DOCID: 3560827

14250

TOP SECRET CREAM

SECRET
By Authority of the
Commanding General
Initials Date
OCT 01 1946

ARMY SECURITY AGENCY

Washington, D. C.

Declassified and approved for release by NSA on 06-01-2009 pursuant to E.O. 12958, as amended. Declass 58017

(EUROPEAN AXIS SIGNAL INTELLIGENCE IN WORLD WAR II)

AS REVEALED BY "TICOM" INVESTIGATIONS

AND BY OTHER PRISONER OF WAR INTERROGATIONS

AND CAPTURED MATERIAL, PRINCIPALLY GERMAN

(VOLUME 3--THE SIGNAL INTELLIGENCE AGENCY OF THE SUPREME COMMAND, ARMED FORCES)

Prepared under the direction of the

CHIEF, ARMY SECURITY AGENCY

1 May 1946

WDGAS-14

RESEARCH LIBRARY

TOP SECRET CREAM

DOCID: 3560827

~~TOP SECRET CREAM~~

VOLUME 3

The Signal Intelligence Agency of the Supreme Command, Armed Forces (Oberkommando der Wehrmacht/Chiffrierabteilung, abbreviated OKW/Chi)

Chapter I. Introduction

Chapter II. Organization

Chapter III. Intercept

Chapter IV. Operations

Chapter V. Relations with other Cryptologic Agencies

Tab A.

Tab B.

~~TOP SECRET CREAM~~

DOCID: 3560827

VOLUME 3: OKW/Chi

Chapter I. Introduction

Paragraph

Sources of information. 1

Notes on OKW/Chi before the war 2

1. Sources of Information. Before the TICOM teams began their investigation in Germany, it was known that the Supreme Command of the German Armed Forces (Oberkommando der Wehrmacht, abbreviated OKW) contained a signal intelligence section (Chiffrierabteilung, abbreviated Chi, hence OKW/Chi).[1] Pre-TICOM knowledge of the activities of OKW/Chi was very limited, but it was assumed that, as the highest echelon signal intelligence service, it would coordinate and perhaps direct the signal intelligence work of the Army, Navy and Air Force and would probably assemble the ablest cryptanalysts for attacks on systems with which the signal intelligence services of the separate branches were unable to cope. Consequently, OKW/Chi was given first priority among the TICOM targets.

By the time the TICOM teams began operations, OKW/Chi had left Berlin and had separated, as was learned later, into a northern and southern group. Shortly afterwards, most of their documents had been disposed of and most of the personnel had been swallowed up by one or another of the large prison camps hastily set up to receive the defeated German armed forces. Thence they were released into civilian life, often without leaving a trace in the records of the camps.[2]

[1] Within the organization of the OKW, the Signal Intelligence Section was subordinated to the Armed Forces Group (Amtsgruppe Wehrmachtnachrichtenverbindungen, abbreviated Ag. WNV). This department was in turn under the Armed Forces Operations Staff (Wehrmachtfuehrungsstab, abbreviated WFSt). The full abbreviation for the Signal Intelligence Section of the Supreme Command of the Armed Forces is, therefore, OKW/WFSt./Ag. WNV/Chi. The Germans ordinarily used the short form, OKW/Chi. For the sake of brevity, this form is used throughout the present paper.

[2] On TICOM's attempt to find some of these people in August 1945, see IF 167, p. 8.

There was no question, therefore, of capturing OKW/Chi as a group. A number of individual prisoners were taken who had once belonged to the organization or who knew something about its activities. Of these, three proved to be of outstanding importance:[3]

a. Col. Hugo Kettler was chief of OKW/Chi (Chef OKW/Chi) from the late summer of 1943 until the evacuation of Berlin by the unit in March 1945. Kettler impressed interrogators as an alert, intelligent officer. He had persuaded himself that, in view of the complete collapse of German arms, he could best serve his country by cooperating with the Western allies in an effort to rebuild Germany on a different basis. He was, therefore, willing to give any information desired, as far as he was able. His task at OKW/Chi was purely administrative. As a consequence, he was well informed on matters of charter, organization, number of personnel engaged, channels for commands and directives, liaison with allies and other German cryptological agencies. He was almost completely ignorant of the technical side of his unit's cryptological operations.[4]

b. Lt. Col. Mettig was second in command of OKW/Chi from December 1943 until immediately before the end of the war, when, as nominal head of the organization, he accompanied the German surrender party first to Flensburg and then to SHAEF Headquarters at Rheims. There he was taken into custody. Like Kettler, Mettig was a regular signal officer, who had occupied important posts in command of intercept and cryptological units. From November 1941 until June 1943 he commanded Inspectorate 7/VI of the Army High Command (OKH/In 7/VI). Between June 1943 and his arrival as second in command of OKW/Chi in December 1943, he had commanded the signal battalion of an armored corps on the eastern front (Armored Corps Signal Battalion 448). In addition to his duties as second in command,

[3]The most complete account of the finding of Kettler and Mettig and their reaction to interrogation will be found in Lt. Kirby's supplement to the report of Ticom Team 6, IF-165.

[4]Col. Kettler was interrogated 15 June 1945 and released(I-47).

Mettig had served in OKW/Chi as officer in charge of intercept. After the re-organization in November 1944, he became head of the cryptographic division. In general, Mettig's knowledge of the work of his organization was, like that of Kettler, the knowledge of an administrative officer. The interrogations of Mettig, however, were more numerous and more thorough than those of Kettler. Unlike Kettler, he was brought to the United Kingdom for detailed interrogation. Besides confirming what had already been obtained from Kettler, therefore, Mettig supplied, on matters of organization and of specific tasks accomplished or attempted, a great many details omitted by Kettler. His knowledge, however, like Kettler's, was principally of a non-technical sort. Mettig was truthful in so far as his statements could be verified, and many of them could be,[5] but he seemed to feel that his dignity as an officer would be compromised by over-eagerness to volunteer information.[6]

c. Specialist Dr. Erich Huettenhain was the chief cryptanalyst of OKW/Chi. Huettenhain had been with the organization from 1937 and had himself built up the section which he headed, personally selecting most of those employed in it. Huettenhain's section may be described as the cryptanalytic research section of the organization. It had a dual task. First, it attacked the more difficult enemy and neutral systems, those which were beyond the capacity of the routine breaking section which consisted mainly of linguists whose primary tasks were the breaking of unenciphered codes and translation. Second, it investigated the security of German systems and made suggestions to the cryptographers. Huettenhain was primarily not an administrator but a working cryptanalyst who had a detailed technical knowledge of the work of his section. He was, therefore, a valuable source of information on cryptanalytic techniques both manual and machine

[5]Below some instances are pointed out where Mettig's account fails to agree in minor details with certain information from other sources. Here it is a question of Mettig's memory rather than his veracity.

[6]Estimate of interrogators in I-78 and I-127; life history in I-78, details on OKW/Chi in I-96.

known to the organization. His position also makes his negative testimony of considerable value, since it is inconceivable that he should not have known of any considerable cryptanalytic accomplishment of the organization. Huettenhain was captured with Kettler, had discussed with him the ethical aspects of the question of revealing information to the western allies, and was in agreement with him that Germany could best be served by an attitude of complete co-operation. The interrogators considered him an honorable and truthful man. In addition, they came to have a high regard for his technical ability.[7] Before he was employed by OKW/Chi, Huettenhain was an academic mathematician whose interest in the problems of Mayan chronology led to an interest in cryptography and finally to OKW/Chi.

In answering the interrogators and in writing papers for them, Huettenhain was always assisted by Technician (Lieutenant Grade) Dr. Walther Fricke. Fricke was a mathematician of some distinction who had been drafted into the Signal Corps and assigned to the Signal Intelligence Service of the Army. Here he came to specialize in the development of German Army ciphers. With his unit, Inspectorate 7/VI of the Army High Command, (OKH/In 7/VI) he was taken into OKW/Chi in November 1944 where he continued his former work on German Army ciphers, but added to it the broader task of assisting Huettenhain and others in the work of revising the security of the German Armed Forces -- a work which had become the primary task of OKW/Chi.[8] In many of the interrogation reports it is impossible to distinguish between the contribution of Fricke and that of Huettenhain. It is a pretty safe assumption however, that in regard to the work of OKW/Chi, Fricke contributed little or nothing that Huettenhain could not have supplied.

[7]This estimate is based on oral statements of the interrogators. Important interrogations are report and "homework" translated in I-2, I-31, I-84.

[8]Fricke's career is described in I-20, 2. His capture and a view of his personality is reported in IF 166.

Compared to Kettler, Mettig, and Huettenhain, the other prisoners taken were of secondary importance, although in some cases they were able to fill out the picture obtained from the principal informants. Mrs. von Nida, the wife of one Major Wolfgang von Nida, officer in charge of the OKW/Chi intercept network in Spain from January 1940 until April 1942 and second in command of OKW/Chi from that date until his death in November 1943, supplied a considerable amount of picturesque detail and some information on the intercept picture in Spain, where she had lived during part of her husband's tour of duty. She also supplied a few shrewd details that throw some light on the relation between officers and civilians and on the general efficiency of the Berlin section of the unit.[9] A considerable amount of information about the intercept station at Lauf near Nuremberg was supplied by three prisoners who were intimately associated with it: Specialist Flicke, in charge of the technical side of the work previous to the autumn of 1944, Technical Inspector Kurt Pokojewski, Flicke's subordinate and later his successor, and [Staff Director) Heinrich Hatz, in charge of administration.[10] The work of at least one of the language desks, the Japanese, is well known because a number of prisoners who formerly worked there were interrogated: Messrs. Grosse, Hierer, Rave, and Schroeder had been detached from OKW/Chi to the Foreign Office Cryptanalytic Section (Pers ZS) and were captured with the members of this section.[11] Cpl. Heinz W. Beyreuther, who was in the Japanese sub-section of OKW/Chi since 1941, supplied a written account of his work and associates. He also gave some valuable details on the later history of the organization.[12] Acting Cpl. Reinhard Wagner, who had worked at the Japanese desk since 1941, was made the subject of a special interrogation.[13] Dr. Werner Weber, one of the mathematicians assigned to Huettenhain's section, but working in close collaboration with the Japanese desk, supplied some

[9] I-49 is a paper by Mrs. von Nida which reached TICOM through intelligence channels. I-105 is a later TICOM interrogation aimed at clarifying the paper.

[10] I-85.

[11] I-22, 8. and I-1,11 et passim.

[12] I-150.

[13] I-90.

details about his work as well as a few things about the research section which Huettenhain had forgotten to mention.[14] On the special problem of OKW/Chi work on ciphony some information was given by S/Sgt. Dr. Otto Buggisch, who was one of the leading Army cryptanalysts. He had been transferred to OKW from the Army in November, 1944 and his work with OKW/Chi was simply an extension of his work with the Army.[15] Dr. Werner Liebknecht, an employee of Army Ordnance Development and Testing Group, Signal Branch (WA Pruef 7), had worked with Huettenhain and Fricke on the practical engineering problems involved in the production of cipher devices. He substantiated the information supplied by Huettenhain and Fricke and supplied a few details omitted by them.[16] Col. Randewig furnished the information on the signal intelligence activity of Armed Forces Signal Officer for Special Employment, Number 700 (Wehrmachtnachrichtenfuehrer z. b. V. 700).[17] This activity was connected with the OKW but had no relation to the activity of OKW/Chi. Rudolf Trappe and the dim light he shed on the obscure problem of the pre-war activity of OKW/Chi is discussed below.

The picture obtained from prisoners can be supplemented and verified, at least in part, by a number of documents now available. Of these documents, three are of the first importance for questions regarding the charter, organization, and history of the organization. They were found in the Chasseurs' Barracks (Jaegerkaserne) in Strub near Berchtesgaden and formed part of the personal files of General Staff Major Nielsen, operations officer on the staff of the Chief Signal Officer, Supreme Command of the Armed Forces (OKW/WFSt./ Chef WNV, Ia.). The documents are:

d) An unsigned document with the heading "Order of Battle of OKW/Chi." This is a brief description of the organization of the unit with the names of the heads of sections. It is undated, but its position in the files is stated

[14] I-124.

[15] I-46, 2.

[16] I-46, 2. and I-57.

[17] I-68.

to indicate a date of approximately April 1945. Translated at Government Code and Cypher School, it was first published as one of their publications.[18] Later the document was discussed with Kettler, and a revised version issued by TICOM.[19]

e) A document with the title "Activity Report of OKW/Chi, 1/1/ 44--25/ 6/44," dated 27 June 1944 and signed Kettler. This is a brief outline of the unit's charter and activities during the Spring of 1944.[20] It was evidently prepared for presenting to Kettler's superiors, probably the Chief, Armed Forces Communications Group (Chef Ag. WNV) and the Chief Signal Officer, Armed Forces Supreme Command (Chef WNV). It is referred to henceforth as the "Kettler report".

f)An order dated 5 September 1944, signed Fraun, subject, "Coordination and Allocation of Cryptanalytic and Cryptographic Work." Fraun was the Chief Signal Officer, Armed Forces Supreme Command (Chef WNV). The document was translated and published as TICOM D-55. The German original was (fortunately) also published.[21]

In addition, there is available a group of captured documents of uncertain provenance assigned the TICOM No. T 1620. The character of these documents suggests that they are from the personal file of a section head in OKW/Chi, in all probability Huettenhain. There are various official bulletins and directives on personnel matters, air-raid precautions, etc., minutes of meetings, correspondence and other documents on security matters. The material throws a considerable amount of light on the cryptographic and security activities of the organization during the winter 1944-1945.[22]

[18] DF-8.

[19] I-29.

[20] TICOMMA file number DF-9.

[21] Filed with D-55. Original TICOM Number is T-4503.

[22] Some of the documents have been translated in D-57 (where the TICOM number is erroneously said to be 1650). The documents are stated to have been received by TICOM in October 1945 from C.I.C. via S.I.D. USFET.

The great bulk of the OKW/Chi documents, the archives of the unit, which consisted principally of broken messages and reports based on broadcast interception, are known to have been moved from Berlin to Lauf near Nuremberg in the spring of 1945. From there, they were brought to the Schliersee south of Munich and, when it became evident that high level signal intelligence work was no longer possible, they were boxed and dumped into the lake. A waterproof box with some of these documents was recovered in July 1945 by accident and eventually taken over by TICOM. It contained a number of translations of decoded messages and some miscellaneous material,[23] among which the most important was a file of correspondence between OKW/Chi and its intercept stations covering the years 1939 to 1945.[24] Other boxes were recovered in September 1945 by American divers operating under the direction of TICOM,[25] but the material therein was not of such nature as to expand our understanding of the workings of OKW/Chi.

