured along with its documents.<sup>40</sup> The sudden Italian armistice on 8 September 1943 ended the German intelligence collaboration with Italy.<sup>41</sup> This event brought on a wave of

---

<sup>34</sup>Albert N. Garland et al, *United States Army in World War II: The Mediterranean Theater of Operations*, vol. 2, *Sicily and the Surrender of Italy* (Washington: Government Printing Office, 1965), 230.

<sup>35</sup>"A Cache at Agrigento," *The ONI Review* 1:7 (May 1946): 32. OA/NHC.

<sup>36</sup>Ibid., 34. There is no mention of this remarkable find in the official British intelligence history.

<sup>37</sup>Garland, 412.

<sup>38</sup>Hinsley, 3 (part 1): 469.

<sup>39</sup>Bonatz, *Die Deutsche Marine*, 101.

<sup>40</sup>Hinsley, 3 (part 1):469.

<sup>41</sup>The Chief of German Naval Communications Division revealed his concerns three days later at a staff meeting. He pointed out the presence of Italian intercept stations posed a serious risk to the German

captured equipment and personnel. American naval intelligence teams were overwhelmed by the vast amount of material that had to be processed.<sup>42</sup> The Director of Italian Naval Intelligence (SIS), Admiral Franco Maugeri, was captured by the Americans. In addition to interrogations, some Italians were allowed to continue their work on special projects with Allied supervision and exploitation. To what degree the Italians collaborated with the Allies on communications intelligence still remains classified.<sup>43</sup>

The B-Dienst was forced to acknowledge defeat in the fall of 1943. The Chief of Naval Communications, Rear Admiral Ludwig Stummel, was compelled to report the bad news to the Naval High Command. Due to the Italian betrayal the German naval communications service had suffered serious damage.<sup>44</sup> It was known that the Allies would have full knowledge of the B-Dienst's work on British systems and what captured material it possessed. He further continued that due to this knowledge that it was expected that the British would be making significant changes to their codes and ciphers. Two months the Allies began introducing the Combined Cipher Machine into naval communications systems. The B-Dienst made no attempt to break this system and resorted to traffic analysis and close scrutiny of medium and low grade message traffic.<sup>45</sup>

The B-Dienst had been a highly capable communications intelligence organization that slowly withered away as the war progressed. While it was able to produce high grade intelligence, up to till the summer of 1943, it lacked authority. Distribution of its intelligence was wide in scope and lacked

---

navy. He recommended that all sites and personnel be placed under German guard and all documents seized. The Chief of the Naval Staff agreed and ordered that German Naval Command, Italy take the necessary actions. War Diary, Volume 49, Part A (September 1943), 154.

<sup>42</sup>Anthony Marsloe, "Collecting Technological Intelligence in Italy," *The Naval Intelligence Quarterly* 2:3 (1958):12-13. OA/NHC.

<sup>43</sup>It is known that several Italian military officers were interrogated by U.S. naval intelligence officers of the Eighth Fleet. They provided detailed information on the normal and modified ENIGMA machines, the details on the "AU-KA" code for aero-naval collaboration, details on "SYKO Card" reconstruction techniques, and Italian-Japanese communications intelligence collaboration. See SECNAV/CNO (SC), RG 80, Commander U.S. Eighth Fleet letter to Chief of Naval Operations, serial 00207/NIU, dated 28 March 1945, Folder A6-3--A6-3(15)/QA, Box 2277 (A6-2(14)--A6-4(11-20 Jan)).

<sup>44</sup>War Diary, Volume 49, Part A (September 1943), 254-55.

<sup>45</sup>Hinsley, 2:638-39; Kahn, *Hitler's Spies*, 222.

proper safeguards. The result was a complete compromise of the German navy's most valuable source of intelligence - decrypted Allied message traffic. Yet, with the B-Dienst reading ULTRA-based intelligence messages, especially the Admiralty's U-boat Situation Report, it could not notice that its own messages were being read. This was due, in part, to the high level of confidence the German naval leaders had on the security of the ENIGMA cipher machine. One participant of the radio war even suggested that due to the operational tempo of the war their just was not enough personnel available to analyze all the intercepted message traffic.<sup>46</sup> Regardless of the causes, the B-Dienst had provided half of the operational intelligence used by the German navy.<sup>47</sup> This contribution was unmatched by any other source and demanded a significant amount of Allied resources.

---

<sup>46</sup>Beesly, 167.

<sup>47</sup>Kahn, *Hitler's Spies*, 222.

## List of Abbreviations

A/C	Aircraft
A/S	Anti-submarine
ASDIC	Underwater sound location device
BAMS	Broadcasts for Allied Merchant Ships
CBM	Cubic meter
CINCCNA	Commander in Chief, Canadian Northwest Atlantic
CINCWA	Commander in Chief, Western Approaches
CESF	Commander, Eastern Sea Frontier
CMSF	Commander, Moroccan Sea Frontier
CNO	Chief of Naval Operations
COMINCH	Commander in Chief
COMNAVEU	Commander, Naval Forces Europe
CRT	Cathode Ray Tube, television screen
CSP	Code and Signal Publication
CVE	Escort aircraft carrier
D/D	Destroyer
D/F	Direction Finding
FOIC	Flag Officer in Charge
GAF	German Air Force
GC&CS	Government Code and Cypher School
GNA	German Naval Attaché
GNAT	German Naval Acoustic Torpedo
GSR	German Search Receiver
H/F	High Frequency
JNA	Japanese Naval Attaché
KCS	Kilocycles
MCS	Megacycles
M/F	Medium Frequency
MPA	German naval D/F divisions
MPHS	German naval D/F main stations
MPNS	German naval D/F subsidiary stations
M/V	Merchant Vessel
NEMO	American code name for captured U-505
NOIC	Naval Officer in Charge

ONI	Office of Naval Intelligence
RAF	Royal Air Force
RIP	Radio Intelligence Publication
RFP	Radio Finger Printing
R/V	Rendezvous
SIS	Italian Naval Communications Intelligence Organization
SKL	German Naval High Command
SPECNAVO	Special Naval Observer
TINA	Radio Transmission Characteristics Intelligence
T-V	Zaunkönig acoustic torpedo
U/B	U-boat
VL/F	Very Low Frequency
WW	German Weather Messages

## Chapter I

### Organization and Working of German Naval Communication Intelligence

\* \* \*

1. In relation to German naval organization.
2. Subdivision of 4 SKL "Marinenachrichtendienst," naval communication service.
3. 4 SKL/III "Funkaufklärung" (radio intelligence).
4. The German radio intelligence bulletin and the handling of ULTRA.
5. Concentration of German communication intelligence on Allied convoy traffic.
6. Use of non-radio intelligence material.

## Organization and Working of German Naval Communication Intelligence

### 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 turned formed one of the six numbered "Naval War Staffs." Late in 1944 these war staffs were as follows:

OKM	Naval High Command	Grand Admiral Dönitz
Stabschef SKL	Vice Chief of Naval Staff	Vice Admiral Meisel
1 SKL	Operations	Rear Admiral Hans Mayer
2 SKL/BdUop	U-boat Operations	Rear Admiral Godt <sup>1</sup>
3 SKL	Intelligence	Rear Admiral Otto Schulz
4 SKL	Communications	Rear Admiral Stummel
5 SKL	Radar Research	Commander Meckel
6 SKL	Hydrography & Meteorology	Vice Admiral Fein

### 2. Subdivision of 4 SKL "Marinenachrichtendienst," naval communication service.

Chef MND: Rear Admiral Stummel

I. Central Office: Captain Möller.

II. German Communications: Captain Lucan

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

III. Radio Intelligence: Captain Kupfer

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

---

<sup>1</sup>Dönitz retained high command of the submarine force. Godt was the U-boat Command's staff officer for operations.

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

Location: After bombardment of Berlin in November 1943, Section I moved to Koralle with Dönitz and staff. Sections II and III moved to Bismark and later to Eberswaldo. When the Russians reached the Oder in 1945, 4 SKL moved to Wilhelmshaven area.  
(Ultra/ZIP/ZG/337)

3. 4 SKL/III "Funkaufklärung" (radio intelligence).

(a) Intercept net.

The intercept net was organized, in part at least, into naval D/F divisions (MPA), naval D/F main stations (MPHS), and naval D/F subsidiary stations (MPNS). 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 RAF traffic, including radio traffic. Of particular interest was MPA Flanders, located in the Castle of Saint Andries near Bruges, where the operators captured from U-664 (Graef) were trained.<sup>2</sup>

In addition to interception, D/F work and the training of B-Dienst operators, MPA Flanders received and broke low to medium grade British naval traffic, such as Loxo and Foxo. 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 English position reporting system.

---

<sup>2</sup>U-664 was sunk by a U.S. Navy aircraft on 9 August 1943. Eight crew members were lost and 44 captured.

(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 two sections, according to the Japanese Naval Attaché: "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 cryptanalysis alone.

(1) "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 02274).

Recovery of delivery groups.  
(Ultra/ZIP/ZG/310)

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

(2) Cryptanalysis.

The internal organization and workings of this section are as yet little known. After the armistice with Italy, officers of the Italian naval communications intelligence organization (SIS), 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. (GC&CS Intel Memo #66)

4. The German radio intelligence bulletin and the handling of ULTRA.<sup>3</sup>

A German naval radio intelligence 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 "Auswertung" section. Presumably a correlation room existed, to which were passed the final results of the entire communications intelligence organization. The bulletin is carefully organized and apparently follows a relatively fixed form.

(a) Distribution of the bulletin.