From the material available, a fairly clear general outline can be extracted of the charter, organization, and major cryptanalytic and cryptographic operations of OKW/Chi during the war and particularly during the last two years of the war. For charter and organization, the Chief of OKW/Chi and his second in command were available for questioning and their statements could be verified by the Nielsen documents. For operations, the chief witness was Huettenhain, whose position was very central. As head of the section composed of the organization's outstanding cryptanalysts, he was personally concerned with all the more difficult cryptanalytic problems faced, both in attacks on enemy systems and in security scrutiny of German systems. It is almost certain that no major cryptanalytic successes were achieved without his knowledge. Of the low-grade successes achieved by the unaided efforts of the language desks, however, --even when these had considerable intelligence value-- he knew little and seems to have cared less. Consequently, our information on minor successes and the intelligence obtained from them is scanty. Fenner, who was head of the routine breaking and translation; von Kalkstein, who had

[23] A-13 contains a complete list of the contents.

[24] T-804.

[25] IF-167.

charge of the evaluation and routing of broken messages; and Schädel, who was head of the archives and in touch with the intelligence picture; could, if found and interrogated, supply considerable valuable information on such details.

2. Notes on OKW/Chi before the War. The pre-war history of OKW/Chi (and its shadowy predecessor) cannot be reconstructed from TICOM material. Of the important prisoners interrogated, only Huettenhain, who joined the service in 1937, was connected with it before the war. Principal Specialist Fenner was with Chi from the beginning and wrote a "History of the Cipher Section" (Geschichte der Chiffrierabteilung) in the winter of 1944-1945. Unless Fenner can be found and interrogated or his history picked up, any treatment of Chi before the war must be confined to a few brief notes developing hints supplied by Huettenhain and Mettig.

According to Mettig, the germ of what later became OKW/Chi is to be found in a "section" of the German Defense Ministry (Reichswehrministerium) formed in 1920 and staffed by cryptological personnel from World War I.[26] This section was organizationally part of Military Intelligence (the Abwehr).[27] Presumably when OKW was formed, it took over Military Intelligence (the Abwehr) from the German Defense Ministry, now called German War Ministry (Kriegsministerium) and with it the cryptologic "section". With the setting up of the Armed Forces Communications Group (Ag/WNV) within the OKW, however, the "section" was taken from Military Intelligence (the Abwehr) and transferred to the Armed Forces Communications Group (Ag/WNV).[28] As will appear later, traces of the old connection with the Abwehr remained.

Huettenhain stated that when he entered OKW/Chi in 1937 he found 40 cryptanalysts headed by Fenner who were known as the "cipher party" and organized as Referat G.[29] Referat is the word used for the smallest unit in the German administrative hierarchy, roughly equivalent to our "sub-section" or "desk". It is unlikely, therefore, that Fenner's Referat G

[26] I-96, 2.

[27] I-86, 2.

[28] I-96, 2.

[29] I-36, 3.

was co-extensive with the cryptological "section" mentioned by Mettig. It was only part of it, but probably the most important part.

We know by name only a few of the earlier members of Referat G. The head of the Referat, Principal Specialist Fenner, later emerges as one of the most important figures in OKW/Chi during the war. Of the early Fenner little is known. That he was primarily interested in the linguistic rather than the mathematical side of cryptanalysis is suggested by his later position as head of the language sections as well as by the fact that Huettenhain was charged with developing the mathematical side of the work. He was, according to Cpl. Beyreuther, born in Petersburg and was thoroughly acquainted with Russian.[30] An early interest in cryptography as well as cryptanalysis is suggested by the fact that in the Nineteen-twenties he assisted one Willi Korn in developing the Enigma.[31] Fenner was apparently valued for his long experience in signal intelligence work and the valuable connections he had made for the organization. He is never praised as a cryptanalyst. One of his directives is found in the TICOM 1620 collection. It lays down grammatical rules to be followed by translators. Perhaps this evidence is too slight to warrant the suggestion that he was a somewhat pedantic type of person.

In any case, the low opinion of the work of Fenner and his colleagues expressed by the second known member of the organization need not be taken too seriously. This member was Principal Specialist Schapper, who later fell into TICOM hands as the head of Goering's "Research" Bureau. According to Mettig, Schapper had once been Fenner's subordinate.[32] Schapper had a somewhat different story. In the Autobiography which he wrote out for the benefit of his interrogators Schapper stated that from 1927 to 1933 he had been in Berlin as "Administration Officer and head of department in the Cryptographic Bureau of the Reichswehr Ministry." He resigned in 1933 "as I could not agree with the thoroughly incompetent methods of the Cryptographic Bureau."[33] Earlier

[30] I-150, 2.

[31] I-84, 2.

[32] I-131, 3.

[33] IF-15, (Report of TICOM Team 1), p. 23.

Schapper had made it clear to the interrogators that not only he but several colleagues had left the Bureau to propose to Goering the establishment of a new intelligence agency. "Head of department" seems a rather elaborate description of Schapper's position if he was really subordinate to Fenner whose sub-section contained in 1937 only 40 people. On a matter involving his vanity, Schapper is perhaps not a reliable witness. On the other hand, Mettig may very well be mistaken, and it is possible that Schapper was not a subordinate of Fenner, but his equal and head of another Referat in the section.

In 1935 Senior InspectorMenzer joined the organization. He is described as an old Regular Army man with little formal education. He had a natural aptitude for cryptologic work, however, and previous to 1940--41, he was wholly responsible for security.[34] His interest seemed to lie in developing cryptographic and later cryptanalytic devices.[35]

Huettenhain appeared in 1937. He spent about a year in training and then was ordered to expand the mathematical side of the cryptologic work. Huettenhain believes that Fenner was responsible for this policy.[36] It was, in any case, a good if somewhat obvious one. Huettenhain evidently used his acquaintance with German mathematical circles to advantage. He introduced into the organization five academic mathematicians, Professors Aumann, Witt, Franz, Weber, and Schultze, and a mathematically interested physician, Dr. Aigner.[37] These men remained with the organization until the end, and formed the backbone of its cryptanalytic work, both in attacks on enemy systems and in security scrutiny.[38]

[34] I-31, 3.

[35] I-31, 16.

[36] I-31, 2.

[37] I-31, 2. Weber later told interrogators that at first he worked at Chi as a Private First Class (Gefreiter). Witt and Aigner were also enlisted men as appears from a note from Huettenhain to Kempf complaining that these key cryptanalysts were overburdened with company duties. (T 1620).

[38] I-123.

A few things can be surmised about the early charter of operations of Chi, or at least of that part of it subordinate to Fenner. Some strictly cryptographic work was done, particularly in the development of systems for Military Intelligence (the Abwehr) and, perhaps, for the army. Fenner's early interest in the Enigma may be one instance of this. Huettenhain states that for some years previous to 1939 there had been a section where "our own codes and cyphers were developed and tested."[39] This section was in all probability under Menzer who was solely responsible for security[40] previous to 1940--41. Huettenhain himself made his acquaintance with OKW/Chi as an amateur cryptographer. His studies in Mayan chronology had inspired him to devise a cryptographic system which he submitted to the "local military authorities". Huettenhain's system was forwarded through channels and eventually found its way to OKW/Chi.[41] This happened in 1937, and is a clear indication that Chi was regarded as the chief authority on security matters at that time.

It is pretty certain, however, that Chi's early mission was primarily to attack the cryptographic systems of foreign nations. The 40 cryptanalysts whom Huettenhain found working under Fenner in 1937 were apparently mainly linguists organized into language desks and getting along without the assistance of professional mathematicians. Between 1937 and 1939 systems of the following countries were under attack: England, U.S.A., France, Holland, Belgium, Switzerland, Russia, Rumania, Bulgaria, Italy, Poland, Czechoslovakia, and Yugoslavia.[42] OKW/Chi's charter is said to have been originally confined to the Armed Forces systems of foreign countries. The Foreign Office Cryptanalytic Section (Pers ZS) handled diplomatic material. On the plea that it needed more material to train

[39] I-36, 3. The context makes it almost certain that this "section" was a part of Fenner's Referat G. In 1940--41 security scrutiny was made the work of a separate section.

[40] I-31, 3. See also I-161, 4.

[41] I-31, 2.

[42] I-36, 3.

cryptanalysts, OKW/Chi took over diplomatic systems also,[43] thus duplicating the work of the Foreign Office. Once having taken these systems over, Chi refused to abandon them.[44] Just when this extension of OKW/Chi's charter took place is unknown.[45] Chi was definitely committed to diplomatic material by 1937.[46] In 1939, the Army intercept stations at Lauf and Treuenbrietzen were given the task of intercepting diplomatic traffic exclusively and were subordinated directly to OKW/Chi.[47]

At the beginning of the war, then, Fenner's section, Referat G, seems to have had at its disposal the following personnel:

> A group of linguists with some cryptanalytic experience.
>
> A group of mathematicians who had been spending the past year familiarizing themselves with cryptologic problems. In 1939, the mathematicians were given a status apart from the linguists and put to tasks such as stripping encipherments from codes.[48]

[43]It is perhaps a safe guess that the dearth of material for training purposes in OKW/Chi was caused (1) by expansion of the service incident to increased militarization and preparation for war and (2) by the assignment of cryptanalytic work on enemy service systems to the separate Branches of the Armed Forces. See Tab "B" below on early relations between the cryptanalytic effort of OKW and of the Army (OKH).

[44]This information came from Karstien, a member of the Foreign Office Cryptanalytic Section (Pers ZS) who felt very strongly against OKW/Chi. (I-22, 9.)

[45]According to one informant (I-62, 5--6) the intercept station at Treuenbrietzen, which was already operating in 1933, in the days of the Reichswehr, specialized in intercepting diplomatic traffic. It is possible that not all this traffic was routed to the Foreign Office and that the Reichswehr predecessor of OKW/Chi had worked on such traffic. In adding diplomatic material to its official commitments, therefore, OKW/Chi was merely expanding a foothold it already had in the cryptanalytic domain of the Foreign Office.

[46]I-31, 10.

[47]I-85, 2 and 3.

[48]I-36, 3.

Menzer, who now had about four years experience in devising cryptographic procedures and devices. He probably had some assistants.

There is no information on the total number of personnel at this time. There had probably been considerable expansion since 1937 when the Referat numbered only about 40.

In 1939 there seem to have been some organizational changes within OKW/Chi. Referat G was upgraded to a section and called Section IV.[49] This implies the existence of sections I, II, and III, but what they did can only be conjectured on the basis of what we know about their later tasks. In general, it is probable that OKW/Chi already had in 1939 the organizational structure and tasks which were to characterize it until the changes of the summer of 1944.

[49] I-36, 3.

Chapter II. Organization Paragraph

Organization from 1939 until the Summer of 1944. . . . 3

Organization from the Summer of 1944 until March 1945. 4

The Disintegration of OKW/Chi. 5

3. Organization from 1939 until the summer of 1944. A solid basis for an understanding of the charter and organization of OKW/Chi in the years from 1939 to 1944 is afforded by Kettler's activity report for the period 1 January to 25 June 1944. From this report the bifurcated character of the organization, reflecting a two-fold mission, is clearly evident. Kettler starts his report by stating that Chi's mission is to intercept and interpret two classes of traffic:

International wireless traffic of enemy and neutral states (enciphered and unenciphered telegraphic communications of diplomats, military attaches, government authorities, economic authorities, etc.)

Radio-telephone transmissions of enemy and neutral states; enemy and neutral commercial wireless transmissions of the major wireless stations and of the wireless news service.[56]

The first part of the mission was high-level signal intelligence work as it is understood in the United States. The second part was essentially the work of a broadcast or news monitoring service.

The organization set up to accomplish this two-fold mission, as it may be deduced from the remarks in the Kettler report, is outlined in chart No. 3-1 . The main work of the service was divided among four sections. Chi I controlled the intercept of class 1 traffic. The job was principally one of liaison. The head of the section was briefed by the head of OKW/Chi who was aware of intelligence requirements. He was also in contact with the cryptanalysts, who knew what they could break. On the basis of this information he gave instructions to the intercept stations. The section was evidently considered important since it was headed by an important officer. Lt. Col. Andrae, who later became second-in-command of the Army Signal Intelligence Agency, was head of Group I

[56] DF-9, 1.

until he was replaced by Major von Nida, who was recalled from his position as head of OKW intercept in Spain for the purpose.[57] Mettig, who had formerly been chief of the Army Cryptanalytic Service, replaced von Nida in December 1943.[58] The Head of Section I (Gruppenleiter I) was also operational head of the service.[59]

The raw material from Chi I's intercept stations was passed on to Chi IV for breaking and translation. This was Fenner's section, the descendant of Referat G, and the most important section of the service from an operational point of view. Kettler's report mentions no sub-sections, but something about the internal organization and division of labor within the section is known from other sources.

The bulk of the personnel in the section were linguists, engaged on code-breaking, removal of simple encipherments, and translation. The linguists were organized into small groups or desks.[60] In 1942 all the desks were lumped together in a subsection called IVb[61] and the desks were given arabic numbers, e.g. IV b 1, etc. The total number of desks increased to 22 in the course of the war but they were never all occupied simultaneously.[62] A desk was, of course, kept in existence only so long as the material was being read and the linguists could be kept usefully occupied.

[57] In I-49, 3, this is said to have been in April 1943; in I-105, 2, in April 1942. Since both publications are reporting statements of Mrs. von Nida, there is no criterion for preferring one or the other date.

[58] I-96, 2.

[59] This at least was Mrs. von Nida's opinion (I-105, 4). Mettig describes himself as "deputy to the Chief OKW/Chi" (I-96, 3).

[60] Called Laendergruppen by Trappe (I-123,3), Referate by Beyreuther (I-150,2).

[61] I-36, 3.

[62] The number is mentioned independently by Huettenhain (I-36, 3) and Mettig (I-96, 3).

Huettenhain and his mathematicians occupied a special position within Section IV from 1939. They were apparently organized into a desk on the same structural level as the individual language desks. In 1942, Huettenhain's people were upgraded to a sub-section and called IVc. This change was doubtless a recognition of the growing importance of their work. Mathematical work and linguistic work were now organizationally on a level. The mathematicians were a research group. Their job was to make the initial break into more difficult ciphers. When the breaking became routine, the work was handed over to the appropriate language desk. If continued expert cryptanalytic assistance was necessary, one or more members of IVc might be permanently detailed to assist a language desk, as Weber seems to have been in the case of the German attack on Japanese transposition systems.[63]

In addition, section IV contained a sub-section devoted to cipher development and security scrutiny. After 1941, Huettenhain was in charge of this sub-section and Menzer, who had formerly been in sole charge of development and security, was attached to it.[64] Just what the organizational status of this sub-section was is not clear. It may have been a desk subordinate to Chi IVb or it may have been a wholly independent subsection perhaps known as IVa, the existence of which is implied by the existence of IVb and IVc.

In connection with security scrutiny, a sub-section for developing cryptanalytic machinery was introduced in 1942 when two graduate engineers, Rotscheidt and Jensen, three working engineers and twenty-five mechanics had been hired. Where this group fitted into the organizational structure is also unknown. Almost certainly, it was ultimately subordinate to

[63] I-124, 3.

[64] The precise historical development is obscure. For some years previous to 1939, Fenner's Referat had contained a "section where our own codes and cyphers were developed and tested". (I-36, 3). Menzer was apparently in charge of this section (I-31, 3; I-161,4). In 1940, a special section was formed for security scrutiny (apparently without development) "to test new service systems and check on old ones." (I-31, 3). This section was "later" under Huettenhain. (I-31,3). Before the reorganization of 1944, however, Menzer was attached to Huettenhain (I-21, 4), so that at some time his security section must have taken over development as well.

Huettenhain and worked in close collaboration with the research sub-section in attacks on enemy systems. After the re-organization in 1944 it emerges as a separate sub-section in Huettenhain's research section.

Whatever the organizational details may have been, it is certain that attacks on more elaborate enemy cipher systems, security scrutiny of German ciphers, and development of cryptanalytic devices were carried on in very close connection with each other and were all under the supervision of Huettenhain. Kettler's report also mentions some training activity, and it is likely that this too was carried on in Chi IV and that Huettenhain had a hand in it.

After messages were broken and translated by Chi IV they were passed on to a section called in Kettler's report Chi "X". Its task was to evaluate the material from an intelligence point of view. Unimportant items were rejected and the others routed to the proper recipients. This work was done by a single officer, Lt. Col. von Kalkstein, and a few assistants.

In the handling of news and broadcast monitoring, Chi II occupied a position analogous to Chi I's position in the intercept of government traffic. But it was somewhat differently organized. Whereas Chi I was primarily a liaison organization maintaining contact between headquarters and the intercept stations which had their own organizational existence, Chi II actually was the intercept organization. It controlled directly the personnel of the main intercept station at Ludwigsfelde and of the subsidiary stations.[65] This difference was probably the result of the difference in the intercept technique involved. The broadcasts picked up at Ludwigsfelde and the outstations were carried by line to Berlin and recorded there, usually by typewriter. They were then translated immediately. The material thus gathered was processed by Chi VI, which was staffed principally by personnel with newspaper experience.[66] On the basis of the foreign broadcasts, a daily news summary was prepared. In addition special reports on various subjects were sent periodically to departments which had regular use for them. Chi III originally did its own distribution. On the broadcast side of the

[65] DF-9, 1.

[66] I-96, 16.

organization, there was no department equivalent to Chi "X", which, as Kettler's report makes clear, sorted only material from Chi IV.

The only operational connection between the two sides of the organization was afforded by the Archives. Here copies of the broken and translated messages and of the broadcast reports were filed and presumably indexed. The accumulated material was available to the code-breakers and others in Chi IV. Later on, the Archives with its chief, S/SGT. Dr. Schaedel, seems to have been subordinated to von Kalkstein's distribution section. At an earlier date, it was under Fenner.[67] The Kettler report of June 1944 does not make it clear what the situation was at that time.

It is probable that this dual nature of OKW/Chi characterized the organization since the outbreak of the war. Already in 1939, Fenner's group had been named section IV. This implies the existence of sections II and III. It is probable that they were engaged in broadcast monitoring and news analysis from the beginning. Whether the pre-war Chi had a similar service is unknown. If Fenner's Referat before the war was Referat G, Referate A--F must have existed. Perhaps some of these Referate were engaged in news and broadcast monitoring.

Besides OKW/Chi's split personality, another fact emerges clearly from the Kettler report, namely that, in so far as its activity is expressed in its organizational structure, OKW/Chi is primarily an agency for gathering intelligence. It is true that a certain amount of development and security work had always been done. The original charter for security and development is obscure, but since the Army, Navy, and Air Force was each responsible for its own security and development, the only definite commitment of OKW/Chi seems to have been to develop ciphers for the agents of Military Intelligence (the Abwehr) and for some government agencies. No special interservice systems seem to have been used. The separate branches were free to submit their systems to OKW for security scrutiny, but originally there was no obligation to do so. This situation was partly changed by an order of Keitel, as Chief of OKW, issued in October 1943 to the effect that no new ciphers could be introduced by any branch of the Armed Forces or

[67] I-96, 16.

government agency "without the prior consent of OKW/Chi".[68] Chi obviously made some efforts to meet the increasing demands for security work, as is evident from the setting up of the security sub-section within Chi IV and the introduction of the machine development group, largely for security purposes, but this work was buried organizationally and perhaps operationally within Chi IV whose principal mission remained that of producing intelligence. The organization as a whole remained an intelligence organization. The pre-war connection with Military Intelligence (the Abwehr) was still apparent in its structure.

It was apparent in other ways too. The regular chain of command was through the OKW signal authority, Hitler -- Keitel (Chief, OKW) -- Jodl (Chief of the Operations staff) -- Thiele (Chief, Armed Forces Communications Group (Chef Ag WNV)-- Kettler (Chief of OKW/Chi). In practice this channel was little used for passing on operational directives. Ordinarily, Fellgiebel was by-passed, and Kettler received his briefing and directives not from the Signal authorities but from the Chief of Military Intelligence (the Abwehr). The briefing seems ordinarily to have consisted of a general outline of the intelligence picture and some suggestions as to the part OKW/Chi was intended to play.

[68] The wording of the original order may have been ambiguous. At a conference held 27 October 1944, the navy representative, Krauss, said, "The Navy refused to allow OKW/Chi .... to forbid the use of a system in a certain place. OKW/Chi's recommendations can only lay down the limits within which it is possible to use a system. The responsibility for whether and where the system will be used must remain with the Navy." Gimmler replied, "According to the order of the Chef OKW 2000/43 Top Secret of 21/10/43, the approval of OKW/Chi is required." (D-57, 14). By the following meeting, however, held on 15/11/44, Gimmler seems to have consulted the order and stated that "according to the Keitel order, the consent of Chi must be asked for before the introduction of a new code or cipher. The decision on the introduction rests with the sections of the Wehrmacht." (D-57, 5). It is odd that the Praun order of 5 September 1944 was not mentioned in this connection.

A further testimony to the strength of the old connection with Military Intelligence (the Abwehr) was the fact that Chi V, which was in charge of the teleprinter connections between Chi I and the Intercept Stations, had the additional (and apparently larger) commitment of providing and maintaining a teleprinter system for the Military Intelligence (the Abwehr).

4. Organization from the summer of 1944 until March 1945. Events during the summer of 1944 resulted in a fundamental change in the official interpretation of OKW/Chi's mission and a corresponding change in the organizational structure. These events centered around the attempt on Hitler's life on 20 July 1944. General of Signal Troops (Lt. Gen.) Erich Fellgiebel, Chief Signal Officer of the Armed Forces and also of the Army was deeply involved in the plot. He was dismissed in disgrace from the Armed Forces on the following day and was later executed. Some of the leading figures in Military Intelligence (the Abwehr) were also involved. As a result, Military Intelligence (the Abwehr) was taken away from the Supreme Command of the Armed Forces and transferred to Himmler's Main Reich Security Office (RSHA). Here it became the "Military Department" ("Mil. Amt") and was subordinated to SS Brigadier Gen. Walter Schellenberg who was already head of the Foreign Security Service (SD Ausland) which was Department VI of the Main Reich Security Office (RSHA).[71]

OKW/Chi became a prize for various National Socialist leaders whose ambition was whetted by the opportunities afforded by the rescrambling. Goering's "Research" Bureau, a safe party organization whose activities duplicated almost completely those of OKW/Chi, made an effort to asorb its rival.[72] Goering's people could point to the political unreliability of OKW/Chi which had been under the traitor Fellgiebel and closely associated with the abolished Military Intelligence (the Abwehr) as well as to the desirability of combining activities and thus

[71]See I-86, 2; I-96, 4; and IF-164, 1. (If-164 is an interrogation report on Schellenberg, without title page but, to judge by the language, of British origin.)

[72]Thus Mettig in I-96, 4, and I-86, 2. In I-131, 3, Mettig says it was only the broadcast and news-monitoring activities of OKW/Chi that the Research Bureau wanted to take over.

conserving manpower, a commodity in increasingly short supply. The ambitions of the "Research" Bureau, however, were defeated by Schellenberg, whose grandiose schemes for a central German intelligence agency called for control of all high-level cryptanalytic work including both OKW/Chi and the Research Bureau (FA).[73]

The immediate reaction of the leaders of OKW/Chi is somewhat obscure. Fellgiebel's second in command, Brig. Gen. Thiele, took over the assignment of Chief Signal Officer of the Armed Forces and the Army. Thiele's old position as second in command and head of the Armed Forces Communications Group (Ag/WNV) was filled with Maj. Gen. Gimmler, who had been Chief of Army Ordnance Development and Testing Group, Signal Branch (Wa Prüf 7) in the Army Ordnance Department (HWA). Kettler continued as chief of OKW/Chi with Mettig as his second in command. According to Schellenberg's story, most of these officers were in accord with his schemes. Thiele was an old friend of his. They had at one time both been on the Board of Directors of the Standard Electric Company. Thiele was completely sympathetic with Schellenberg's schemes to unite all high-level cryptanalytic services and put them at the disposal of Schellenberg. After Thiele was arrested for his part in the July plot, Kettler continued to seek close contact with Schellenberg. When OKW/Chi evacuated Berlin, Kettler modeled his evacuation measures on those of Schellenberg "because he had always thought, just as Gimmler had done, that Schellenberg by taking over the Forschungsamt [Goering's Research Bureau] would acquire decisive influence over the deciphering department."[74]

Now Schellenberg is not a reliable source of information on the affairs of OKW/Chi. Cryptanalysis was, of course, only a very small corner of his vast field of interest. Besides, he tends to confuse his magnificent schemes with actual accomplishments. There is, for example, no evidence that Kettler modeled his evacuation plans on those of Schellenberg, but the core of truth in Schellenberg's remarks on the subject is perhaps to be found in Mettig's statement, made of course quite independently and in an entirely different connection, that there was a plan to accomodate some of the OKW/Chi personnel,

[73] IF-164, 7. See also the proposed organization at the end of the report.

[74] IF-164, 7.

those directly concerned with ciphers of the Reich Main Security Office (RSHA), in one of the latter organization's headquarters. This plan was not adopted because the Reich Main Security Office (RSHA) could not furnish the transport to move the Chi personnel when Berlin was evacuated.[75] It is likely too that there was similar exaggeration in Schellenberg's claim to enthusiastic support from the heads of OKW/Chi for his plans to absorb the organization. The chief result of the disappearance of the old Military Intelligence (Abwehr), indeed, seems to have been a marked loosening of OKW/Chi's ties with military intelligence. Huettenhain and Fricke stated that Kettler never saw Schellenberg after 20 July, the date of the attempt on Hitler's life.[76] Mettig, who was in a better position to know, said Kettler saw Schellenberg only five or six times--presumably for briefing on intelligence matters.[77] It may be true that when Thiele was arrested and the plans of Goering's Research Bureau (FA) to take over OKW/Chi reached a climax in the early autumn of 1944, Kettler and Mettig welcomed the protection of Schellenberg as the less of two evils.

Meanwhile, the development of OKW/Chi was in quite a different direction -- away from intelligence and towards cipher security as the main task of the agency. Doubtless the moving spirit in this change was Major General Gimmler. The Army Ordnance Development and Testing Group, Signal Branch (Wa Prüf 7) which Gimmler had formerly headed included a section for directing the production of cipher devices. He is known to have had very marked opinions on the purpose of a signal intelligence service. Huettenhain and Fricke give what is obviously an unsympathetic account of these opinions:

> He [Gimmler] gave a sort of standard lecture to various groups at various times. His approach was that of the Officer-layman. He had no technical knowledge and no one could tell him anything. His speech began something like this: "I will make Chi an orderly organization.

[75] I-96, 22.

[76] I-84, 3.

[77] I-86, 2. Compare I-96, 4.

> Before this, it has not been so. We must have three pillars in our work: Development, Security, Cryptanalysis." Then he would expound his views on the relation between these three. The head of the first branch must be an Officer, who would know what the troops need. The second could be left to a civil servant. It is the most important of the three, and the other two exist primarily to fertilize it. He considered cryptanalysis very unimportant in itself.[78]

While Thiele was still Chief Signal Officer, Gimmler made plans to put his ideas into operation. Huettenhain and his mathematicians were upgraded to a separate section and a series of monthly conferences under Huettenhain was inaugurated. These conferences were to be attended by representatives of all the branches of the Armed Forces and the SS. Their purpose was to co-ordinate all work on cipher security in Germany.[79]

Meanwhile, Thiele himself was relieved of his command and imprisoned. He was replaced by Maj. Gen. Albert Praun. Praun had been a divisional commander, and Gimmler's ideas on a signal intelligence service whose primary mission would be to furnish practical and secure ciphers for the use of troops in the field probably appealed to him. Also, he seems to have had no connection with Schellenberg, who now represented the intelligence, and hence, cryptanalytic point of view.[80] Finally, the whole cryptographic service of the Army had fallen under political suspicion. Gimmler seized his opportunity to push his theories into action. The old orientation of OKW/Chi was towards intelligence. The new was to be towards security. The new orientation is most clearly apparent in an order dated 5 September 1944 and signed by Praun.[81] Concerning cryptanalysis there is little change. Army, Navy, and Air Force are to attack the systems of their enemy counterparts as heretofore. This leaves diplomatic and military attaché traffic as

[78] I-84, 2.

[79] I-96, 13. I-84, 4.

[80] IF-164, 7. Schellenberg could not recall his name.

[81] D-55.

the cryptanalytic sphere of OKW/Chi.[82] It is emphasized, however, that the separate branches are to adhere strictly to material within their competence and to pass on to OKW/Chi all other material. They are further ordered to acquaint OKW/Chi with all cryptographic systems under study or solved. In short, the old cryptanalytic charter is restated. In addition, OKW/Chi is made a sort of clearing house for cryptanalytic information obtained by the separate branches of the armed forces.

With regard to cipher development and security scrutiny, however, the charter and authority of OKW/Chi is enlarged. In so far as Praun could accomplish it, OKW/Chi was turned into a central authority for these matters. For the Army, this could be done thoroughly. The Army had no influential party members like Goering or Doenitz to protect its operations, and besides, Army cryptographers had been deeply involved in the 20 July plot. Originally, the Army had a section devoted to cipher production and development (Inspectorate 7/IV (In 7/IV) and, in addition, some personnel in Inspectorate 7/VI (In 7/VI) were employed on security scrutiny. All of Inspectorate 7/IV (In 7/IV)and the personnel in Inspectorate 7/VI (In 7/VI) who were engaged on security scrutiny were moved into OKW/Chi, which was made directly responsible for the scrutiny of Army systems, and, in collaboration with the Chief Signal Officer of the Army (Chef HNW), for their development. The actual production of keys is left as a responsibility of the Army, but OKW/Chi will devise key systems and supply material for Army key production.[83]

[82]Although there is no mention of the matter, the order, in effect, removes the attack on enemy agents' systems from the Army and puts it officially under OKW/Chi. This made no practical difference in the structure for attacks on enemy agents' ciphers. See below.