According to the introductory printed pages, 25 copies of the bulletin were made, 22 of which were distributed and 3 held in reserve. This distribution list is considerably longer than is customary in the case of U.S. Navy radio intelligence 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 Destroyer Flotilla in northern Norway)

Comsubs Norway/Admiral Northern Waters at Narvik

Naval Liaison with Wehrmacht Field Headquarters

German Naval Command Italy

---

<sup>3</sup>These bulletins are on file at the National Archives, Washington, D.C. Records of the National Security Agency, "German Navy Reports on Intercepted Radio Messages (B./X.B. Berichte), 8 September 1939-23 March 1945," SRS-548, SRS-1166 and SRS-1870. Record Group 457, National Archives, Washington, D.C.

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 submarines, explosive motor boats, special commandos for mining and sabotage)

Distribution within Naval High Command:

6 copies to various sections of COMINCH and CNO including U-boat operational command (i.e. Chief of SKL, 1 SKL section, 2 SKL/BdU 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 DNC

- (b) Grades of radio intelligence information and its dissemination by dispatch.

Two kinds of radio intelligence information are distinguished according to their source:

"B-Reports" or "B-Information": based on traffic analysis and 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 radio intelligence organization, which contain information from all intelligence sources, but mainly from the B-service itself. (ZIP/ZG/233, p. 1)

In addition to the above standard dissemination, radio intelligence 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) Captured bulletin's information, its organization and scope.

If the captured copy of the 23 June 1944 issue is a fair sample, the German naval radio intelligence 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, U.S. Navy Communications Security section (OP-20-X) examined the document but found "no evidence that U.S. cryptographic systems have been successfully attacked." Other than the monitoring of BAMS 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 as

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 communication intelligence on Allied convoy traffic.

The captured bulletin tends to confirm the natural supposition that the German navy's communication intelligence organization would concentrate its energies on serving the most important operational part of the navy, the U-boat, 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-boat traffic. There were exceptions, but on the whole German radio intelligence did furnish the U-boat navy with that essential requisite for the successful prosecution of the U-boat 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 convoy chart well posted and up to date. Against this background, however, they were able at times to read 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-radio intelligence material.

It will be noted that four copies were routed to 3 SKL (German Naval Intelligence) 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 German radio intelligence organization was itself responsible for the correlation of its own material with that from non-radio intelligence sources is not known. The fact remains that it undoubtedly furnished the most important intelligence for U-boat Command. Before discussing German convoy intelligence,

it is necessary to review the kinds of information sent to U-boats at sea, with particular reference to the various sources, both radio intelligence and non-radio intelligence, which were acknowledged in U-boat traffic.

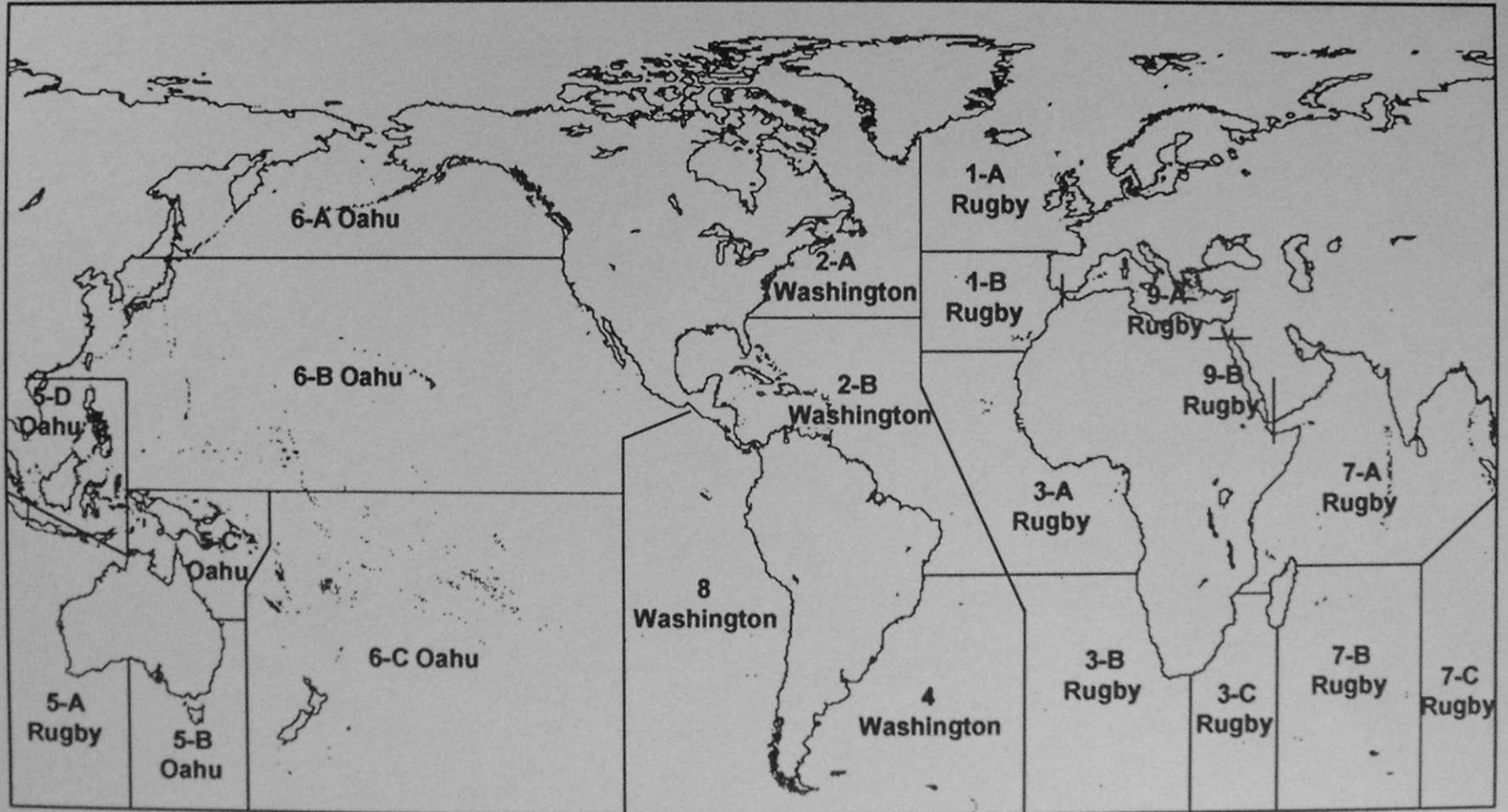
## Chapter II

### Intelligence Disseminated to U-boats and the Sources Acknowledged in U-boat Traffic

\* \* \*

1. Dissemination to U-boats at sea.
2. The course of the war as reflected in intelligence sent to U-boats at sea.
3. Sources acknowledged in U-boat traffic.
4. Aerial reconnaissance.
5. Submarine reconnaissance and observations of enemy conduct.
6. Agents.
7. Prisoners of war and survivors of encounters at sea.
8. Radio interception.

## Areas for Broadcasts to Allied Merchant Ships (BAMS)



**Intelligence Disseminated to U-boats  
and the Sources Acknowledged  
in U-boat Traffic**

1. Dissemination to U-boats at sea.

A constant effort was critically made to inform U-boats 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 anti-submarine activities. Intelligence for the U-boats defensive war included not only the number and disposition of anti-submarine units, whether surface or air, but also tactics, armament, and especially anti-submarine location devices. From time to time general estimates of Allied defenses for the various U-boat operational areas were added to the voluminous files of instructions which U-boats were obliged to carry and which were kept up to date by radio transmissions. The nature and tempo of the U-boat 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-boat 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-boat task changed or as the conditions surrounding its execution altered, the intelligence sent to the U-boats was modified.

2. The course of the war as reflected in intelligence sent to U-boats at sea.

(a) During the winter offensive, 1942-1943.

Intelligence disseminated to U-boats during the winter offensive of 1942-1943 was almost altogether on convoys, with emphasis on UK-US 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-boat circuits, and then merely to request

a clarification from the U-boat concerned.<sup>1</sup> Reports of merchant sinkings in distant areas were occasionally relayed on appropriate circuits with requests for the identity of the U-boats responsible for the sinkings.

(b) During the summer of 1943.

As the U-boat went on the defensive and sought out distant areas of operations, a distinct type of U-boat message gradually became a commonplace, and was to remain such: namely, the repetition of Allied contact and attack reports. The Allied reports became a kind of substitute for U-boat unit transmissions in view of the increasing need for radio silence on the part of the U-boat. 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 of distant coastal areas and the Caribbean were on the air.

(c) Resumption of convoy offensive. Winter 1943-1944.

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 almost 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 onboard U-boats. Allied knowledge of the U-boats 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 U.S. Navy CVE groups were pressing concerns which necessitated

---

<sup>1</sup>For example - see 1034/2 January 1943: B-Service report of attack on U-Boat in 08°N - 55°W.; Mohr (U-124) replied. Also 1324/5 February 1943 to Group *Nordsturm*: "We have two English reports of attack." Gretschel (U-707) replied.

revisions of current orders of the defense situation in an effort to determine where and when U-boats might safely surface. Attempts were made to evaluate all underwater sounds reported by U-boats in terms of new kinds of Asdic, search buoys, counter-devices for the acoustic torpedo, bluff, or marine biology.

(d) After the summer of 1944.

The German attempt to fight with an outmoded U-boat which could not escape detection by a superior enemy gradually filled U-boat traffic with messages concerning the problem of U-boat defense. A time was reached when U-boat traffic seemed to reflect more Allied activity than German activity. With the introduction of the schnorchel U-boat German interest in underwater sound 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-boat traffic.

A summary of the various sources of intelligence which were acknowledged in U-boat 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.

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 English-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-boats on UK-US convoys by means of special long range aircraft in the area of 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-boats about to enter the area concerned. Some of this information could be traced to a particular U-boats own transmitted reports, but here again there was no certainty on many points. U-boat war logs were sometimes acknowledged as the source.