[83]The German text is clear here, but the translation in D-55, p. 43, is misleading. The distinction is between the devising of methods of key production and preparation of the necessary material (Aufstellung von Schluesseln) and the actual production (printing, manufacture of grids, etc.) (Herstellung). On this subject, see Fricke's description of his duties (clearly Aufstellung von Schluesseln) in I-2. Section IV of the order should be translated:

IV

Devising and Producing Keys.

The Air Force and the Navy, both of them under reliable Nazis and never really subordinate to OKW as the Army was, had to be handled more carefully. They were requested to keep OKW/Chi informed on their work in development. In return, OKW/Chi would keep them in the general picture regarding German cryptography. The agreement of OKW/Chi had to be obtained, however, before any new system could be introduced by any of the separate branches. This is, of course, merely a restatement of Keitel's order of October 1943, and it is perhaps significant that it needed to be restated.[84] All separate branches were requested to submit material for security scrutiny to OKW/Chi which was in this matter the central authority. Finally, OKW/Cni was to furnish guidance in devising keys to the separate branches. The Waffen-SS, over which OKW had not even a shadow authority, was put in a third category. OKW/Chi was ordered to maintain close liaison with it on all matters relating to cryptanalysis, development, security scrutiny, and devising of keys.

By 1 November 1944, a wholly new structure was on paper and partly in operation.[85] This is the structure outlined in Chart No. 3-1 . Our evidence for its genuineness is good. A rough draft of the organization was found in the same personal file with the two documents already discussed. It is undated and unsigned. The document was made the basis of an interrogation of Kettler after he was captured. He suggested a few changes, mainly in the names of section heads, and added the statistics on the numbers employed in each of the sections. Mettig supplied independently an almost identical picture of the new structure.[86]

OKW/Ag. WNV will furnish guidance for the branches of the Armed Forces in devising keys and will act for the Army in devising keys. The production of keys is the affair of the separate branches of the Armed Forces, in the case of the Army, the affair of the Chief of Army Equipment and Commander of the Replacement Army/General Army Office/Signal Department.

[84] cf. note 73.

[85] Fricke refers to the re-organization 1 November 1944 (I-20, pp. 6-7.) and it is very likely that Chi started to operate according to the new structure at about that time.

[86] Original document is DF-8. Revised document with Kettler's corrections is I-39. Mettig's testimony is in I-96.

The new emphasis on cryptography is evident in the separation of the main work of OKW/Chi into two divisions (Hauptgruppen), Division A devoted to cryptography and Division B for cryptanalysis. It is worth noting that the second in command (Mettig definitely describes himself as such) [87] is no longer head of Section I, but of Division A, which was evidently intended to be the more important division. From other sources too, we know that it was intended that the activities of the organization should reach their climax in Division A.[88] The cryptanalytic sections of Division B were to serve directly or indirectly the purposes of German security. Consequently, the research section of Division B (Chi B IV, Huettenhain's section) had a divided mission. Part of its resources were devoted to initial breaks into more difficult enemy cipher systems, part to security scrutiny of German systems. Of the 46 experts available to the section, 10 spent their time wholly on security and 10 on enemy systems. The 26 experts in the machine section evidently divided their time between the two.

In general, the work of Chi seems much better articulated in the new organization. The heterogeneous character of the old Section IV in which the most diverse activities were incorporated has been rectified. The following comments on the details of the new organization may be made:

Section Z.

Section Z dealt with details of payroll and other purely administrative matters. It also exercised a political scrutiny over all the members of the organization.[89] Some such section doubtless existed in the old organization, but no mention would be made of it in the purely operational report which is our chief source of information on that organization.

Section I.

After the second-in-command became head of Division A rather than Section I, Section I probably lost much of its

[87] I-96, 3.

[88] I-84, p. 2.

[89] All enlisted personnel working in the organization were organized into the Operational Comapny (Einsatzkompanie) OKW/Chi under Major Hein. This was formerly called First Company of those Detached to OKW/Chi (1. Kommandiertenkompanie OKW/Chi). Previous commanding officers had been Captain Krüger, Major Walter. See I-150, 5.

old importance. Logically, it should have been subordinate to Division B, since all its intercept was routed there. It was probably kept directly under the Chief in order to keep it in entirely military control. Division B was under civilian control. The new head of Section I, Capt. Grotz, was formerly commanding officer of the intercept station at Sofia.[90] Sub-section Ib, whose mission was to study call signs and frequencies used in world diplomatic traffic as a guide to the intercept stations, seems seriously understaffed. The fact that the head of the sub-section was originally to have been a captain suggests that a larger group was originally planned. The T/Sgt. Schnueckel, who according to Kettler was head of the sub-section, is probably identical with the T/Sgt. Suenkel who was said to have been in charge of call sign and frequency study in the intercept station at Lauf.[91]

Sub-sectionIc was identical with the Chi V of the old organization, which, it will be recalled, had charge of the teleprinter network of Military Intelligence (the Abwehr) as well as of OKW/Chi. When the work (and probably many of the personnel) of Military Intelligence (Abwehr) was taken over into the Main Reich Security Office (RSHA), Chi continued to service its network until early in 1945, when Himmler's people took over this task for themselves, thus severing the last link between OKW/Chi and the old military intelligence organization. The work of section Ic then became appreciably lighter and Senior Inspector Buck, formerly in charge, left in April 1945.[92] The name of his successor is not known.

Division A was staffed almost entirely with personnel taken over from the Army. The chief exception to this was Senior Inspector Menzer and perhaps some of his assistants in sub-section II c. In complete charge of security and development at first, and then attached to Huettenhain's security section, Menzer had always acted more or less as a free lance, specialising in agents' ciphers and ciphers for government services. He had only occasionally consulted Huettenhain on security problems "when questions of probability were involved".[93]

[90] I-105, 4.

[91] I-85, 4.

[92] I-96, 7.

[93] I-31, 3.

The new structure recognized his independent status. His section is large and it is not unlikely that some of the personnel came from the Army.

There were elaborate plans for sub-section II a. Here the closer contact with the needs of the troops in the field, in cryptographic matters -- obviously one of the leading ideas behind the re-organization of OKW/Chi -- was to become a reality. The function of the section was to allocate keys and cipher systems. To carry out this task, the sub-section was to maintain intimate liaison with field units through skilled signal personnel from the services who were to be assigned to the sub-section and then detached back to the field where they were to observe the reaction of the troops to various systems and thus to advise II a on allocation. They would also be in a position to give on-the-spot instruction to the troops in the use and security of ciphers. The head of the sub-section was to be Capt. Bernsdorff, whom Mettig describes as "an experienced tank signaller....peculiarly suited for this job."[94] Fricke, who may only have been revealing an academic lack of sympathy with the practical turn being given to the work of OKW/Chi, told interrogators that Bernsdorff was a tank captain who "had no knowledge of cryptography".[95] Whatever Bernsdorff's personal qualifications may have been, he did not arrive until January 1945 and never really had an opportunity to get the section operating. He apparently did succeed in assembling First Lt. Eckert of the Air Force, Senior Specialist Franke of the Navy, and SS First Lt. Fricke of the Main Reich Security Office (RSHA) to represent their services in his sub-section. He himself was to represent the Army and the SS. No one was ever sent into the field. However sound the basic idea of the section may have been, Mettig and Fricke agree that it accomplished nothing. Bernsdorff had to be assigned to more urgent work very shortly after his arrival.[96]

Despite the relatively few people allotted to it, Fricke's sub-section (IIb) seems to have been very active. According to the plan, IIb was to carry out the details of cipher and key composition in close conjunction with IIa, which was presumably

[94] I-96, 8.

[95] I-20, pp. 6-7.

[96] I-96, 8.

thoroughly acquainted with the needs, usages, and desire of the field. Since IIa never really functioned, Fricke apparently simply carried out the same tasks of key and cipher development that had been his mission while he and his section had been attached to the Army.[97] In addition, he personally worked in close collaboration with Huettenhain on security problems.

Section III was originally subordinate to the Army. The main body of the Section was located in Dresden and remained there after the change in subordination. The mission of Section III was the compilation of keys and of codes in so far as this could be accomplished by mechanical processes of randomization, the printing of this material, and its distribution. The basic material for the compilation was supplied by Fricke and his sub-section. The work of printing was mostly farmed out to about thirty printing firms, most of which were located in Saxony. Printed ciphers were packed in Dresden and sent by truck to the OKW Distribution Office (Kurierstelle) at Zossen, whence they were forwarded. Field units notified Section III of compromises and alternative keys were then brought into operation. There was a sub-section (IIIb) in Berlin under S/Sgt. Mertz (5 soldiers, 20 women) who kept up liaison with the Field Economic Office (Feldwirtschaftsamt) and other agencies on procuring paper. There were also small liaison groups with the printing firms.[98] It is doubtful that the work of this section was changed appreciably when it came under OKW/Chi in November 1944. Liaison with the Army through the Army Chief Signal Officer (Chef/HNW) continued. The head of the section, Major Metzger, was injured early in 1945 and was replaced by Bernsdorff.[99]

Division B was the old Chi IV. All strictly cryptographic work had been removed and the organization revised to reflect more perfectly the actual tasks performed. The old mathematical sub-section, IVc, was upgraded to new section IV.[100] Some of the subsections of the new section IV were further subdivided

[97] Described in I-2.

[98] Such groups existed at Halle, Zwickau, Chemnitz, Leipzig, Frankfurt/Oder, Bischofswerda, Magdeburg, and Reichenbach (Vogtland) according to Kettler (I-39, 4.)

[99] On Section III se I-36, 2, and I-96, 13 and 17.

[100] It will be recalled that this had been done in August 1944 prior to the reorganization. See above.

DOCID: 3560827

into desks. We hear of a desk B IV c1,[101] headed by Dr. Weber who was one of the mathematicians brought in by Huettenhain before the war. No further details of this subdivision are known.

The old linguistic sub-section, IV b, became Section V. The designation of the language desks of the new section V is anomalous for historical reasons. Originally, the language desks had been IV b 1--22. When sub-section IVb became section V, strict logic would have demanded that the language desks be upgraded to subsections and lettered. Actually, they kept their arabic numerals. Doubtless, the small size of most of the language desks and the ephemeral character of some of them contributed to this result.

Technician Koehler's sub-section (Va) was brought into OKW/Chi from the Army Cryptanalytic Service in November 1944. All we know about it is what Mettig tells us:[102] "It was contemplated that this department would not only advise the cryptographers on linguistic problems but would also direct all matters that concerned foreign languages for the OKW. ..... This coordination was desirable owing to the number of independent agencies concerned."[103] The plan for co-ordination was never actually put into operation.

Section VII.

Section VII is the old Chi "X". The organizational plan called for the subordination of the section with its task of evaluating and distributing broken and translated messages (VII a) and maintenance of the Archives (VII b) to Fenner's Division B. Since VII a handled only the output of Division B and VII b served mostly the personnel of Division B, this seems to have been a logical arrangement. The Section, however, was left directly subordinate to the Chief of Service out of

[101] I-124, 2.

[102] I-96, 15.

[103] For instance, Interpreter Training Battalion (Dolmetscher Lehrabteilung), Berlin, Newspaper Section (Nachrichtenabteilung), Berlin, General of Signal Intelligence (General der Nachrichtenaufklärung, the final German designation of the Army Signal Intelligence Agency), Signal Interpreter Replacement and Training Battalion (Nachrichtendolmetscherersatz und Ausbauabteilung), etc.

DOCID: 3560827

regard to the feelings of Lt. Col. von Kalkstein who would presumably have considered subordination to Fenner a humiliation. According to an order of the Fuehrer, von Kalkstein was to be dismissed from the forces anyway "because he had friendly relations with people outside Germany." After his departure Section VII was to be subordinated to Division B.[104] He never departed.

The broadcast monitoring sections, old Chi II and Chi III, were combined into a single section, Section VI. Operations were continued in the same location and were probably little affected by the change. The new orientation of the whole service towards security rather than intelligence has altered the relative importance of the activities of this section, however. In the earlier structure, the activities of Chi II and Chi III form an important part of the activities of the whole organization, if not quite half as Chart 3-1 suggests. In the later structure, when Division A was the supremely important unit and Division B existed primarily to assist the security work of A, Section VI appears as a vestigial irrelevance. It could have ceased operations without noticeable effect on the rest of the work of OKW/Chi.

The history of the charter and organization of OKW/Chi during the war illustrates the development of the German idea of the purpose of a signal intelligence organization at the highest command level. OKW/Chi began the war as a purely intelligence organization, born within the Military Intelligence Department and incorporating news and broadcast monitoring as important parts of its operations. It ended as a high level security organization where even the cryptanalysis of enemy traffic was intended primarily to assist in assuring German security among all branches of the Armed Forces and government agencies. This change was accelerated by changes in command caused by events wholly unrelated to signal intelligence, but it would be a mistake to regard it as caused solely by the replacement of Fellgiebel and Thiele by Praun and Gimmler. It reflects a more general trend of thought on the part of the German High Command and of the leading signal intelligence personnel.

[104] I-96, 17.

DOCID: 3560827

5. The Disintegration of OKW/Chi. The plan put partly into effect in November 1944 is the final organizational expression of German ideas on high-level signal intelligence. Later organizational changes were ad hoc, forced by the pressure of Germany's impending defeat. The local movements towards the end are clearer than the changes in organization and command. They may be mentioned first. In February 1945, plans were made to move OKW/Chi out of Berlin. In March, the move actually took place and most of the personnel were moved to Halle along with the cryptanalytic machinery. Operations were started at the Army Signal School (Heeresnachrichtenschule) there.[105] The archives were probably moved to Lauf at this time. In any case, they were there before 10 April.[106] Section III moved from Dresden to Halle but did not begin operations in the new location.[107] On 10 April[108] most of the unit moved to Ammersdorf and there entrained on the 12th for South Germany under Major Hein as Commander of Transport (Transportfuehrer). The train was routed to the Chiemsee via Falkenberg, Dresden, Prague, Pilsen.[109] Part of the shipment (sections II, IV, V, VI) was at one time reported stuck between Prague and Pilsen.[110] Most of the personnel, however, got through to Werfen near Salzburg.[111] Some of the people from the intercept station at Treuenbrietzen also reached Werfen.[112]

[105] I-150, 6; I-36, 2.

[106] I-39, 4.

[107] I-36, 2.