When schnorchel U-boats undertook a close-in blockade of British ports during the winter of 1944-1945 their situation reports on British coastal waters became especially detailed and systematic. The "Halm" ("Blade of grass") series of Offiziers sent to U-boats on the 13-14 February 1945 offered a correlation of information on shipping which undoubtedly used non-U-boat sources. By such means U-boats were given a clear and accurate summary against which to judge the significance of their own observations.

In addition to reconnaissance, U-boats 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-boat with Allied radar, from reports of radar transmissions intercepted on the early U-boat search receivers through all the subsequent attempts to isolate the mysterious source of Allied superiority. A numbered series of "Experience Messages" kept U-boats informed of Allied anti-submarine behavior and German interpretations.

6. Agents.

(a) Gibraltar area.

Information from agents, as seen through U-boat 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-boat circuits, or on Atlantic circuits in the case of an outbound convoy. Clandestine traffic from the agents themselves was available to the Atlantic Section.<sup>2</sup>

(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-boats 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 of a minefield off Fastnet, Ireland.

In addition to details on shipping in the Gibraltar area, Japanese Military Attaché 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 Attaché's office in Lisbon as the source of his report on the disposition of the U.S. fleet. (PPB 33, 3 November 1944) 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 (UGS 27) was attributed to an agent's report. (2013/16 December 1943 to *Alsterufer* and *Osorno*) As a rule, however, German U-boat traffic reflected only a small part of an organization which was apparently extensive and active but whose outline could not be discerned.

---

<sup>2</sup>The majority of the clandestine traffic received in the Atlantic Section came from the U.S. Coast Guard and other government agencies. These documents are now on file at the National Archives, Washington, D.C. Records of the National Security Agency, "Messages of German Intelligence/Clandestine Agents, 1942-1945," SRIA 01-1550, SRIB 01-7361, SRIC 01-4164, and SRID 01-73. Record Group 457, National Archives, Washington, D.C.

7. Prisoners of war and survivors of encounters at sea.

Statements from survivors were occasionally passed immediately to Control by U-boat commanders. 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: Rudloff'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 February 1943)

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 anti-submarine measures U-boats were urged to take prisoners, especially from aircraft shot down, and interrogate them on tactics and devices for U-boat 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-boats with current D/F's. Beginning with the resumption of the North Atlantic battle, however, U-boat 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-boats 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-boats 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-boat traffic. In 1944-1945 U-boats 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 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 communication intelligence placed considerable emphasis. (see ZIP/ZG/252, p. 4). Captured German documents 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.<sup>3</sup> RAF Coastal Command traffic was also exploited in connection with convoy movements. The GAF communications intelligence organization work in close collaboration with the navy in such matters.

(c) Allied transmissions in plain language or in self-evident code.

The repetitions of merchant vessel distress signals, BAMS submarine contact and attack reports, and aircraft reports on U-boats were frequently acknowledged by the phrase "according to B-Service." It became quite evident that German intercept service guarded the BAMS circuits with care and that U-boat 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

---

<sup>3</sup>In addition to the naval radio intelligence bulletin of 23 June 1944 already referred to, see ZIP/SAC/P. 7, a GAF radio intelligence bulletin.

German traffic and invited COMINCH's attention to the advantages derived from them by the enemy.

(d) Interception by U-boats.

Although there are a few cases of U-boat monitoring on the international distress frequency in connection with attacks on merchant shipping, U-boat traffic does not show this to have been of any importance. It was certainly never stressed by Command. The only serious attempt, by U-boats 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 Aboard U-boats" in Chapter V) The most persistent attempt at interception of Allied transmissions was that directed against radar. In addition to warning for the individual U-boat, radar interception was intended to build up a knowledge of Allied radar characteristics and tactics. Early in 1944 certain U-boats 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-boat receiver could not pick up.

## Chapter III

### German Intelligence on Allied Convoys in the Atlantic

\* \* \*

1. "Convoy expected."
2. In relation to cipher compromise.
3. Convoy chart for blockade runners, December 1943 - January 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.

## 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 the routes and day by day plotting. Although independents were not neglected, information on convoys was obviously more important for the U-boat 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. "north eastbound 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-boat traffic by initials (e.g. 1626/16 September 1943, "ON," "ONS" to Group *Leuthen*). That the enemy knew the correct convoy designators and numbers, however, was clearly shown in blockade runner traffic (December 1943 - January 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 the 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, December 1943 - January 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 (abbr. "HX") and Sidney-Canada-England convoys (abbr. "SC") and English convoys (abbr. "ON" or "ONS") generally navigate a great circle from which deviation occurs only if threat from U-boat warrants. Therefore convoys are paired on fixed lanes. The northern portion of these fixed lanes is by far the most navigated." (0105/17 December 1943 ALLE 66)
- "2) "HX" and "ON" convoys have a day's run of 204 miles. "SC" and "ONS" a day's run of 180. "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 December 1943 ALLE 67)

(b) US-Gibraltar convoys, general:

"Designations: "UG" = US to Gibraltar  
"GU" = Gibraltar to US

Add "S" for slow and "F" for fast  
(0854/5 January 1944 ALLE 91)  
(1054/22 January 1944)

Cycle: 10 Days

Speed: 204 miles per day (8.5 knots) for "S"  
(0854/5 January 1944 ALLE 91)

Route: Between 32°N and 36°N from 63°W to  
Gibraltar  
(0854/5 January 1944 ALLE 91)

Escort: . . . varies. (Details) not exactly known  
here. Far ranging reconnaissance by  
aircraft and close escort by destroyers  
and destroyer escorts must be  
assumed."  
(1540/8 January 1944 ALLE 92)

(c) Dead reckoning for particular convoys.

On 16 December 1943 blockade runners *Osorno* and *Alsterufer* received dead reckoning estimates for the following convoys: HX 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 December 1943 DAN 7-10; 1013, 1037, 1102/18 December 1943 DAN 33-35).

Dead reckoning plots on GUS 26 and UGS 30 were sent 5 January, (0854/5 January 1944 ALLE 91). The convoy identifications were correct. Dead reckoning estimates for US-UK convoys were given in terms of successive "standing lines." For example, convoy HX 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 HX 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 route taken by these convoys. Had any one of the "standing lines" west of 30°W been occupied by U-boats after the fashion of the preceding winter, contact would have been made at about the estimated time. Group *Rügen*, then in the area east of 30°W, was informed of these "eastbound" convoys,

but, strangely enough, the timing given to the U-boats was not as accurate as that given to 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.

Accumulated evidence indicates that convoys which were not "expected" by U-boats were simply those in which the enemy could not take an operational interest. As the North Atlantic began to fill up with U-boats 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-boat patrol lines appropriately. In addition, the large number of U-boats 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-boats 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-boat 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 1943-1944 than the campaign of the preceding winter. From an average of about 7 a month during the winter campaign of 1942-1943, 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 1943-1944 which had been unheard of in the North Atlantic during the preceding winter; warning to U-boats of the possibility of encountering carrier borne aircraft and

other forms of anti-submarine 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-boat; of the 35 ON and ONS convoys during the same period, 27 were mentioned.

There are several instances in which U-boat 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 supplementary information in local British "low-grade" communications.

#### 5. US-North Africa convoys.

Although the German navy had no advance information the North African landings in November 1942, they had no difficulty in building up a knowledge of US-North African 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-boat group operations 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-boat groups kept vigil on the US-Gibraltar lane (winter 1942-1943) at least 4 eastbound convoys were "expected," one of the UGS 6, on the basis of cipher compromise. Only one 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-boat bound for the Trinidad area. COMSUBs recognized the target, however, as the first Trinidad-North Africa convoy. When U-boats (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 1943-1944.

Information on US-Gibraltar convoys did not reappear in U-boat traffic until the fall of 1943, when U-177 (*Gysae*), returning from an extended patrol off South Africa, was given dead reckoning 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 dead reckoning plots on convoys UGS 26 and GUS 23 were sent out to five U-boats 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 and GUS 26-32) was referred to in terms of Gibraltar arrival or departure for benefit of U-boats trying to enter the Mediterranean. Thereafter such information was disseminated only on the few occasions when U-boats were ordered to individual patrols in the Gibraltar approaches.

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

submarines or to change their rendezvous positions during June, July and November 1943. Two supply submarines 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 dead reckoning positions farther west than 37°W were ever given to the U-boats, blockade runners had been furnished with dead reckoning positions on UGS 30 and GUS 26 as far west as Bermuda. The latter had been originated by a non-U-boat section of the Navy (1 SKL), but it is hard to believe that U-boat 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 Czygan's (U-118) sinking 1410Z/12 June 1943, in 30°49'N - 33°49'W by TG 21.12 (*Bogue*).

Plans for Czygan's refueling station in 30°45'N - 33°40'W were announced in U-boat traffic on 31 May. On 12 June he was sighted on the surface and sunk within six miles of this position. No change had been ordered in his rendezvous assignment despite German knowledge that between 31 May and 12 June considerable aircraft 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 TG 21.12.

Czygan was warned late on 5 June that an eastbound convoy with aircraft escort could be expected on the 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 the 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 submarine, was in the immediate vicinity. Command showed no awareness of UGS 9 until after Manseck (U-758) had accidentally sighted a 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 submarines warned that Manseck's sightings were probably on an eastbound convoy and that they should watch out for carrier aircraft 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 rendezvous 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 for refueling rendezvous' many times in the past without mishap. One might also argue that Command had every reason to believe the three to four day old wake of a convoy a safe place for a refueling rendezvous. Czygan's sinking, however, surely indicates, besides ignorance of UGS 9, that Command was unprepared for the offensive nature of the task group that might engage in free maneuvers of its own.