[108] I-150, 6, from Beyreuther who was on the spot. Mettig (I-96, 22) says 9 April.

[109] I-96, 22.

[110] I-39, 4.

[111] Trappe arrived there 3 May (I-123, 2).

[112] I-85, 5. Kettler says, probably speaking broadly, Salzburg, (I-39, 4).

The Lauf station with the archives set out for the Schliersee south of Munich on 10 April, arrived on 19 April, set up, and operated for three days. On the thirtieth orders were received for some of the personnel to proceed with one-tenth of the intercept equipment to Werfen. Those who remained disposed of the rest of the equipment and the archives in the lake.[113] The others joined the remnants of OKW/Chi at Werfen.[114] There the Chi personnel were incorporated into an ad hoc unit called Corps Group (Korpsgruppe) Bork, which was apparently picking up stragglers, whether for a last stand or an orderly surrender we do not know. The Chi personnel were finally captured by American units under Colonel Clifton.[116] Some of them worked for the Americans until the end of May. They were then moved to Heufeld near Bad Aibling whence they were released.

Kettler, Huettenhain, and Fricke, on the other hand, ended the war in the North. They had, according to an unreliable authority, left Berlin for the intercept station at Husum.[117] Kettler was captured in the town of Ausacker, near Flensburg, Huettenhain and Fricke in the vicinity of Ausacker. They were accompanied by First Lt. Schubert, one of the leading Army cryptanalysts.[118] Mettig went with the OKW mission to the allies, first to Flensburg and then to the SHAEF headquarters at Rheims, where he was taken into custody.[119]

No one obtained from the prisoners a consistent account of the organizational changes accompanying the collapse of German arms, but from occasional remarks recorded in the reports and our knowledge of the movements of the personnel a fairly consistent picture can be reconstructed. When Chi evacuated Berlin and arrived in Halle, a mysterious Col. Hoepfner seems to have taken

[113]Their account in I-85,5, is substantiated by the Team 5 report (IF-167, p. 6).

[114]I-85, 5.

[116]I-150, 6.

[117]From Beyreuther (I-150, 11) who was not in a position to know Kettler's plans.

[118]See Kirby's supplement to the report of Team 6. (IF-165)

[119]I-78, 2; I-17, 4.

DOCID: 3560827

command.[120] Kettler and Mettig remained behind in Berlin, perhaps to assist in high-level decisions being made regarding splitting the Supreme Command of the Armed Forces into a northern and southern group. The head of the Army Signal Intelligence Service, Col. Boetzel, and his immediate staff also were in Berlin at the time, and remained there until April.[121] It was apparently decided to amalgamate the signal intelligence forces of the OKW and the Army (OKH) into a single Army Signal Intelligence Service. Boetzel was to command the combined forces in the South and Kettler in the North. The plan was put into operation on 14 April.[122] Boetzel took over the elements of OKW/Chi in the south. Just when Kettler left to take charge in the North is not known, but in its initial report on him, the SHAEF control party at Flensburg describes him as the northern counterpart of Boetzel, head of the Army Signal Intelligence service in the South.[123] Mettig, himself, perhaps with a skeleton staff, seems to have remained as the sole representative of OKW/Chi. Mettig told his first TICOM interrogators that Boetzel was head of Army Signal Intelligence in the south and Kettler in the north.[124] As such, he accompanied the OKW surrender mission to SHAEF. He told his interrogators that he was "in charge of OKW/Chi in the closing stages."[125]

[120]The Foreign Office people, who knew the Chi situation in Halle, mentioned him as titular head of Chi, although none of them was quite certain of the name (I-1, 19). Quite independently, Trappe mentions Colonel Hoepfner as head of OKW/Chi in March 1945 (I-123, 4). Nothing else is known about him. He does not seem to have accompanied the Chi-train to the south. Major Hein, the CO of Troops, and Lt. Col. Kaehler, the head of Section VI, seem to have been in charge here. At least they are mentioned as having lists of the personnel who made the trip. (I-150, 11).

[121]I-17, 4.

[122]The date is Weber's (I-124, 2). Trappe says OKW took over late in April (I-123, 4). Grube, a high ranking signal officer, told interrogators that the final split of OKW did not take place until 22 April 1945 (I-17, 2).

[123]I-5.

[124]I-17, 4.

[125]I-78, 2.

DOCID: 3560827

Chapter III. Intercept Paragraph

OKW/Chi Had Two Wholly Distinct Intercept Systems. . . . 6

6. OKW/Chi had two wholly distinct intercept systems. The dual character of OKW/Chi's operations, reflected particularly in the earlier organization, is also apparent in the intercept structure (See Chart No. 3-1). One intercept system concentrated on diplomatic Morse networks of enemy and neutral countries. Secondary commitments were nets of other government agencies (military attachés, economic authorities, etc.). This system consequently took mostly encrypted traffic. The material picked up was passed on to the breaking sections of OKW/Chi. The second system concentrated on monitoring foreign broadcasts, principally news broadcasts. A second important task was monitoring the correspondents' reports of news agencies such as Reuter and Domei. In addition, the second system seems to have had the mission of taking material requiring special apparatus, such as multiple Morse and commercial radio telephone. Some agents' traffic was apparently also covered, but most of traffic picked up by the second system was in clear.[131]

The core of the first intercept system was constituted by two large intercept stations, one at Treuenbrietzen, near Berlin, and the other at Lauf near Nuremberg.[132] Treuenbrietzen was one of the old intercept stations.[133] It was apparently already in existence by 1933 and is said to have specialized in intercepting diplomatic traffic.[134] It was definitely subordinated to OKW/Chi for the interception of

[131]See DF-9, 2 (Kettler's report). In his report, Kettler also mentions Hellsendungen as picked up by the second system. This probably means transmissions with the Hellschreiber, rather than picture transmissions as it is translated.

[132]Called Feste Horchstellen up to 1941, after that Feste Nachrichtenaufklärungsstellen (I-85, 2-3).

[133]It was originally situated at Frankfurt/Oder and moved to Treuenbrietzen at an unspecified date (I-85, 2-3).

[134]I-62, 5-6. This information, from an army intercept operator named Raatz, cannot be considered wholly reliable.

diplomatic traffic in 1939. Although the personnel of the station got to Werfen at the end of the war, none of them was interrogated. Little is known about the station except that its commanding officer was a captain, Dr. Rust.[135] Apparently it controlled no subsidiary stations, at least towards the end of the war.[136] Some of the personnel were despersed to Tennenlohe, a subsidiary station of Lauf, because of danger of air attack in the spring of 1944.[137]

Lauf was developed after the army was ordered to expand its intercept system in 1933. The original location was at Hersbruck.[138] It was intended primarily to operate against Czech traffic. By 1939, the necessity for intercepting Czech traffic had passed and the station was turned over to OKW/Chi for diplomatic traffic.[139] Lauf had three small intercept stations subordinate to it. The one at Loerrach near the Swiss border was set up in order to pick up traffic from Switzerland on the ground wave. This traffic could be heard at Lauf only with difficulty. Loerrach had eight or nine sets. While Lauf was being completed, there had been a temporary station at Tennenlohe. This was left equipped with four or five sets and retained for emergencies. Finally,

[135] I-96, 6.

[136] Mettig mentions none although he does mention the outstations of Lauf. Dettmann and Samsonow, two reliable informants on Army matters, mention an Army intercept station (Feste Horchstelle) which operated at Treuenbrietzen in 1939 and had subsidiary stations at Meserik, Fraustadt, Schneidemuehl, and Schlochau. The relation of this station to the OKW station is obscure. (I-116, 12).

[137] DF-9, 2.

[138] I-85, 3. See also Mettig, I-96, 6, who makes it clear that Tennenlohe, Lorrach, and Libourne were subordinateto Lauf. Kettler's report(DF-9, 2) says Flicke was in charge at Libourne until June, 1944.

[139] Operations were begun at Tennenlohe pending the completion of Lauf. The statement in I-85, 3 that Lauf itself did not become operational until December 1944 must be an error, perhaps a typists's error, since the informant Flicke, in charge of operations at Lauf, was certainly in a position to know. Kettler speaks of Lauf as well as Tennenlohe as operating in the spring of 1944. (DF-9).

there was a subsidiary station at Libourne near Bordeaux in France. This operated eight or nine sets from autumn 1943 until the spring of 1944. It was used principally for the interception of Swedish and Turkish traffic.[140]

The total establishment at Lauf, apparently including the outstations, was 200-250 persons. After January 1944 about eighty of these were women. The operators were apparently mostly soldiers organized in a military unit.[141] The total number of sets in operation, including those in the outstations, was eighty to ninety.[142] Specialist Flicke, our principal informant on the activity of the station, states that up to the beginning of 1943, the station attempted to cover "all diplomatic traffic" and the traffic of the Polish underground. After this time, Berlin assumed closer control and sent priority directives as a result of which the total intercept dropped from 25,000 to 10,000 messages per month. The station carried on no cryptanalytic work, but hada sergeant, perhaps with some assistants, who was an expert in traffic identification.[143] Flicke was in general charge on the technical side. The commanding officer from 1 December 1939 until the end was Reserve Major Wend.[144]

Intercept stations in foreign countries had a special status. They are called "special outstations" by Mettig.[145] They were not large or elaborate enough to be called Fixed Intercept Stations, but unlike the smaller stations at home (and in occupied territory) they were subordinated directly to Group I of OKW/Chi rather than to a larger station .

[140] I-85, 5. See also Mettig (I-96, 6) who makes it clear that Tennenlohe, Lörrach and Libourne were subordinate to Lauf. Kettler's report (DF-9, 2) is liable to misinterpretation on this point.

[141] I-85, 6. The head of this unit was Staff Director Hatz.

[142] I-85, 6-7 has a list of equipment. 60 Hellschreiber are also mentioned. What these were used for is obscure.

[143] His name was said to be Suenkel, but see above note 91.

[144] I-85, 4. Wenden according to Mettig (I-96, 6) whose memory for names was not entirely accurate. I-49, 3 says Wendt.

[145] I-96, 6.

DOCID: 3560827

They were administered by Military Intelligence (Abwehr) through its organization in foreign countries. Two such special out stations are known to have existed, one in Spain and one in Sofia.[146] Of the latter, little is known beyond the fact that it existed. It specialized in intercepting short-wave traffic from England.[147] Its communications with Berlin were probably poor, although teleprinter lines existed.[148] One informant stated that the messages he had handled from Sofia were always delayed.[149] Fenner visited the station several times.[150] The commanding officer was Capt. Grotz who was replaced by First Lt. Thielen[151] when Grotz became head of Chi I.

Considerable information is available, on the other hand, about the German intercept system in Spain. The OKW conducted a small network there which in 1941 employed, according to Mrs. von Nida, about fifty men.[152] It was established in 1940 in order to intercept Mediterranean traffic and also short-wave traffic from Sweden.[153] The original plan seems to have been that it should also supervise the Spanish stations of the other branches of the Armed Forces.[154] The commanding officer was Major (at that time Capt.) von Nida, who served from the winter of 1940 until April 1943.[155] Von Nida was succeeded by

[146] I-96, 6. Df. DF-9.

[147] I-96, 6.

[148] DF-9, 2.

[149] I-150, 6.

[150] I-150, 11.

[151] I-96, 6.

[152] I-105.

[153] I-96, 7.

[154] This supervision was not maintained. See below. Ltn. August Schroeder (I-75, 203), who was in intercept work in Spain in 1940 considered that he was working for a joint OKW-Army organization.

[155] See note 57. Mettig's statement (I-96, 7) that Major Marquardt was in charge is almost certainly an error. Mrs von Nida states positively that her husband was CO until relieved by Plankert.

First Lt. Plankert.[156] Communication between stations and to Berlin was by courier and wireless, for which the unit had a powerful transmitter.[157] There were also teleprinter communications to Berlin.[158] All intercepts were sent back to Berlin; no cryptanalytic work was carried on by the unit.[159]

The controlling station was in Madrid, originally situated in the German consulate (10 Ayala).[160] Because of interference from the nearby broadcasting station EFE, and perhaps for security reasons, the outfit was moved to the northeast section of the city (Castillana). After 1942, perhaps as a result of expansion, the unit took over the Florida, a large night club in the vicinity.

The largest outstation was on a German owned cattle ranch north of Seville.[161] Second Lt. Eichner was in charge.[162] Apparently on the same site but under separate navy control was a naval D/F station under Lt. Comdr. Zeimer.[163] Previous to 1944, there had been some wireless operators, probably intercept people, in Tangiers.[164] Whether they were subordinate to the Madrid unit is not entirely clear. On the Canary Islands, there was a single intercept operator, Jeschol by name, a former

[156] From Mrs. von Nida (I-49,3) Mettig (I096,7) also mentions Plankert as finally in command. The "Planhart" on the previous page is probably a mistake.

[157] I-105, 3.

[158] I-105, 3 and DF-9, 2.

[159] I-105, 2.

[160] I-49, 4. The "embassy" of the text is probably a mistranslation See I-105, 3.

[161] I-105, 4; I-96, 7; DF-9, 2.

[162] I-96, 6. He is probably identical with the Eichsner mentioned in I-105, 4, as an outstanding enlisted man brought from Seville to Madrid and commissioned.

[163] I-93, 7. This information is from the chief cryptanalyst of the Navy cryptanalytic agency and is probably reliable. Mettig's statement that "the naval D/F station was controlled by the OKW/Chi" (I-96, 7) is, therefore, not wholly accurate.

[164] DF-9, 2.

DOCID: 3560827

Lufthansa man. He was in contact with the Madrid station by wireless.[165] The air intercept station at Barcelona came under exclusive Air Force control in 1942.[166] Mrs. von Nida also mentions a sub-station in the Balearic Islands and a large one at Bordeaux (at first at Arcachon).[167] The Balearic station, if it existed, was probably very small. The fact that the large Bordeaux station is not mentioned in the Kettler report makes it almost certain that Mrs. von Nida was mistaken about its being subordinate to Madrid, or to the OKW. The station was almost certainly under the Army.[168]

The Spanish network was apparently conducted without the official approval of the Spanish government. Very elaborate security precautions were taken to keep the work secret. The personnel were encouraged to keep to themselves in small groups and to avoid contact even with other Germans in Spain.[169] Married men might not be accompanied by their wives, and single men were strictly forbidden to marry Spanish women. In January 1944, the Seville station was betrayed to the Spanish police and had to be closed to avoid being raided.[170] About the same time the intercept operators in Tangiers were expelled.[171] Mettig believes that the personnel of the Madrid unit were interned in April 1945.

A clandestine relationship did, however, exist with certain individual Spaniards, some of them highly placed in

[165] I-105, 3-4.

[166] I-49, 4. Cf. I-96, 7.

[167] I-105, 4.

[168] See I-76, 5 where the Army intercept operator Werner Klett mentions his being assigned to Arcachon.

[169] This exclusiveness was well observed. Friedhelm Baechle, a wireless operator for the Abwehr in Spain, had only the vaguest information on German intercept activity there (I-61, 3).

[170] DF-9, 2; I-96, 7.

[171] DF-9, 2.

the Spanish Army.[172] It was the job of two Military Intelligence (Abwehr) officials, Amberg and Friedemann, to contact such Spaniards as well as to take care of the economic side of the unit, doubtless as representatives of the War Organization (Kriegsorganisation). The only known case of Spanish military cooperation with the Madrid intercept unit did not turn out happily for the Germans.[173] According to Mettig, contact was made with the Spanish General Staff regarding the equipment of the naval D/F station at Seville which had been closed in January 1944. Colonel Sarmiento, Chief Signal Officer of the Spanish Army, was persuaded to agree to let the equipment be set up by Spaniards on Spanish military ground. Some of it was then to be operated by Germans for German purposes; the rest was to become Spanish property. The equipment was delivered to the Spaniards, but was never set up and never operated. Apparently, it remained in Spanish hands, tactfully expropriated.[174]

It is likely that around 1940 there was a plan to set up a number of interservice networks in neutral and Allied countries under the control of OKW/Chi. Capt. Wadim Herold, an Air Force officer, told interrogators that he was detached to OKW/Chi in January 1940 and given a tour of the establishment preparatory to being sent into the field as an intercept officer, because OKW was at this time interested in establishing stations in Bulgaria for the Army, Navy, and Air Force. The Navy refused to come in on the project. By the time Herold arrived in the field at Varna (cover name Kommando Nordland), the Air Force had evidently already taken over the station. But Herold said that it was "formerly part of the OKW complex".

[172]Mrs. von Nida's assumption (I-105, 3) that, because the von Nidas enjoyed "friendly personal contact with the head of the Spanish intelligence service" the Spanish authorities, as a whole, knew "what was going on" is too sweeping and inconsistent with the strictly enforced security measures, and with the threatened of the Spanish police against the Seville station once it was betrayed.

[173]Traffic obtained from the Spaniards seems to have been passed via military intelligence (the Abwehr) rather than through the Madrid station. On this traffic see below, p. 45.

[174]Mettig's story in I-96, 7.

The station consisted of 22 men, who wore civilian clothes. There were five receivers. They covered air force traffic in Syria, Greece, Rumania, and some ferry flights in the Mediterranean. Plain language was dealt with on the spot. Cipher messages were sent back to Berlin; Herold thinks to OKW/Chi.[175] If true, this may be a vestige of former OKW control of the station.

Mrs. von Nida speaks of other OKW outstations at Belgrade, at Budapest, at Vienna, and at Rome.[176] One may reasonably doubt that these were actually OKW stations. It has already been noted that Mrs. von Nida was probably mistaken about the subordination of the station at Bordeaux. Foreign Office cryptanalytic workers told interrogators that OKW had an intercept station in Greece.[177] One may doubt this also. It is clear from documents[178] that the firm and permanent part of OKW's intercept structure consisted of the Treuenbrietzen station, the Lauf station with its subsidiary stations, Sofia, and the Spanish network.[179]

Control of Intercept was in the hands of the head of Group I. The method of control is described by Mettig who held this position from December 1943 until November 1944.[180] The Chief of OKW/Chi prepared a monthly report on the most interesting links as he appreciated them from his knowledge of the military and political situation. Doubtless, the regular briefings he received from Military Intelligence (the Abwehr) were the basis for these evaluations. A report from the cryptanalytic point of view was prepared by Section IV (later SectionV). On the basis of these reports, the head of Group I

[175] I-65, 2-3.

[176] I-105, 4; I-49.

[177] I-22, 13. They also mention one in France (probably Libourne) and in the Balkans (probably Sofia).

[178] Particularly DF-9 and the Kempf list of intercept stations in T 1620.

[179] See also the account of the cryptanalytic worker Beyreuther (I-150, 6) who said he worked on signals from Lauf, Treuenbrietzen, and "one place in Bulgaria". He also knew of an intercept system in Spain which had been visited by Fenner and the head of the Archives, S/Sgt. Schaedel (I-150, 11).

[180] I-96, 6.

DOCID: 3560827

made his decisions as to what links were to be covered and then passed on orders to the intercept stations. A persistent difficulty was created by the heads of the language sections who demanded that only traffic being currently solved should be intercepted, "in order that the results of their work would appear more effective." If we can believe Flicke, it must be assumed that this careful system of intercept control must have been introduced around the beginning of 1943.[181] Before that time, the stations seem to have had more choice of what they were to cover although it is hard to believe that the situation was as chaotic as Flicke implies.

Various outside organizations contributed traffic to the OKW/Chi cryptanalysts. Of these, the most closely related to OKW/Chi from an organizational point of view was the German Radio Defense Corps (Funküberwachung, abbreviated Fu) which was also part of the OKW and was subordinated, like OKW/Chi, to the Armed Forces Communications Group (Ag. WNV) hence the abbreviation OKW/ Ag. WNV/Fu.[182] Mettig describes the work of the Service as follows:

"In conjunction with the Reichspost, OKW/Fu gave permission for transmission, distributed frequencies and call signs to Army agencies, Government agencies and industries, and was responsible for the distribution of codes. These matters were the concern of Gruppe I (Organization and Tactical employment) and Gruppe II (Supply). Gruppe III was responsible for WT security and as such controlled the agencies that enforced it."[183] Part of the work of Gruppe III was the interception of agents' traffic. For this purpose it controlled units of its own and also gave operational directives to the intercept units of the Regular Police (Ordnungspolizei), who passed the intercepted traffic back to Fu III.[184] There was a special unit attached

[181] See above, page 15 .

[182] See above, note 1.

[183] I-115, 2.

[184] For further details on the intercept facilities and methods of Fu III see I-115. For the division of labor with the police, see I-91, an interrogation report of Robert K. H. Schlake, Brigadier General of the Regular Police and Chief of Communications in the Main Office.

DOCID: 3560827

to Fu III for cryptanalysis of agents' traffic,[185] but some of the agents' traffic picked up found its way into OKW/Chi. Military Intelligence (Abwehr) organizations in foreign countries conducted line tapping operations in Bordeaux, Lisbon, Madrid, Sofia, and Ankara.[186] The heads of OKW/Chi's special outstations in Madrid and Sofia had some liaison with Military Intelligence (the Abwehr) on the matter, but actual operations were entirely in the hands of Military Intelligence (the Abwehr). The material was passed directly to the head of OKW/Chi or to Fenner as head of cryptanalytic work. It did not go, like ordinary intercepts, through Section I. Line intercepts, according to Mettig, formed about one-third of the traffic dealt with by OKW/Chi.[187] This agrees with the Kettler report of Spring 1944 according to which a monthly average of 36,480 wireless messages (both plain and enciphered) and 12,330 line messages were taken from January to June 1944. It is surprising that Kettler includes the line messages in his report of the regular intercept from facilities "centrally controlled by Chi." He must have included the Military Intelligence (Abwehr) line intercept service in this category, because there is no evidence for line intercept work on the part of any of the stations directly subordinate to OKW/Chi.[188]

Of the other German signal intelligence agencies, Goering's "Research" Bureau seems to have made the largest contribution to OKW/Chi's raw traffic. According to the Kettler report, "rather more than a third" of the total traffic handled by his cryptanalytic section in the period January to June 1944

[185]This unit (Referat Vauck) finally became a part of OKW/Chi. See below, chapter III.

[186]Military Intelligence (the Abwehr) also procured cryptographic material through agents (I-127, 5). See the case of the code purchased from the Hungarians (Section V C).

[187]I-96, 5.

[188]DF-9, 2. Morgenroth (I-114, 2) stated that postoffice intercepts had gone to OKW/Chi. This may mean that copies of messages handed over to the Postoffice (which controlled cables and telegraphs) were passed on to OKW/Chi. There is, however, no other mention of traffic from this source.

DOCID: 3560827

was intercepted and handed over by the "Research" Bureau.[189] No mention is made of any other German signal intelligence service. In a list of sources of traffic dated 28 April 1943, however, Kettler's predecessor, Kempf,[190] mentions the Foreign Office as well as Goering's service. Of the signal intelligence services of allied and neutral countries the Kettler report mentions only Hungary. Budapest, he says, contributed about one-eighth of his cryptanalysts' total raw material.[191] In the 1943 lists, however, Kempf mentions traffic from Bulgaria, Italy, Finland, Rumania, and Spain.[192] The Bulgarian material seems to have been passed on from the German station at Sofia. Rumanian material was apparently handled by Military Intelligence (the Abwehr) although it was to be separately handled, or at least separately marked, after April 1943. Spanish material had likewise been handled previously by Military Intelligence (the Abwehr), but was now to be separately handled or at least separately marked. The suggested source for this material is the Spanish Signal Intelligence Service whose head was Rafael Sarmiento. This Spanish officer is almost certainly to be identified with the Sarmiento whom Mettig mentions as the one with whom the deal on the D/F equipment was made. He was apparently one of the leading Abwehr contacts in Spain.[193]

The total personnel engaged in intercept for Group I was according to Kettler "about 420".[194] The personnel in Spain and Bulgaria are not included in this figure. Perhaps about 500 is a maximum estimate for the number of people directly engaged on intercept for OKW/Chi's cryptanalysts. For the total accomplishment of the intercept organization, we have the statistics for the period January to June 1944 in the Kettler report: in that period, the monthly average was about

[189] DF-9, 3.

[190] T 1620.

[191] DF-9, 3.

[192] He also mentions the German Armistice Commission at Wiesbaden, which doubtless monitored Vichy traffic, and Military Intelligence (the Abwehr) as German sources of traffic.

[193] See above p. 42

[194] I-39, 4.

36,500 messages. It must be remembered, however, that at this time the effect of the Allied bombings was making itself felt. It had been necessary to organize an emergency plan whereby intercept of important traffic could be switched from one station to another in case of local disturbances or air attack. The emergency plan was controlled by wireless from the Fehrbellinerplatz, Berlin, (where Section VI was located).[195] In addition, Kettler complains of breakdown of teleprinter communications with Libourne, Madrid, and Sofia, "especially since the beginning of the invasion".[196]

Less is known about the second intercept system, which had its main station at Ludwigsfelde, and branch stations at Koenigsberg, Gleiwitz, Muenster, and Husum.[197] The material intercepted was conveyed from both Ludwigsfelde and the branch stations to the Fehrbellinerplatz in Berlin. The technician in charge of intercept equipment was Graduate Engineer Salzbrunn. Mettig says that, as a result of his efficiency, Ludwigsfelde was particularly well equipped. There were 80 receivers here. Ludwigsfelde was completely destroyed by air attack on 2 January 1944 and was not back in operation until autumn of that year. It was, therefore, out of operation for the entire period covered by the Kettler report of June 1944. Despite the fact that the main station was not operating, Kettler states that the broadcast intercept system kept up a monthly average of 7,280 press reports and 7,340 radio telephone transmissions (average duration 20 minutes) during the period from January to June 1944.[198]

The general impression derived from the Kettler report and the remarks of the informants is that the great bulk of the material picked up by the whole intercept system of OKW/Chi was either ordinary Morse or ordinary radio telephone. To be sure, the commitment of Ludwigsfelde and its associated stations included "enemy multiple Morse transmissions", but in general

[195] I-96, 6; DF-9, 2.

[196] DF-9, 2.

[197] DF-9, 2; I-9C, 15.

[198] DF-9, 2.

it is clear that the signal officers who controlled OKW/Chi were interested in efficient administration rather than in experiments or attempts to expand into new fields. This is doubtless what Huettenhain meant when he said "OKW/Chi itself was not concerned with intercept problems."[199]

OKW/Chi had, apparently, no facilities for intercepting Baudot. Huettenhain had seen some Baudot traffic, and this had come from the intercept station at Staats. This station was conducted by the Reserve Army and was subordinate to a section of the Army Ordnance Testing Department whose work was the development of Signal Equipment. Staats also picked up Multiplex, Duplex, and Verdun transmissions and passed them to OKW/Chi.[200] It was in operation since before the war, but its subordination indicates that the chief mission of the station was the development of equipment rather than operational intercept. It does not seem to have passed on any considerable amount of material to OKW/Chi. It is mentioned neither in the Kempf list nor in the Kettler report as a source of traffic.

The only elaborate attempts to develop intercept facilities for special kinds of transmission were made late in the war. They were not directed by OKW/Chi and, as far as can be discovered, OKW/Chi had no particular interest in them. The moving spirit behind these attempts was Col. Randewig, an officer who had been engaged in signal intelligence work for the Army on the western front in 1940.[201] He was impressed with the need for a large, centrally controlled intercept organization, staffed with at least 3000 technicians. For two years (1940-1942), he addressed a series of memoranda on the subject to the Chief Signal Officer of the Armed Forces.[202] He held various signal assignments but never had a chance to put his ideas into operation. In August 1944, he was made responsible for all questions concerning wireless in connection with rockets.[203] Since retaliation was feared, this mission

[199] I-31, 19.

[200] I-31, 19.

[201] See I-68. Other activities of Randewig are mentioned in I-47 and I-98.

[202] I-68, 4.

[203] I-68, 5.

DOCID: 3560827

included keeping a watch for enemy transmissions which might be control beams or signals for rockets. In November 1944, Randewig was given the title: Armed Forces Signal Commander for Special Employment No. 700 (Wehrmachtnachrichtenfuehrer Zu Besonderer Verwendung 700).[204] As such, he was chief of a unit consisting of a staff of technical specialists and liaison officer from the Army, Navy, Air Force, Waffen SS, and about 300 men. The unit was directly subordinate to the Chief Signal Officer of the Armed Forces. Its original mission was to study remote control and remote jamming and to devise counter-measures for enemy attempts in this field. Since this mission involved work along all wave lengths, the unit acquired the additional task of covering all gaps in the German intercept scheme, including particularly the centimeter and decimeter wave lengths, which had been completely ignored by all German intercept organizations. To accomplish this the unit had at its disposal the following three intercept stations:[205]

Husum, midway between Schobüll and Husum town. By means of an intercept receiver coupled to a sound film recorder (Tonschreiber) this station picked up a considerable volume of unidentified traffic ranging between 30 and 60 kcs. It was hoped that further study of this traffic would reveal its nature and origin. Radar impulses were also picked up which Randewig believed would be useful in developing radar counter-measures.

Kahle Asten (on a hill near Winterberg overlooking the Ruhr). This station specialized in attempts to pick up Allied decimeter traffic. Electrical disturbances during the brief period the station was in operation made it impossible to obtain any positive information.

Feldberg in the Black Forest. Nothing is known about the activity of this station.

Randewig's intercept activities came too late to be of any practical importance.