- (b) Case of refueler Metz (U-487) sinking 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 concentrated on his safety. Yet he had not quite arrived at his assigned rendezvous position, 27°09'N - 33°27'W, when he was sunk 131700Z July. Convoy and Routing's plot for GUS 9 at 132000Z was 27°01'N - 33°39'W, within nine miles of the rendezvous position assigned to Metz. In blocking the US-Gibraltar lane to the north of 30°N with Group *Trutz*, U-boat 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-118 and U-487 may have started the policy of warning U-boats 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 rendezvous position to another in the area

mid-way between Bermuda and the Azores he was 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 dead reckoning position on a Gibraltar-England convoy. Warning messages were not sent because of a near collision on the German U-boat chart; U-boats were warned, when warned, even on a remote chance of encounter. For one thing, Command's day by day knowledge of a U-boats 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, U-boat Command gave the following account of US-Gibraltar convoy routes in Operational Order #56 (Nemo document):

"The convoy routes lie between 30°N and 40°N latitude; the convoys coming from America travel the southern part, those going to America in the northern part of the 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-boats 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 35°W) and DF (from 26° to 34°N - 35° to 43°W). Many repulsed attacks and the unexplained loss of several submarines 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 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 carries to the area between 25°W and 40°W, 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-boat 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-boats 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, five Offizier messages were sent to U-boats along the northwest African coast informing them of dead reckoning positions on UK-African convoys. These cases should 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 13 on "Cases of Presumed and Confirmed Compromise of Allied Communications 1943-1945)

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 demands of security theory, but the apparent ease with which the German communications intelligence 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 Cipher #3.

(a) Findings.

It was found that standard procedure made the task of enemy traffic analysts 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 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 CINCCNA approximately four 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 BAMS 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 cycles. A surprisingly large amount of fixed pattern radio traffic was broadcast in the world-wide table of the 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 U.S. Navy 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 "M" 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 no immediate action is required, be sent as in (a), above, with appropriate passing instructions in the text.
- c. CINCCNA make greater use of aircraft to carry home messages for ships and that such aircraft report last location of convoy rather than 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 CINCCNA 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 Cipher #3 and #5 (Anglo - US)

\* \* \*

1. Statistical summary, with comment.
2. Fears of compromise, February 1943.
3. Fears communicated.
4. Further evidence, March 1943.
  - (a) *Raubgraf* - 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-boat 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 apprehensions 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-boat traffic.

## Compromise of Naval Cipher #3 and #5 (Anglo - US)

### 1. Statistical summary, with comment.

For the period from January through June 1943 there are at least 39 cases in U-boat traffic of presumed or confirmed compromise of Allied naval radio communications. These cases are listed in Appendix 13 together with cases which appeared after this period. Appendix 12, taken from a British study, lists confirmed cases of cipher compromise for 1942. The enemy sources referred to in Appendix 12 were not available to the Atlantic Section of OP-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.

**Tabulation for January - June 1943**  
(The case numbers refer to Appendix 13)

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

(Appendix 13 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-boats. See case 5 for May.) After the introduction of Naval Cipher #5 in June only two cases of confirmed compromised were recorded, one in October and one in November 1943.

(a) Comment.

For a discussion of the 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 U.S. Navy communications intelligence 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 not one of the three 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.

The highly successful attack on convoy ON 166 in February 1943 crystallized 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 the German Naval High Command 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-boats, *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 (Höltring) hydrophones having picked up the convoy's screws. Three diversions had been sent to ON 166 on 17-18 February in Naval Cipher #3, table "S" as the convoy attempted to clear the U-boat 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-boat Command had accurate information on the convoy can scarcely be questioned.

The disposition and shifting of the U-boat groups between 18 and 20 February suggest knowledge of the convoy's diversion rather than reckoning based on the convoy's own position reports. Of the three diversions sent, the first

one, 1001Z/17 February 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-boat 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-boat line from 18 to 20 February, and the fear of compromise was orally communicated to COMINCH by the Commanding Officer of the Atlantic Section.

4. Further evidence, March 1943.

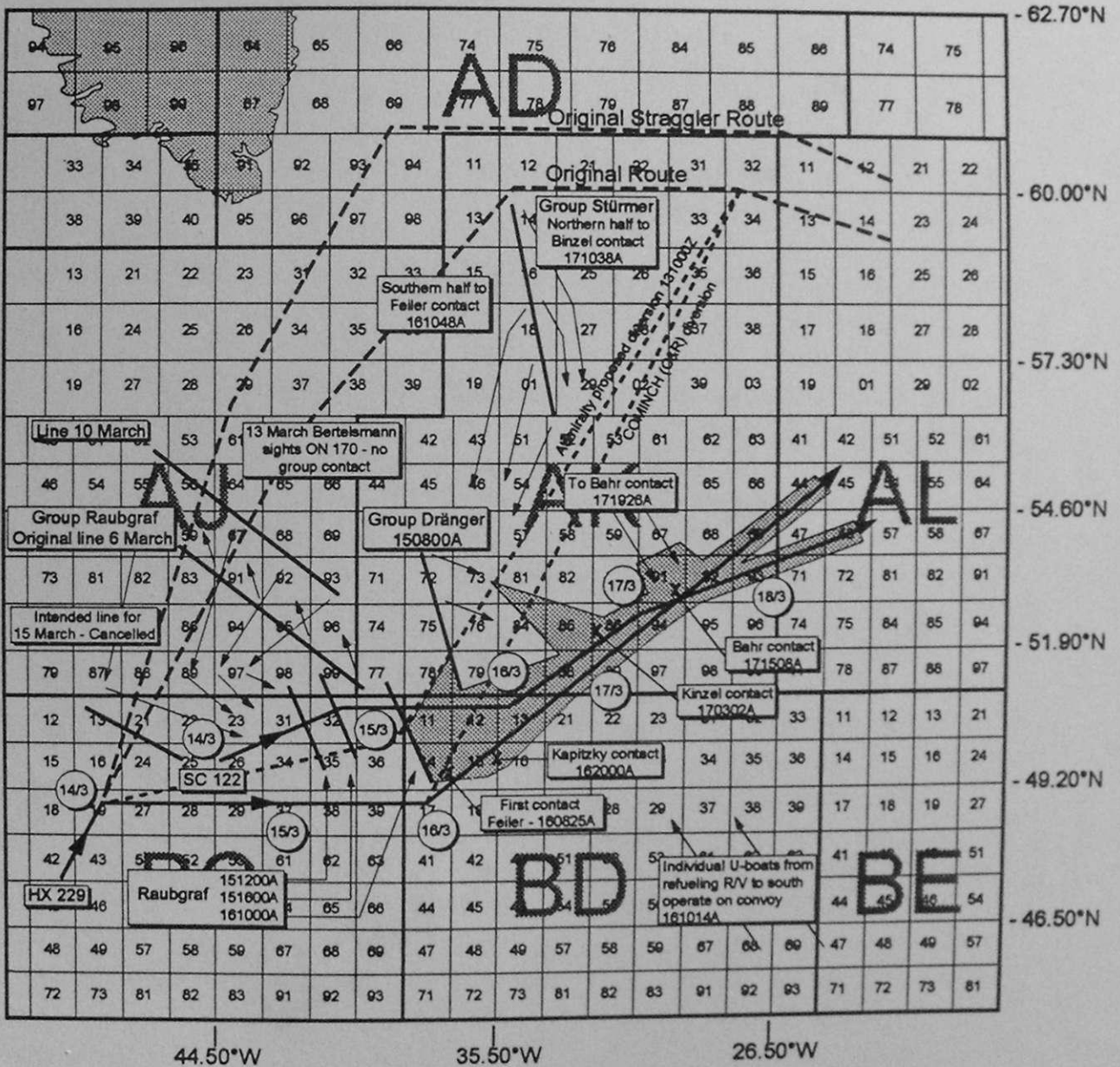
(a) *Raubgraf* - Convoy HX 229.

The *Raubgraf* operation in mid-March of 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-boat 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-boat dispatches in their chronological relation.

041704Z March	Original route for HX 229, sent in Naval Cipher #3, "M"
1602Z/13	HX 229 diverted; ordered to turn due east on reaching 49°N - 48°W. (J) Sent in Naval Cipher #3, "M"

(The presence of U-boats across the original route between Newfoundland and Greenland was known.)

## Groups Raubgraf, Dränger, and Stürmer - HX 229 and SC 122 March 1943



- 1214A/14            *Raubgraf* ordered to form new line off Newfoundland for 15 March in expectation of a "north eastbound 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* submarines transmitted, two to give their positions and three to report land based aircraft.

There is nothing in these reports which could have justified Command's conclusion that a northeast convoy not yet sighted was turning into an eastward 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 aircraft before he could investigate. Walkerling remained close, for he made contact on a destroyer 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-boats 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 to the north for HX 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 1847A/14 actually lay between the routes of SC 122 and HX 229, but orders to U-boats showed no awareness of two

convoys and U-boat maneuvers pointed to HX 229. German uncertainty as to the precise location of the convoy and Command's failure to arrange his U-boats with requisite precision before Feiler's accidental contact probably indicate that Command did not possess a complete recovery of the HX 229 diversion dispatch. It should be noted that neither in the case of HX 229 nor in the case of ON 166 were critical German messages sent in the Offizier setting.

(b) Convoy TO 2.

On 18 March U-boats 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 estimated time of arrival 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 OP-20-G but on the convoy position estimates of COMINCH Convoy and Routing.

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 NOIC 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  
Point G: 15°02'N - 51°55'W  
Point 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 knot  
(The above positions are  
the mid-points of German  
grid squares.)

It was later learned that GC&CS traced the German Offizier to two Allied dispatches, one from Flag Officer Gibraltar on 10 March (2247A) and the other from FOC WAC on 13 March

(1402), both in Naval Cipher #3, table "S". Neither of these dispatches was seen in the convoy files in COMINCH Convoy and Routing. 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-boats 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-boats. From area 42°N - 45°W *Seewolf* U-boats 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 Marbach (U-953) was informed in Offizier setting that "until March 1943, traffic proceeded to port (Casablanca) via DJ 2196 (34°03'N 08°00'W)." (1517/19 January 1944) 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 8 May showed convoys HX 237 and SC 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-boat 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* submarines had made a rapid sweep to the southeast and had found the convoy, for there were no other U-boats 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 Offizier messages. Grammatical variations of the crib "Ein erwarteter Geleitzug" (an expected convoy) were tried and the compromising information came out.

(a) Investigation of first Offizier.

"2307

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 apparently eastward.  
Speed 9.3"

A careful study was at once undertaken but for several day yielded no satisfactory result because the Atlantic Section had not received all the pertinent Allied dispatches. Not until access to Convoy and Routing had been gained via COMINCH submarine tracking room was it possible to find the source of compromise. The examination of the convoy files showed that German cryptanalysis 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 7 May, for example, there were at least 6 transmissions from escorts (5 from C2 and 1 from W6). While there was no way of determining how many dispatches the Germans had read, the first Offizier could be traced without question to:

W6 Secret 062130Z to CINCCNA (in Naval Cipher #3, table "S")  
HX 237's position 43°56'N - 48°27'W, course 131, speed 9.5.

Allied dispatch

Time: 2130Z  
46°56'N  
48°27'W

German Information

2330B  
43°57'N (mid-point of  
48°25'W German 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 Offizier.

"0025/9

To: (Group) *Rhein*  
Offizier K

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 CG 2927 (BD 7927 = 43°33'N - 34°55'W) to VA 9154 (CE 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 2015B and 2310B on 8 May, for at 2051 the failure of the U-boats 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 canceled and U-boats were put on course 120 at top speed. U-359 (Förstner) made contact the following afternoon in 41°N - 37°W. Any one of several dispatches between CINCCNA and convoy escort, which resulted from difficulties in trying to change course, would have yielded the information, especially CINCCNA 060900Z to W6 and CINCCNA 061530Z to escorts, both in table "S."

(c) The third Offizier and the straggler rendezvous.

"0952/11

To: (Group) *Drossel*  
Offizier X

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 Commander of U-403. This U-boat had regained contact on HX 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 because *Dexterous* was in part responsible for the broadcast of straggler rendezvous for the 11th that was sent to Group *Drossel* in the third Offizier.

Allied dispatch

(CINCWA Liverpool  
090901)  
R/V 1400Z/11 in  
44°22'N - 27°20'W

German Information

1600B in 44°21'N - 27°15'W  
(mid-point of German grid  
square)

Escort had informed CINCWA Liverpool that *Dexterous* had strayed and requested that she be informed of rendezvous position, adding that what books she held was not known. CINCWA Liverpool broadcast the rendezvous positions in 090901, which was sent in Naval Code #3, Auxiliary Vessel System SP 02358/44 and marked BAMS. 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 Convoy and Routing. There were other puzzling points for which satisfactory explanations could not be obtained. (For British conclusions see Appendix 13, case 4 under May 1943.)

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 for First Sea Lord 072250, 072255, 072302 June 1943)

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 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 in June 22 cases of compromise (confirmed or presumed) appeared in U-boat traffic. Three of these cases are of particular interest to the U.S. Navy.

(a) COMINCH submarine notices:

COMINCH Sub Notice

Confidential  
291613Z May (in part)  
"USS Herring on patrol  
within 20 miles of 54°N  
- 42°W. USS Haddo on  
patrol vicinity 51°N -  
35°W"

German Offizier

(Positions converted  
from grid)  
1531B/31 May  
"On evening of 29 May an  
American submarine 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.

Confidential

051606Z Jun  
"Hake on patrol vicinity  
53°20'N - 37°00'W. Haddo  
on patrol vicinity 51°00'N  
- 35°00'W. Herring 54°41'N  
- 28°48'W submerged by day  
enroute 54°45'N - 28°01'W.  
ETA 051800 thence to 54°01'N  
- 22°02'W. ETA 061800  
surfaced at discretion."

1729B/8 Jun  
"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 JUN  
"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 CESF, NOB Bermuda, and others in Naval Cipher #3 that 19 British LCI(L)'s were to set 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 U-boats to leave their stations in the North Atlantic and head at once for area 35°15'N - 42°05'W. The U-boats 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 . . ."

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 and from 39° to 32°N. It was to be occupied by 0800B/1 June. Position "H" for Flight 10 was given as 33°10'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 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-boats. CMSF 240300Z was not believed compromised, for it had been sent in ECM 38. 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-boat decline.

If one may judge from U-boat traffic, German ULTRA intelligence had never been better than it was just a that period when the decline in U-boat fortunes became so evident. The increase in ULTRA intelligence disseminated to U-boats 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-boats 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-boat group attempt in May to destroy an US-UK convoy (Group *Mosel* - HX 239) made use of a decrypted dispatch giving straggler rendezvous positions, yet the operation ended on 24 May in miserable failure. At least six U-boats 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 radio intelligence 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-boat 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-boats 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-boats.

Group *Leuthen* was prepared for the initial attack with the familiar signs of convoy intelligence. In addition, two of *Leuthen's* 21 U-boats were equipped with intercept teams prepared to hear and D/F convoy voice traffic. At 1626B/16 September COMSUBs sent the following to *Leuthen*:

- "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-boats were kept informed of their progress. On the morning of 19 September U-boats 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 four and six days respectively, it was necessary to account for the accuracy of the 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 CINCWA 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 the fact "that enemy at times possesses general picture of convoy cycles and nomenclature

from various low-grade sources including WTI." (GC&CS 191858 September 1943 to OP-20-G)

10. German awareness of standard convoy routes.

Quite apart from subsequent shifts in anticipation of the convoys, *Leuthen's* original line lay across the standard route used by the majority of ONS convoys since July. There was no reason to doubt German intelligence had been keeping accurate tab on North Atlantic convoys during the period of U-boat 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 the disguised U-boat heading points and lines, particularly in those cases which read "convoy expected."

11. Evidence accumulates. SC 142 and U-220.

After the first *Leuthen* operation U-boat dispositions showed even more clearly that enemy coverage on convoy movements was reliable. On 22 September (1115B) a large minelaying-supply U-boat, U-220 (Barber), was warned of an eastbound convoy (SC 142) in the 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 apprehensions to First Sea Lord.

ON 23 September *Leuthen* boats were informed that their next operation would be against an eastbound convoy about 27 September. The convoy was HX 257. But on the following day plans were changed and U-boats were directed to proceed eastward at high speed to intercept what was clearly ON 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 the Admiralty and to COMINCH, who communicated his apprehensions to the First Sea Lord.

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

On 19-20 October U-boats were enroute from the mid-North Atlantic, when Group *Schlieffen's* operations had proved discouraging, to form a new line (Group *Siegfried*) off Newfoundland. At 2239A/19 they received the following Offizier:

"Eastbound convoy will be in nav. sq. AK 97 (area 51° to 51°54'N - 29°30' to 31°00'W) at noon 20 October. No operation; count on strong aircraft. Take advantage of chances that are offered."

The convoy, HX 261, had been diverted by CINCCNA 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," C3's Secret 181659Z October 1943 to CINCWA was established by the Atlantic Section as the source for German information.

C3 Secret 181659 to CINCWA (table "S")

"HX 261: request BAMS for  
noon R/V 19th: 50°18'N - 35°35'W  
noon R/V 20th: 51°36'N - 30°50'W."

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

14. SC 146 diversion compromised. November 1943.

By 7 November the last attempt to mass U-boats off Newfoundland was breaking up. U-boat groups had been well informed on eastbound convoys but had been powerless before aircraft. 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 November 1943)

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 November 1943)

Late on the 14th (2300) U-boats received the following Offizier setting:

"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 CINCCNA's diversion dispatch, sent in table "M", could not have been mere coincidence.

CINCCNA Secret 100606Z to Escorts to 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 BAMS 100615Z, but past experience threw the weight of suspicion on CINCCNA's dispatch in table "M." Of CINCCNA'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 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 northeast is in the same area."

15. Indications of Combined Cipher compromise cease in U-boat traffic.

After *Eisenhart's* attempt to operate on SC 146 no further cases of combined cipher compromises were seen in U-boat traffic. If the German communications intelligence organization was having difficulties at home, for which, according to a Japanese Naval Attaché report, Italian betrayal was blamed, the U-boat at sea was scarcely in a position to exploit convoy intelligence. U-boats had been told in October 1943 that locating convoys was the principal problem of the U-boat war and that the solution of this problem was the U-boats own responsibility.

To assist the U-boats an effort was made to locate convoys by radio intercept teams onboard, by relays of D/F fixes from shore, and finally by very long range aircraft. But instead of finding convoys, U-boats were being found by anti-submarine forces, while the convoys proceeded more or less in peace. Whatever the cryptanalytic situation at home may have been, U-boat 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-boat traffic carried only occasional decryption intelligence taken from merchant signals. (See Appendix 13)

## Chapter V

### "B-Dienst" Aboard U-boats

\* \* \*

1. U-boat radio intercept teams, fall 1943.
2. Previous warning in U-boat traffic.
3. U-boat D/F equipment.
4. Warning from traffic of beginning of U-boat D/F on 2410 kcs.
5. U-664 (Graef).
6. Renewal of North Atlantic battle, September - November 1943.
7. *Leuthen's* success, ONS 18 - ON 202.
8. *Rosbach's* failure.
9. COMSUBs turns to U-boat radio intercept teams.
10. B-Group performed well in *Schlieffen* operation, although attack failed.
11. Examination of U-boat Command's analysis.
12. Allied preparations.
13. Allied deception.
14. Special long range maritime patrol aircraft for convoy location, November 1943.
15. Subsequent use of B-Dienst on board.
16. COMSUBs Standing War Order Number 256 (captured document).