[204] That this is the correct title is established by a find of some German monitoring pro-formas addressed to Wehrmachtnachrichtenfuehrer 700. T 3366). In I-68, Randewig is called Heeresnachrichtenfuehrer ZBV 700 on p. 4 (although he operated for the Wehrmacht rather than the army alone), Wehrmachtnachrichtenfuehrer on p. 5, Hoeherer Wehrmachtnachtrichtenfuehrer on page 1.

[205] I-68, 5.

Chapter IV. Operations — Paragraph

Practical Cryptanalysis. 7

Cryptanalytic Research, Security and Development . . 8

Miscellaneous Operations 9

1. Practical cryptanalysis. In a sense, Fenner's linguists were the core of OKW/Chi. This unit operated in much the same way from the beginning. It seems to have represented the original German idea of a highlevel signal intelligence organization. The guiding principle behind its operations seems to have been to supply a steady stream of intelligence by breaking codes and ciphers which did not offer a very high degree of resistence to cryptanalysis and by furnishing translations of clear texts so obtained and of signals originally sent in the clear text. Innovations such as the introduction of a mathematical research section and the late attempt to reorient the whole organization towards cryptographic security rather than intelligence seem to have had little effect on this group. Fenner appears, in fact, to have been hostile to Gimmler's innovations.[211]

a. "VN's": The final product of the linguistic section was the translation of decoded traffic. These translations were called "VN's", or "Verlässliche Nachrichten", "reliable reports". A large number of these VN's have fallen into TICOM hands. They are all typed on form sheets headed by a large VN and classified "Geheime Kommandosache," the German classification for "Top Secret" material. Missing groups and garbles are indicated by dots, doubtful groups by dots underneath the translation. We are told that dubious translations were enclosed in parentheses and marked with question marks and that free translations were sometimes accompanied by a literal translation in brackets if necessary.[213] The date of the message and the date of publication are indicated. No evaluation was done by the sections and no reports were written. As we have seen above,[214] the

[212] IF-167, 7.

[213] I-84, 6.

[214] p. 18

completed product was passed on to von Kalkstein's evaluation section. Here material judged to be of no importance was put aside and the rest routed to authorized recipients. The principal recipients were, of course, Jodl, the Chief of the Operations Staff of the Supreme Command of the Armed Forces (Chef OKW/WFST.); Keitel, the Chief of the Supreme Command of the Armed Forces (Chef OKW); and Hitler. We know that Friedrich, the head of the Air Force Signal Intelligence Service, received the VN's[215] and it is likely that this courtesy was extended to the heads of the Navy and the Army Signal Intelligence Services also. Within OKW/Chi itself one copy went to the Archives where it was available to the members of the research section and one copy to the language sub-section which had produced it. Here it was used in compiling lists of cribs and for similar purposes. The total number of copies ordinarily distributed is indicated by the fact that, "for a long time," thirteen copies were prepared, "later on," more copies were prepared and for this purpose stencils were cut. The recipients are said to have kept the VN's and handled them in the same way as any other "Top Secret" document.[216]

Captured VN's in the possession of TICOM represent the traffic of twentynine countries. Most of the messages were from the Foreign Ministry of the country in question to its representatives in the various national capitals, or vice versa. In some cases the correspondents were two such representatives away from home. Some of the messages were signed with the name of the originator; some were signed "Foreign Ministry"; and many were unsigned.

With respect to content, the captured VN's can be roughly classified as follows:

Diplomatic household affairs such as personnel moves, exchange of stranded personnel through neutral countries, requests for jobs, moves of embassies into new quarters;

Requests for passports and visas;

Press reports;

Non-press reports;

Commercial and shipping arrangements.

[215] I-13, 6.

[216] I-84, 5.

It can be assumed that the German High Command had little interest in such housekeeping problems of the diplomatic establishments as are represented by the journey of one Leon Lévy from Algiers to Paris to fetch the archives, 2 empty mail-bags, and the typewriter.

The requests for passports and visas, which take up much VN space, were probably likewise of little interest to the OKW, unless it happened that the request came from a person of international importance.

The press reports are merely résumés of what the Germans could very well read for themselves in the papers.

The non-press reports, on the other hand, could conceivably have borne some interest for the Germans. Topics included formation of new cabinets, situation on the battle and home fronts, morale, and impending or accomplished political moves. A few examples of non-press reports from captured VN's follow.

Brazil No. 1514[217]
Ankara-Rio
19.9.44

The Vice-president of the National Party has been appointed new Foreign Minister. This appointment is, it seems to me, significant of a striving toward a closer approach to Russia, whose advance in Bulgaria is growing into a threat to Turkey.

Brazil No. 2006[218]
Ankara-Rio
29.9.44

The sudden departure of the Anglo-American Military Mission from Sofia upon the demand of the Russians has caused animated perturbation here. This appears to be the first conflict of interests betwixt the Russians and the Anglo-Americans. In Turkey, public opinion is disturbed by the attempt of the Russians to proceed in the Balkans without any control and to exclude any influence, no matter from what quarter or in what form.

Brazil No. 1703[219]
Stockholm-Rio
22.8.44

The arrival of Keitel in Helsingfors, concerning which silence was kept up to now, was announced today for the first time. It is certain that this third visit of Nazis brought

[217]T 791.

[218]T 791.

[219]T 791.

a result quite opposite to that of the other two; for Mannerheim did not allow himself to be impressed either by the usual threats or by any kind of promises. Many believe that this firm attitude strengthens the prestige of the Finnish President with the Soviets in connection with the peace negotiations reported in my telegram of yesterday. However, the first impression in Moscow of Keitel's journey was very bad.

Brazil No. 309 or 319[220]
Ankara-Rio
5.10.44

The new Thrace-statute imposed by Russia without previous announcement and (discussion) negotiations has called forth in Greek circles deep indignation and among the Allies great suspicion and not groundless fears. It is not known here what the English reaction will turn out to be. However, Turkey sees its European frontier seriously menaced by the Russian troops.

Chungking-China No. 1300[221]
. . . - Chungking
13.9.44

The reason for the visit of the Vice-minister of the Interior to consul Hou was . . . and the meeting at Quebec. This time he informed Consul Hou as follows:

The reason for the discussions of the two statesmen Churchill and Roosevelt concerning problems of English-American conduct of the war is said to lie in the necessity for sending new contigents of troops to . . . Churchill and . . . will confer on the preparation of further contingents of troops for landing in the Netherlands Indies or the Bonin Islands. The fleet movements are to be accelerated, even though it appears as if the European war were more pressing than the war in the Pacific.

One Japanese message in which the Germans would undoubtedly have been interested was, unfortunately for them, solved just 10 months late. Intercepted on 10 December 1943, it was marked "Solved after delay" and issued as a VN under date 11 October 1944. It was sent from Moscow to Tokyo and contains over five pages of annual report for the year 1943 on the situation of the Soviet Union. Such topics as the German-Russian front, Russian home-front morale, and Russian foreign policy are treated in some detail.[222]

[220]T 788.

[221]T 788.

[222]T 803.

Among the messages dealing with shipping and other commercial matters, ones such as the following may have interested the Germans:

Brazil 1704[223]
Rio-London
23.8.44

The Economic Office for Sugar and Alcohol approves the extension of the international agreement for two years and deems it suitable to ask for an increase of the quota, which of course could not be used at once, but would afford greater assurance in planning; for . . . increased during the effectiveness of the London agreement by 25% . . .

France No. ? [224]
Washington-Paris
19.10.44

Sodium Cyanide. For Import and Production.

The situation here is very critical. Before the war the United States was the principal customer for French sodium cyanide. The War Production Board inquires whether France is at this time in a position to supply a certain amount to the United States. Please answer by telegram.

DeGaulle-France No. 740[225]
Madrid-Algiers
4.9.44

The steamer "Sac II" sailed this morning, 4 September, from Huelva bound for Port Lyautey with a cargo of 4,601 tons of pyrites.

The following messages are presented as miscellaneous material which may have interested the Germans:

Brazil 324[226]
Lisbon-Rio
20.9.44

On the basis of the instructions issued by Minister Aranha in the telegram of 28 July I yesterday gave Dino Grandi as remuneration for his work the sum of 24,600 escudos, equals 1,000 dollars. I had received this sum from our clearing-house for this purpose. Dino Grandi hailed the Brazilian Government in words of acknowledgement. The text, which was handed out to me, I shall send air-mail.

[223] T-791

[224] T-782

[225] T-782

[226] T-791

Chile No. ? [227]
Washington-Santiago
7.10.44

The Government of the United States has granted to the Military Mission the following war material: 12 howitzers . . . with 9,000 . . ., 24 machine guns caliber 30 with 50,000 rounds, 48 anti-tank cannon with 9,000 rounds, 500 gasoline tanks . . .

Directives as to what systems were to be attacked came to Fenner from the head of OKW/Chi (Kempf, and later, Kettler). The head of the service was in turn, as we have seen, briefed by Military Intelligence (the Abwehr). From what little we know, liaison was, at least from the cryptanalysts' point of view, not very satisfactory. Neither Military Intelligence (the Abwehr) nor-oddly enough - the heads of OKW/Chi seem to have had an adequate idea of the difficulties faced by the cryptanalysts. As a result, directives always came too late.[228] Huettenhain remarks that Kempf had requested that an American strip system be broken by a particular Sunday. By a great stroke of luck the system was broken to meet the deadline. This caused the operational personnel some concern, "because", as Huettenhain said, "they were always afraid after that he [Kempf] would expect systems to be broken to order."[229]

When Mettig was asked point blank what was the greatest cryptanalytic achievement of OKW/Chi, he hesitated.[230] It became apparent that OKW/Chi had not achieved any outstanding cryptanalytic success. Nevertheless, Fenner's group, aided by the research section, did achieve a series of minor successes and kept a steady stream of intelligence flowing to their superiors. During the period from January to June 1944, as we are informed by Kettler's report, Fenner's linguists produced a monthly average of about 3,000 VN's.[231] It may be noted in

[227] T-789.

[228] I-84, 3.

[229] I-84, 5.

[230] I-111, 2.

[231] DF-9, 3.

passing that during the same period SSA reported a number of completed diplomatic messages which averaged 3,700 per month. Earlier, it may well be that OKW/Chi's output of VN's was greater, because during the period for which we have the report the effects of the Allied air raids on the German cities were beginning to be felt. OKW/Chi had been bombed out of its regular quarters in the Tirpitzufer section in Berlin in November 1943.[232] During the period covered by the report, Kettler's crypto-linguists were working in temporary quarters, unheated, and in many cases without doors and windows.[233] In 1944 the number of crypto-linguists engaged was about 320. It is probable that this number had declined from a peak reached about 1941. Kettler in his report refers to a combing out of able-bodied personnel for active service.[234]

Fenner's linguists, it will be recalled, were organized into desks according to the language used in the material attacked. What we know about their work in detail can best be arranged according to the language in question. When Mettig was asked the embarrassing question about OKW/Chi's outstanding cryptanalytic achievement, he was able to point out that from an intelligence point of view the Turkish section perhaps made the most important contribution. He also mentions Polish traffic as having proved important for intelligence.[235] This was confirmed by Kettler's report, where Turkey and the Polish Government in exile were mentioned as fruitful sources of information. To these he adds the United States of America.[236]

b. Turkey:

The Turkish desk in OKW/Chi consisted of about ten people[237]

[232] I-105, 2.

[233] DF-9, 4.

[234] DF-9, 4.

[235] I-128, 3.

[236] DF-9, p. 3.

[237] I-1, 20.

and seems to have been headed by Specialist Dr. Locker.[238] Beyond the fact that the achievements of this desk were very valuable, we have no information about what systems were broken. Scherschmidt, who was in charge of Turkish cryptanalysis in the Foreign Office Cryptanalytic Section (Pers ZS) said that the bulk of the work on Turkish Military Systems was done by OKW/Chi. Despite the fact that he had a low estimate of their ability as linguists, Scherschmidt believed OKW/Chi had considerable success, particularly with Turkish military systems.[239]

c. Poland:

The Polish desk had twenty people and was one of the largest language desks.[240] It was headed by a civil servant named Berndt.[241] The main success of OKW/Chi in the polish field was attained against an enciphered four-figure code used by the London Government in Exile. This system was first attacked and solved by Huettenhain's research section toward the end of 1942 or the beginning of 1943.[242] It was worked on continually and changes in the system were followed. Weber mentions having worked on the material in the spring of 1944.[243] Kettler in his report of spring '44 mentions the solution of a Polish cipher as one of the outstanding cryptanalytic achievements of his organization. This cipher was probably one of the variations in the system under consideration. By 1945, twelve different stencils and a large number of enciphering tables had been recovered.[244] In the attack

[238] Thus Beyreuther (I-150, 3). Mettig (I-96, 3) says a Lt. Dr. Kern was head of the desk and Locker his subordinate. Trappe (I-123,3) puts Turkey, Greece, and Persia at a desk under Min. Rat Seifert and Dr. Locker. Scherschmidt of the Foreign Office Cryptanalytic Section (Pers ZS) (I-103, 3) said Locker was head of the OKW/Chi Turkish desk.

[239] I-103, 3.

[240] I-150, 3.

[241] I-96, 3; I-150, 3; I-1, 20.

[242] See I-31, 20-21.

[243] I-124, 3.

[244] I-118, 9.

on the system, Huettenhain's people used a specially developed cryptanalytic device called the Witzkiste ("Brainbox") and also ordinary IBM machinery.[245] The system was referred to by some informants as "Military Attaché",[246] by others as"Diplomatic".[247]

The most valuable intelligence results from Polish traffic, however, were obtained through the breaking of the traffic between the underground organization in Poland and its government in London. This traffic was said to have been particularly valuable during the period immediately preceding the Normandy invasion. All wireless traffic from England was banned, but the traffic of Polish agents to England continued and was read.[248] Most of this traffic seems to have been in a five-figure system. The original break was apparently made not by OKW/Chi but by the Agents Section of Inspectorate 7/VI (In 7/VI).[250] Once the break had been made, however, the traffic proved to be so valuable that in the autumn of 1943 a group from The Agents Section of In 7/VI was transferred to the Polish desk of OKW/Chi where it worked as part of the organization. The translated clear texts were published as regular VN's and given an extremely limited distribution. The traffic itself was intercepted by the OKW/Chi intercept station at Lauf.[251]

d. U.S.A. and Great Britain:

The precise organization of the attack on the traffic of the English-Speaking Allies is not quite clear. Mettig stated that there was a special desk for U.S.A. and that this desk was headed by Senior Specialist Rohen. British traffic was separately handled by a desk under Senior Specialist Rotter.[252] All the other informants, however, put both Great Britain and the U.S.A. in a single desk headed by Rohen.[253]

[245] I-31, 21.

[246] By Huettenhain in I-118.

[247] By Weber in I-124.