## "B-Dienst" Aboard U-boats

### 1. U-boat radio intercept teams, fall 1943.

With the resumption of the North Atlantic convoy offensive in September 1943, U-boats made a serious attempt to exploit convoy and aircraft 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 experiments with U-boat interception on 2410 kcs were well advertised in past U-boat 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).<sup>1</sup> During the interrogations, OP-16-Z frequently consulted the Officer in Charge of the 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 intercept at sea.

### 2. Previous warning in U-boat traffic.

The first known instant of convoy voice interception by a U-boat occurred in some of the earliest current traffic read by the Atlantic Section in December 1942. U-boat Group *Panzer* was expecting a northeast 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 English transmission on 124.5 meters in 51°27'N - 47°35'W.

Whether or not the shift in the 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-boats in Group *Meise* reported voice interceptions and signal strengths. Group *Meise* was patrolling the area north of the 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

---

<sup>1</sup>U-664 was sunk on 9 August 1943 by aircraft from USS *Card* (CVE 11) at 40°12'N - 37°29'W.

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-boats were not yet able to take bearings on frequency as high as 2410 but might be in the near future.<sup>2</sup>

### 3. U-boat D/F equipment.

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

### 4. Warning from traffic of beginning of U-boat D/F on 2410 kcs.

Early in August 1943, it was discovered from traffic that eight code groups were being added to the U-boat 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 prisoners of war, an operator named Dobberstein left St. Andries, the communications intelligence training station, in April 1943 for Brest, where he was assigned

---

<sup>2</sup>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)."

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 HX 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-boats 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 aircraft signals by shore B-Dienst stations. Special operators with such receivers as SADIR were probably to assist the U-boat 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 (U-459) a supply U-boat, 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-487) had been sunk in their rendezvous areas by aircraft from carrier task groups, and at the time of U-459's departure Command warned that a carrier force was in the 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 submarines and have drawn on B-Dienst personnel and equipment to intercept aircraft traffic for warning purposes.<sup>3</sup> The Germans had temporarily abandoned convoy operations

---

<sup>3</sup>It is presumed that SADIR was withdrawn because of re-radiation, 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 anti-aircraft U-boats as protection for U-tankers.

and hence had no opportunity to carry on with plans for intercepting convoy traffic for group attacks.

6. Renewal of North Atlantic battle, September - November 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 suitable disposed in line for taking cross bearings. The last four, *Siegfried*, *Körner-Jahn*, *Tirpitz* and *Eisenhart*, had only one, *Poel* (U-413).

7. *Leuthen's* success, ONS 18 - ON 202.

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

8. *Rossbach's* failure.

Enthusiasm was short lived, for the next three westbound convoys, ON 203, 204, and ONS 19, all slipped around the north end of the *Rossbach* line. Contacts had been made but the risks involved in transmitting to Control had discouraged U-boat commanders. COMSUBs reaction came quickly in the form of a Current War Order (#4, 1035 and 1137/6/10). The location of the convoy was the "chief problem of the U-boat warfare" and the responsibility rested on the U-boats themselves. Short signals for sighting 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. COMSUBs turns to U-boat radio intercept teams.

Despite assistance of German long range reconnaissance aircraft 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 aircraft, 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 (Krüger) were singled out by name, for there were two B-Group men on board. (1150/15 and 1852/16) The above sequence suggests that U-boat operational Command was slower than Allied communications intelligence 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 effort with B-Dienst in the Atlantic. A premature sighting of ON 206 confused the beginning of the attack, for COMSUBs apparently assumed the convoy to be ONS 20, the one he seemed to know more about. The B-Dienst U-boats were called upon to clarify the situation, but COMSUBs' initial confusion continued to show-up in his misinterpretation of their data. The sinking of Krüger on the night of the 16th placed the full burden of B-Service on Poel's U-boat.

A careful analysis of the operation indicated, however, that Poel'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 Poel's bearings in directing the attack but could not form a clear picture from the various types of reports which all U-boats submitted. At a critical moment, for example, there was considerable hesitation in trying to decide between a radio bearing reported by Poel and a conflicting hydrophone bearing sent in by Hungershausen (U-91).

After the operation had been 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 circumstances that during a convoy operation submarines have taken medium frequency bearings on aircraft or escort groups which are far from the convoy, a bearing on escort groups is a valuable clue to the convoy's position (for example, noon on 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 the bearings are taken, insofar as this is known. Procedure regulations will follow."  
(0716/20 October 1943)

#### 11. Examination of U-boat Command's analysis.

Poel's bearing, noon 16th, had been an accurate one on ON 206, then approximately 190 miles north-northeast of U-413 and on a diversion course to the northwest. 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-boats were probably right but that Poel's bearing was on ONS 20, then about to alter from

a northwest to a southwest course, and that Hungershausen had heard stragglers or rear escort of ON 206, then clearing the infested area on a southwest course. When COMSUBs clarification finally came, it rejected Hungershausen's evidence altogether. Using Poel's bearings Command drew the wrong conclusion and sent his boats in a sweep to the northwest. Meanwhile convoy ONS 20 was cutting in behind the U-boats on a southwest course. COMSUBs' 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 preparations.

Although the U-boat 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 CINCWA sent instructions and defined states or degrees of radio silence to be enjoined according to the situation. Early in November CINCWA reported two cases in which U-boats "used radio in apparent effort to obtain D/F bearing of reply. Correct convoy call sign and phonetic alphabet employed." (COMNAVEU Secret 051651Z November 1943) Operators were warned "against answering transmissions made with incorrect procedure or with foreign accents." Other cases of presumed deception by U-boat intercept parties were reported, but no one of them was ever confirmed by Atlantic U-boat traffic.

## 13. Allied deception.

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

14. Special long range maritime patrol aircraft 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 long range maritime patrol aircraft (Ju-290) for the location of convoys and the homing of U-boats. U-boat 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-boat operations were too fundamental to be overcome by a device which was tried on a limited scale and which at best presupposed some degree of mobility for the U-boat. 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 November 1943)

15. Subsequent use of B-Dienst on board.

The U-boat radio intercept project seems gradually to have been abandoned, at least in the Atlantic, for as U-boat 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 aircraft. A few U-boats on inshore operations around the British Isles continued to carry B-Groups. One of these, Albrecht (U-386), claimed that radio interception warned him of an impending search for his boat during an operation off North Ireland in January 1944.<sup>4</sup> During 1944, U-boat radio interception was confined largely to Arctic waters, where in fact it is still being used to a considerable extent.

---

<sup>4</sup>Some radio interception by U-Boats could have been on VHF (above 30 mcs) since this equipment (LO 10 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.

16. COMSUBs Standing War Order Number 256 (captured document).

Standing War Order No. 256, "Observation of Enemy Convoy Voice Traffic," was issued in October 1943. It warned U-boat operators that they must distinguish between ground and sky waves, disregarding the latter, and that they must make certain if the bearings 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 80 to 100 km.

The digest on convoy communications procedure included types of traffic originators, together with methods for identifying the convoy and originators and methods for determining the sea area, direction, and speed of the convoy. 82 codewords were listed with convoy designators and call letters of the radio guard ships. Of the 101 convoys identified with codewords there were three GUS, four UGS, four FT, four TF, one TH, and two HT convoys.

Although Standing War Order No. 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-boat offensive, it is probable that Standing War Order Number 256 would have been a modest introduction to U-boat radio interception at sea rather than an unintended, final summary.

## Chapter VI

### German-Japanese Cooperation in Communication Intelligence

\* \* \*

1. Introduction: Little evidence of effective exchange.
2. Early proposals 1942. German successes with British systems to be exchanged for Japanese assistance with U.S. navy systems.
3. Tokyo's silence.
4. The Joint Communications Agreements.
5. German communications intelligence relayed to Tokyo via the German Naval Attaché, August - September 1943.
6. Cipher material for shipment to Japan, November 1942. Indication of German progress, November 1942. Merchant signals.
7. Neglect of "Clause 7" and the Japanese Naval Attaché'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.
15. Japanese compliance.
16. The Japanese Naval Attaché'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 Tokyo via dispatch.
19. Critical situation, fall 1944.

## German-Japanese Cooperation in Communication Intelligence<sup>1</sup>

### 1. Introduction: Little evidence of effective exchange.

While information on German-Japanese cooperation in communications intelligence is still incomplete, it seems evident that effective exchange has never been established, despite the endeavors of the Japanese Naval Attaché and apparent willingness of the German Navy to share its material. On the whole the past history of German-Japanese cooperation in communications intelligence seems to be an account of professions and intentions, without any evidence of combined efforts in attacking high grade naval ciphers. The Germans have talked darkly about their successes with such ciphers but there is no record here that the Japanese have ever done that much. This conclusion is based largely on the earlier Japanese Naval Attaché traffic which became available in 1944, and on the few days of German Naval Attaché traffic which have been read for 1942-1943.<sup>2</sup>

The more recent dispatches of the German Naval Attaché (including the Offizier 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 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 communications intelligence, as indeed was claimed for a German report of December 1943 (see paragraph 7 below), but it is not possible to give a detailed derivation for them.

#### (a) Germany to Japan exchanges.

##### (1) BAMS intercepts (Indian Ocean).

Via dispatch to German Naval Attaché, Tokyo. Instances available from 1942, 1943, and 1944. Comment: Presumably passed for correlation with Axis submarine activity in Indian

---

<sup>1</sup>Based on information available as of 8 December 1944.

<sup>2</sup>See note at end of Chapter.

Ocean. German information on current locations of Japanese submarines was apparently very limited, at least prior to the establishment of the U-boat base in Penang. In July 1943, for example, the Japanese Naval Attaché stated that German navy had many radio intelligence reports of merchant vessels 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 Japanese Naval Attaché to check. At this very time the German *Monsoon* U-boats were departing western France for Indian Ocean operations and the establishment of the base at Penang.

- (2) General information on British D/F via Japanese Naval Attaché 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 the Indian Ocean as well as the Atlantic. It is interesting to note that in another dispatch of the same day (10 July) the Japanese Naval Attaché accounted for the loss of the *Satsuki #2* as follows: ". . . she was first located by D/F . . ."

- (3) Traffic analysis.

British naval frequencies, British call signs and call sign construction (ready for shipment November 1942). The same with addition of similar information on U.S. Navy and outline of joint British and American naval communications (principally for Atlantic and Mediterranean). (to be shipped August 1944, not sent). This material was requested by dispatch in view of transportation difficulties. (Sent by dispatch fall of 1944 (?)).

- (4) Captured documents

"Merchant navy code." (included in material ready in November 1942.)

- (5) Merchant signal recoveries, 1942.

Included in the material ready in November 1942 with promise to include any subsequent recoveries.

- (6) Presumably from decryption, exact source unknown.

Via dispatch to German Naval Attaché, 9 September 1942. Merchant vessel movements, Allied escort rendezvous' in Indian Ocean.

- (a) Japan to Germany exchange.

- (b) (1) BAMS intercepts.

Via German Naval Attaché 1944.

- (2) Allied anti-submarine aircraft reports.

Via German Naval Attaché. One instance known, July 1944, and this may have been a BAMS. There was also the operation *Transom* deception message which the Japanese reported on request.

- (3) Allied submarine positions and ship movements.

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

- (4) Decryption.

Via German Naval Attaché dispatch 26 October 1944. Only instance seen here. Japanese communications intelligence deciphered a message "from New Dehli to agents (probably in Penang) containing request for information on German U-boat armament and speeds."

2. Early proposals 1942. German successes with British systems to be exchanged for Japanese assistance with U.S. Navy systems.

As early as January 1942, the Japanese Naval Attaché 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 solving the U.S. Navy systems." Lacking adequate data on U.S. Navy systems, the Germans hoped to meet this need through joint research with the Japanese. The Japanese Naval Attaché proposed that intercepts of what the Japanese regarded as the principal U.S. Navy systems be forwarded via the German Naval Attaché to Germany, where "the Germans will endeavor to break them." It is clear that the Japanese Naval Attaché 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 Japanese Naval Attaché 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 U.S. Navy systems."

The Japanese Naval Attaché had planned to assign a Lieutenant Commander Mishina to joint work with the Germans in these matters but this officer had been transferred and no qualified person was now available. The Attaché 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 submarine struck a mine and sank.

#### 4. The Joint Communications Agreements.

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 Naval Communications. The 7th Clause provided that:

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

#### 5. German communications intelligence relayed to Tokyo via the German Naval Attaché, August - September 1943.

The few days of German Naval Attaché traffic which have been read for 1942 suggests that Germany made a show of compliance with "Clause 7." The German Naval Attaché received intercepts of U-boat sightings broadcast (BAMS) 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*, American transports *Cremer* and *Maetsuyeker*, and the Australian *Manunda*.

In addition, the German Naval Attaché was informed that at 0600/8 September an Allied unit was to relieve another unit in 23°15'S - 90°10'E (about 1440 miles northwest of Perth). The above items bore "B" serial numbers and were probably taken from current German communication intelligence bulletins. It is unfortunate that evidence available is not sufficient for judging the extent of German communication intelligence information which reached the German Naval Attaché in the above manner.

#### 6. Cipher material for shipment to Japan, November 1942. Indication of German progress, November 1942. Merchant signals.

A message of 26 November 1942, from the Japanese Naval Attaché 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."<sup>3</sup> 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 words of the new key word groups.<sup>4</sup>

7. Neglect of "Clause 7" and the Japanese Naval Attaché's complaint of December 1943.

The Japanese Naval Attaché 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 Japanese Naval Attaché'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,<sup>5</sup> but they had at least given the Japanese some operational information gained from radio

---

<sup>3</sup>The submarine 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 on 8 February 1943 to rendezvous with the I-29 in April, or the U-511 which departed Lorient on 10 May 1943, carrying Admiral Nomura home.

<sup>4</sup>It has been the case from viewinintercepted traffic. In fact, the B-Dienst captured a copy of the new codebook, in the Arctic theater, four weeks before it came into effect. F. H. Hinsley et al, *British Intelligence in the Second World War*, 5 vols. (New York: Cambridge University Press, 1979-90) 2:639.

<sup>5</sup>There seems to have been at least one exchange in 1943. See paragraph 16 below.

intelligence, for it was an instance of this that occasioned the Japanese Naval Attaché's complaint.

German radio intelligence had warned Japan via the German Naval Attaché 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 Japanese Naval Attaché 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 of 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 exchange of material between Japanese and German navies, it is hoped that there will be a gradual development of cryptanalytical intelligence. Even when it is difficult to get concrete decrypted material, analyses should be possible." The Germans had evidently put the Japanese Naval Attaché 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 reported 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 Japanese Naval Attaché recognized how little material

of operational value the Germans could actually furnish the Imperial Navy at that time.<sup>6</sup>

8. 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 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 successes with Naval Cipher #3. (The source of British information was not U-boat traffic.) Certainly U-boat traffic up to the summer of 1943 showed an impressive total of German decryptions in Naval Cipher #3, and some successes with Naval Cipher #5 was obtained in the fall of 1943.

It is conceivable that the Germans might have shown these to the Japanese Naval Attaché and have convinced him 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 communications intelligence ever seen in the Atlantic Section bore the date 3 February 1944.

"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 manner as possible; but the situation at present is that as yet little of the material we

---

<sup>6</sup>See note at the end of the Chapter.

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 Attaché in Tokyo . . ."

(Remainder of this message was not intercepted.)

As far as it 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 aircraft 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 Japanese Naval Attaché 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 aircraft 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 *Transom* and was sent in self-evident code.<sup>7</sup>

11. The situation in general combined intelligence, May 1944.

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

---

<sup>7</sup>Operation *Transom* was the 17 May 1944 Allied carrier raid on Soerabaya.

- (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 Attaché in Russia.
- (e) Tokyo was requested to send weekly:
  - "Our intelligence reports."
  - "Lessons learned in air in 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 Japanese Naval Attaché and Ambassador Oshima were receiving from German Headquarters and relaying to Tokyo, the Germans were not only surprised by the landings 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 threatened an invasion of Dieppe throughout July.

13. Concrete liaison July 1944. Description of German cryptanalytic activity.

Following a very friendly interview with Rear Admiral Stummel, Chief of Naval Communications, the Japanese Naval Attaché 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 communications intelligence organization. Furthermore, the Germans would make up a shipment of all types of communications intelligence 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 Japanese Naval Attaché 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 disposition of the British and American fleets."

(c) "They would also like to have the forms of all 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 form of Japanese naval communication" in terms of the different types of call-signs and the different types of textual grouping.

16. The Japanese Naval Attaché's plans and instructions.  
Japanese proposals.

As part of his immediate program for cooperation the Japanese Naval Attaché 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 Japanese Naval Attaché 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 Japanese Naval Attaché's office will be assigned.

(b) "If occasion warrants," German specialists to be employed in joint research in Japan.

(c) Exchange of Material:

(1) Material offered by the Germans to be sent on the Momi's return trip.

(2) Material offered by the Japanese to be sent by German vessel or by next Japanese cargo submarine.

(3) "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 in 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 Japanese Naval Attaché 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.<sup>8</sup> The Imperial Navy could judge from the list of contents what was of immediate necessity, extracts of which could be sent by dispatch. The contents were:

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

---

<sup>8</sup>The large consignment (70) of German ENIGMA machines and all non-crypto material destined for the I-52 were destroyed at Lorient in September.

18. Material requested by Tokyo 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 for 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 "KU 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 situation 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 Admiral Abe and Admiral Meisel on 30 October sounds characteristic of the Axis plight. Admiral 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 use special long range reconnaissance planes "or did it have any other special help?" "Other special help" surely includes communication intelligence. 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 Admiral 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 Attaché, transmitted the day before the Japanese Naval Attaché'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.

#### Concluding notes:

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

A report from the German Naval Attaché 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 Nanking showing disposition of Japanese fleet have apparently aroused the impression that their own communication service is inadequately secure. Japanese communication practices is modeled on English and American. Crystal controlled transmitters. Cipher procedure only by hand

substitution. Radio, cipher and teletype personnel separate; each understands part of the field. Control station personnel unknown."

(PPA 91, #469 2 September 1942)

More than a year later, in March 1943, a report on the general war situation mentioned above was sent to the Germans in a form which indicated a desire for consideration for cooperation. In an exchange of views reviewing the general war situation between the German Naval Staff (Rear Admiral Wegner) and the Japanese Naval Staff "information on the Greater East Asia Area was given on general conditions, based on weekly intelligence reports from the army." The lack of current and specific intelligence from Tokyo again placed the Japanese Naval Staff in an embarrassing position for, in response to a report on Japanese submarines in the Singapore area, the German staff refer to a German intelligence report on the general war situation. Hence his request, included in the report, was for the Naval Staff "arrange immediately to furnish a report on the war situation in Greater East Asia and in the Indian and Pacific Oceans requested in 'N' Serial #299" as well as in the present and future policy in regard to operations in the Indian and Pacific Oceans (JNA #049, 03/080900/45)

## References

### Paragraphs

- 1 JNA #675, 07/061830/43  
JNA #209, 07/102000/44
- 2 JNA #087, 01/24/44
- 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, Diplogerma
- 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, 1150/26/7/44
- 16 JNA #751, 2100/26/7/44
- 17 JNA #355, 2200/25/8/44
- 18 JNA #825, ----/31/8/44
- 19 JNA #649, 1000/4/12/44  
JNA #035, 03/011350/45  
PPB 31, 2 March 1945

## Chapter VII

### German Fears of the Compromise of Their Naval Cipher

\* \* \*

1. German precautions have been against physical compromise.
2. Allied radar blamed for U-boat losses.
3. Minor scare, August 1943.
4. U-boat prisoners of war warning, September 1943.
5. Possible rumors in the fleet.
6. Sinking of the *Schliemann* and *Brake*, Indian Ocean cipher crisis 12 March 1944.
7. Sinking of U-IT-22.
8. Examination of U-boat rendezvous, September 1943 - March 1944.
9. Cipher changes introduced at once.
10. These changes not effective against cryptanalytic attack.
11. Confidence in U-boat cipher.
12. Case of Herwartz, 30 March 1944, as example of enemy's problem. Allied D/F net.
13. U-boat special ciphers.
14. Increasing fear of physical compromise.

## German Fears of the Compromise of Their Naval Cipher

1. German precautions have been against physical compromise.

German Naval High Command'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 Section. This concern has been, of course, fully shared by COMINCH. After each direct offensive use of decryption intelligence, principally in attacks on rendezvous 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 seen designed to defeat physical compromise rather than the Allied cryptanalytical attack.

2. Allied radar blamed for U-boat losses.

Other than a statement in U-boat traffic of January 1943 that British naval units had been assigned to patrol Neumann's (U-117) refueling rendezvous 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 anti-submarine 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-boats.

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 wide coverage of Atlantic anti-submarine aircraft patrols, both land based and carrier borne, probably diverted attention from communications security. Whatever the speculations at headquarters, the decline in U-boat successes was officially explained by the advances in

Allied radar. This explanation was repeatedly offered to the U-boats 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-boat plans by sinkings at successive mid-Atlantic refueling rendezvous' in June, July, and August (by August the existing fleet of supply U-boats had been practically destroyed), fully half of the U-boats 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-boat attempts to make emergency rendezvous' off Brazil brought a reaction from COMSUBs that made the Atlantic Section anxious.

The rendezvous' had been necessitated by a surprise aircraft attack on U-604 (Höltring) which left the U-boat and its crew in a serious difficulty. U-185 (Maus) was ordered to the rescue after U-591 (Ziesmer) failed to respond to requests. (U-591 had already gone down.) On 1 August, Maus radioed that he would meet Höltring in 09°45'S - 29°21'W at 1400B 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-boat motionless on surface in area 09°45'S - 30°15'W. If rendezvous has taken place Maus and Höltring are to report positions." (Note: the plain language dispatch which had been intercepted actually read "still on surface.")  
(0058/4 August 1943)

The rendezvous had not been effected due to successive interruptions from aircraft. New assignments were made and a third U-boat, U-172 (Emmermann), was brought into the rescue. On the 11th the three submarines got together but another aircraft intervened before Emmermann could assist Maus with the crew of the scuttled U-604. On the 12th COMSUBs instructed Emmermann to:

"suggest rendezvous with Maus further to the north for the evening of the 12th using

ENIGMA Offizier and disguised grid squares.  
Carry out transshipment of half of Höltring's  
complement as early as possible."  
(0012/12 August 1943)

That Emmermann should have been superficially instructed to use Offizier settings was clearly a measure of security. The reading of Emmermann's rendezvous proposal was delayed for eight days. Suffice it to say, Maus was sunk on his way home at the Kuppisch (U-847) refueling rendezvous, whose location was known through decryption three days before its scheduled time.<sup>1</sup>

#### 4. U-boat prisoners of war warning, September 1943.

A further suggestion concerning German reactions to the ever present anti-submarine forces came in September 1943, from a code message within a letter written by prisoner of war Hans Werner Kraus, ex-Commander of U-199.<sup>2</sup> "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 rendezvous with Guggenberger (U-513), who had already been sunk.

#### 5. Possible rumors in the fleet.

The decision early in 1944 to supply U-boat base Penang with cipher data was accompanied with a warning of responsibility for security: "Breaking into the cipher aids would mean the greatest danger for the U-boat war." (1539/10 February 1944) Such a statement was not exceptional in itself, but it was noted with unusual interest here because of the increasing number of molested rendezvous'. Furthermore, talk

---

<sup>1</sup>The Atlantic Section's concerns were well founded. The entry in the War Diary of the Naval War Staff for 10 August 1943 states "A report from an agent in the USA states that for several months, the American's have allegedly been able to pick up our submarine radio traffic. Although this is very improbable, a most careful check and investigation is again being made." War Diary of the German Naval War Staff (Operations Division), Volume 48, Part A (August 1943), 135. Operational Archives/Naval Historical Center, Washington, D.C.

<sup>2</sup>Code messages from prisoners of war were furnished by OP-16-Z.

of cipher compromise was apparently making the rounds among U-boat crews. A prisoner (ex-Commander U-231, Wenzel) informed OP-16-Z interrogators in February that German Command feared cipher compromise as a result of the destroyer losses in the Biscay battle of December.<sup>3</sup> (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 prisoner of war story was possibly indicative, however, of rumors and gossip in the fleet. The distress of the U-boat arm would naturally have stimulated every sort of tale. In August 1944 prisoner of war coded messages protested that everything was known to the enemy and that there was treason in the highest places.

6. Sinking of the *Schliemann* and *Brake*, Indian Ocean cipher crisis 12 March 1944.

The only cipher crisis actually known through U-boat 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 March 1944)<sup>4</sup>

7. Sinking of U-IT-22.

---

<sup>3</sup>Presumably physical compromise.

<sup>4</sup>See note at end of chapter.

To make matters worse, German Naval High Command had that very morning received warning from B-Service that the Spahr-Wunderlich rendezvous 480 miles south of Cape Town, was being tampered with. 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 submarine 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-boats.

8. Examination of U-boat rendezvous, September 1943 - March 1944.

The rendezvous disturbances which occasioned this crisis were of course due to decryption. In an attempt to appreciate the problem as it might conceivably confront German Naval High Command, the Atlantic Section of OP-20-G examined the rendezvous traffic record for the period of September 1943 to March 1944, inclusive. Participating U-boats reported the presence of Allied forces in 21 of the 48 major rendezvous' 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 *Schliemann* and *Brake* within so short a period of time and in such a remote area, fears of compromise might have been 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 rendezvous with assurance. To meet this intolerable situation German Naval High Command 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 Studt (U-488), a refueler,

and the three submarines who were to refuel from him. At the same time their rendezvous position which had been ordered in a regular Offizier message of 10 March was canceled. The new rendezvous was to be assigned in a "Maske" message, which in consequence could be read by the Commanders of those four submarines and those four only.

On 16 March a similar procedure ("Schatten") was followed for a U-boat rendezvous in the Indian Ocean. In all, eight such special settings were sent out to various groups of U-boats during the next four weeks until all U-boats at sea had been reached. Aside from changing rendezvous 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.<sup>5</sup>

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

- (a) Physical compromise of U-boat ENIGMA with regular and Offizier settings.
- (b) Officer prisoners of war being interrogated immediately upon capture and revealing information about rendezvous.
- (c) Enlisted personnel having access to Offizier settings, "Bellatrix" system, and Offizier information with the attendant danger of (b) above.<sup>6</sup>

Support for this view seemed implied in such statements to U-boat Commanders as the following: "Strictest secrecy. Only officers to have access to information. No exceptions." A

---

<sup>5</sup>See Commander Roeder memorandum to G-1 of 23 March 1944.

<sup>6</sup>Prisoners of war had in fact accurately discussed the Bellatrix procedure. The information was not really necessary for the Allied cryptanalytic attack and made the Atlantic communication intelligence people worry about their own security problems primarily for fear that word of these interrogations results might get back to the enemy.

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 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 Abbasia, 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 as so very keen that anything untoward might put them on the true scent with dangerous repercussions."

#### 11. Confidence in U-boat cipher.

On the whole German confidence in the U-boat 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-boat special ciphers can be regarded as such.<sup>7</sup>

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

That the Germans were using their own communications intelligence results in an examination of the security problem was evident from an exchange of messages with Herwartz (U-843) during the period of the cipher alarm. Herwartz had been provisioned at the "Maske" rendezvous 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 rendezvous 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

---

<sup>7</sup>See paragraph 13 below.

state "if, when, and where you were observed by enemy before that date."

It was clear that German communications intelligence had decrypted a submarine estimate for 1200Z/30 (1300 German time) sent by Commander Fourth 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 (2221/8 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 submarine estimate, reckoning from the position Herwartz himself gave for the time of transmission. The Germans had to consider, however, that the submarine 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 U-boats of Allied skill in D/F-ing and presumably could not in this case eliminate D/F as the source of Allied information.

### 13. U-boat special ciphers.

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

It was believed at the time that the introduction of the 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-boats 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-boats that:

"Loss of U-boats 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 steckers, take out the wheels and disarrange them. Keep everything concealed in separate places. See further Standing War Order Number 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-boat war."

(Offizier 2107/2237/28 December 1944)

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-boats, that he attempts in every possible way to board U-boats . . ."

(2108/9 January 1945)

On the eve of surrender,

A U-boat 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-boat and board it, presumably in order to capture classified material." (Experience message #236, 1255/27 April 1945)

In April the compromise of the Reserve Hand Procedure for U-boats was announced, presumably as a result of shore station losses.

At last, on 8 May, it was announced that U-boat 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.

Concluding note:

From German Naval Attaché 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 rendezvous 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)