[248] I-115, 9.

[250] See below under "Agents' Systems".

[251] I-115, 9.

[252] I-96, 3.

[253] So Beyreuther (I-150, 2). Trappe (I-123, 3) and the Foreign Office people (I-1, 20).

This was a large section containing forty to fifty people.[254] Rotter was apparently a cryptanalyst of some experience. He had once headed the Czechoslovakian desk[255] and later the Bulgarian desk.[256] It may be suggested that there was actually one desk for England and the U.S.A. and that Rohen was the head of it. Since success with U.S.A. traffic was much greater than success with English traffic, most of the personnel were probably employed against the U.S.A. It is possible that Rotter headed a small research group engaged, perhaps unsuccessfully, on some of the English systems.

With high grade American machine ciphers, OKW/Chi had no success and seems to have made very little effort. Huettenhain knew nothing of the "big American machine".[257] He apparently had never concerned himself with American diplomatic machine ciphers. No work was done on American enciphered teleprinter traffic. Huettenhain stated that he had never seen any such traffic.[258] OKW/Chi's work on the American Hagelin is mentioned below.[259] Hagelin was, of course, never a practical problem for OKW/Chi since it was never employed for diplomatic traffic.

The leading German success in the American diplomatic field was the reading of the American strip systems. We know that the American strip system (0-2) was read by the Foreign Office Cryptanalytic Section (Pers ZS).[260] Whether this is the same system mentioned by Huettenhain as having been broken at OKW/Chi is not known. The story told by Huettenhain - that Kempf had ordered the section to break an American strip system before a certain Sunday and that this was done, much to the consternation of the personnel who feared that after that he would expect systems to be broken to order - does not state

[254] I-1, 30.

[255] I-123, 3. From Trappe, who knew the situation in 1938.

[256] I-1, 20.

[257] I-84, 6.

[258] I-31, 19-20; I-84, 6.

[259] See Chapter IV.

[260] I-89.

specifically which American strip system was meant.[261] In any case, OKW/Chi deserves credit for the development of a cryptanalytic machine which facilitated the regular breaking of the traffic once the initial break-in had been made.[262] Huettenhain says the break-in was obtained through mistakes in the use of the system and that there was no physical compromise.[263] No German agency read American strip systems after the introduction of channel elimination.

For a short time, some sort of American military attaché traffic seems to have been read. Huettenhain says this was emergency double transposition but he was not sure, on thinking it over, whether this was British or American.[264] Mettig had a vague recollection of the matter. He described the system as a military attaché system although the sender was not a military attaché. The traffic was between Washington and North Africa. He thought the system was M-209.[265] Rave, who, it will be recalled, was a minor light in the Japanese section and who cannot therefore be taken seriously as the other two witnesses, had heard some vague rumors of the breaking of American military attaché traffic. He thought the system in question was a book with encipherment.[268] The most likely conclusion from these confused remarks is that an American military attaché double transposition used in Cairo sometime during Rommel's campaign was read by anagramming two messages of identical length. The evidence is so contradictory and confused, however, that the matter must remain very doubtful. It is a case where the prisoners' memory failed.

In addition, an unenciphered code of about 100,000 groups in use since 1926 was read.[269]

[261] I-84, 5.

[262] I-31, 4.

[263] I-2, p 2; I-84, 5.

[264] I-31, 9. See below note.

[265] I-111, p 2.

[268] I-22, 8.

[269] I-31, 9.

The U.S.A. desk of OKW/Chi also broke a code encipherment system employing twenty-letter alphabets.[271] Weber said that in June or July of 1941 he and a crypto-linguist named Teischmueller worked on a United States diplomatic five-letter system to which an encipherment using seven to ten alphabets was applied. Different alphabets were used for the odd and even groups. Weber did not read the system and whether it was read later we do not know.[272]

There is no evidence for high-level success against British systems. A Typex machine captured at Dunkerque was on display at OKW/Chi. This machine was without rotors and no rotors were ever obtained.[273] The OKW/Chi prisoners could give a reasonable accurate description of the machine but they were not sure how many rotors were actually used.[274] Carefully questioned on the subject, they were emphatic in their statements that it had never been solved, either by OKW/Chi or any other German cryptanalytic agency.[275]

There is considerable evidence for successful work on the British Interdepartmental Cypher. The book was captured in Bergen, Norway, and OKW/Chi collaborated with the Navy and Air Forces in solving the encipherment and reading the traffic.[276] The rest of the evidence is largely negative. Miss Hagen, head of the English desk in the Foreign Office Cryptanalytic Section

[271] I 31, 9

[272] I 124, 3

[273] See I 161, 4; I 31, 11; I 66, p 3

[274] I 31, 11

[275] An unsuccessful effort was made to trap Huettenhain and Mettig on this point. At the conclusion of the interrogation, even the most skeptical of the interrogators was convinced that they were telling the truth. See I 161.

[276] See I 22, p. 12; I 119, 4; I 93, 4. Mettig (I 111) is probably mistaken in his statement that OKW/Chi did not work on the Interdepartmental Cypher. Huettenhain (I 31; 11) simply said he knew nothing about it, so that it had not been referred to the research section. The linguists may have worked on it unaided.

(Pers ZS), said she believed that OKW/Chi was not successful with British diplomatic ciphers although they were attempted.[277] No work was done by OKW/Chi on India-Office traffic, British Commercial or Bank of England systems. Huettenhain said that no English systems had been read since 1943.[278]

e. France, Belgium, Netherlands:

At the beginning of the war OKW/Chi detached Huettenhain to the armies on the Western Front for the purpose of working on French high-level military traffic. This traffic was probably passed between the Ministry of War and the Southern District, later between the Ministry and all important commands.[279] The personal file in T-1620 contains two letters written by Huettenhain to Fenner during the time of his detachment. From these letters it is clear that Huettenhain was wholly successful. The traffic was read up to the end of October 1939 and leads were apparently given for continued reading. The military authorities were pleased with Huettenhain's work but Huettenhain made it clear that he could not have been successful without preliminary work in reconstructing French books done by Trappe and others at OKW/Chi before the outbreak of the war. Towards the end of the war the French desk was headed by Senior Specialist Mueller and consisted of about twenty people.[280] Huettenhain's interest in the primitive French form of the Hagelin, the C-36, and in the more complicated French cipher device, the B-211,[281] was an indication that some of the traffic in these systems was perhaps dealt with by this desk. This desk may have assisted with the supervision of the Vichy French traffic which was under the direct control of the French Armistice Commission at Wiesbaden, but we know no details of this work.

[277] I-27.

[278] I-31, 6. Huettenhain adds as an exception: except "a Double Transposition system... where the same key length was used on both cages". This may be a confusion with the American military attaché system discussed above.

[279] I-31, 5.

[280] I-96, 3; I-150, 2; I-123, 3; I-1, 20.

[281] See below, Chapter IV.

Of successes against the other western allies, we can say only that prior to the fall of Belgium a Belgian desk existed in OKW/Chi.[282] Since the division of labor with the Army does not seem to have been so rigorously carried out in the early days of the war as it was later, it is possible that this desk had something to do with the reading of the Belgian military three-figure code enciphered by substitution tables. In any case, this system was read. No Belgian attaché systems were studied.[283]

At the outbreak of the war there was a desk for Netherlands traffic.[284] Of the work of this desk we know nothing.

f. Russia.

The Russian desk was under Professor Nowopaschenny.[285] Wendland,[286] the head of the practical cryptanalysis section, (Section V) was also interested in Russian. It is known that, as early as 1934, Nowopaschenny was connected with the Cipher Section, and was interested at that early date in Russian problems. At that time, Russian military traffic was being worked on. During the war, the Russian section was small, and it seems to have been able to accomplish nothing. Mettig stated definitely that Russian diplomatic traffic was enciphered with a one-time pad and was never read. Traffic was intercepted from time to time and tested, but the desk never had any luck.[287] The Foreign Office People said that up to the time of Stalingrad the Army had read a Russian diplomatic system based on a one-time pad.[288] They were probably mistaken. The system read was almost certainly a military system. We know that such a system was read. A diplomatic system would not have been handled by the Army.

[282] I-36, 3.

[283] I-31, 6.

[284] I-36, 3.

[285] I-96, 3; I-123, 3.

[286] Beyreuther was, however, wrong in considering him head of the Russian desk (I-150, 3).

[287] I-96, 14.

[288] I-22, 15.

DOCID: 3560827

g. Yugoslavia:

The Yugoslavian desk was headed by Principal Specialist Wendland, who seems for a time to have been assisted by Senior Specialist Bailovic.[289] The desk is said to have been small,[290] and we do not know precisely what it attempted or accomplished. Buggisch stated that OKW/Chi attacked the systems of Mihailovic and Tito.[291] However this may be, it is known that the Army also worked on these systems.[292] What the division of labor was we do not know.

h. Japan, China, Manchukuo:

The Japanese Desk was headed by First Lt. Adler and seems to have consisted of about fifteen people.[293] Five members of this section were interrogated, and we have a fairly complete picture of its accomplishments. The following Japanese systems were read:[294]

(1.) A two and four-digit code [illegible]iphered, known as the LA Code. Another informant adds the CA and IP Codes.[295]

(2.) The KOKOK Code.[296] This was a two and four-letter code transposed on the basis of a repeating nineteen digit keyword. This system was solved up until the time it was dropped on 1 January, 1942.

[289] I-96, 3; I-123, 3.

[290] I-1, 20.

[291] I-58, 7.

[292] I-69.

[293] I-96, 4; I-123, 3. Beyreuther, who was a member of the section, mentions 14 names (I-150, 4). This is, therefore, a minimum number. The Foreign Office people simply refer to a "largish group". (I-1, 20).

[294] The following list is based on that given by Reinhard Wagner, a member of the desk in I-90.

[295] Beyreuther (I-150, 8.).

[296] Called KAKAK by Beyreuther (I-150, 8). The system was worked on by the Research Section (I-31, 8; I-31, 5; I-118, 7).

(3.) FUJI, a transposition by means of a transposition square with nulls applied to a two and four letter code.[297] This system was read until it ended in August, 1943. It was broken in a very short time by the use of special apparatus designed by the research section and operated by Weber.[298] New traffic could be read in less than two hours with the aid of this machine.

(4.) The slightly more complicated system which succeeded FUJI in January, 1944 was also read.[299]

(5.) A four-figure basic code with 1,200 values enciphered by an additive book of 400,000 values.

(6.) Various commercial codes, each of about 10,000 values, enciphered by transposition. For example: AMSAJ, a three, four, six-letter code; ETGAV, a six-letter code; AMNUM, a five-letter code. The enciphering processes were indicated by letters CIFOL or VEVAZ.[300]

(7.) ABABA BCBCB CDCDC. This system was exclusively employed in the Far East and consisted of a very primitive basic code enciphered by transposition. It was not read after New Year, 1944, because interception became impossible.

(8.) A system used by Satō, Oshima's counter-intelligence man, to pass messages which Satō did not wish to come to the attention of the Ambassador. For each letter of the alphabet two digits were substituted. The resulting text was then enciphered by a repeating additive of ten figures which never changed.

(9.) A machine which apparently consisted of two enciphering wheels, one with six letters of the alphabet, the other with the remaining twenty. This system was read until February, 1939.

[297] See also I-31, 8; I-84, 5. This is probably identical with the Kennwort (indicator) code mentioned by Rave (I-22, 8) and Beyreuther (I-150, 8).

[298] The apparatus was called the Bigrammsuchgeraet "the bigram-searching machine" (I-31, 4). Weber himself says traffic three to four days old was read (I-124, 3).

[299] Weber denies that any success was obtained with "new Jap systems" after August 1943. Weber may not be a reliable informant.

[300] I-31, 8; I-150, 8.

It was originally broken, however, by the Foreign Office Cryptanalytic Section (Pers ZS).[301] After 1939, the machine was replaced by another machine, and this second machine was never broken by any German cryptanalytic agency. When the Army cryptanalyst, Steinberg, who had worked on American machine systems, was transferred to OKW/Chi in November 1944, he was assigned the mission of attacking the Japanese machine.[302] To assist him, Steinberg had only one or two enlisted men. It was determined that, like the old machine, the new machine enciphered letters in two groups, a group of six and a group of twenty. The work, however, was interrupted by the end of the war, and no traffic in this system was ever read.[303]

No Japanese Military Attaché systems, either Rikugun or Kaigun, were ever read, although they were attacked at various times.[304] Huettenhain himself investigated them in 1943. In 1942, a very favorable opportunity offered itself when the Germans passed the details of certain book recoveries to the Japanese. These details were passed by Hayashi to Tokyo in the Military Attaché system. Despite the wealth of cribs offered by this process, the Germans did not succeed in solving the system.[305]

Adler's section also worked with Chinese, although not many people were engaged on this. No Chinese systems were ever referred to the research section.[306] The only clear success we are certain of was with the Chinese Military Attaché system which was discontinued in April or May, 1943. This was a three-letter code, and the first groups were always EFR SKW JKW. The encipherment consisted of transposition within the code groups.

[301] From Huettenhain, I-118, 7.

[302] I-150, 5.

[303] I-31, 8; I-118, 7-8, from Huettenhain. Buggisch's idea (I-64,3) that Steinberg solved the machine is certainly wrong.

[304] I-84, 5; I-118, 7; I-31, 8.

[305] I-31, 9.

[306] I-31, 9.

The encipherment was solved, but no messages were ever read.[307] Chinese traffic with the discriminant NKDBN was also "investigated", with what success we do not know. It consisted of three-letter groups, unenciphered, with many spells. Apparently enough traffic was read to show that it was of a purely military character.[308] Some Manchurian material was also worked on, but no details are known.[309]

i. Italy:

Senior Specialist Raffel was head of the Italian desk.[310] The section contained thirty-five to forty people and apparently had considerable success. Senior Specialist Paschke, of the Foreign Office Cryptanalytic Section (Pers ZS) said that between 1935 and 1942 his people had "read everything" in Italian, and it is likely that their results were passed on to OKW/Chi. We know that OKW/Chi read a diplomatic system called AR 22, and the Impero Code. Between 1942 and 1943, the Italians increased their additive material and employed digraphic substitution. After the surrender of the Italian Government, the Impero Code continued to be read by the Foreign Office Cryptanalytic Section (Pers ZS) for a while. Later, there was no longer sufficient depth to do this, and it was suspected that a double transposition was being employed. The systems of the Neofascist Italian Republic were also read by the Foreign Office Cryptanalytic Section (Pers ZS). They used a 5,000-figure additive; during the last three months, they also used unenciphered books and an alphabetical book with a short additive called RA 1.[311]

j. Bulgaria, Rumania, Hungary, Finland:

At an early date a desk existed for attack on Bulgarian traffic.[312] At one time after its establishment this desk was headed by Rotter.[313] There was a Rumanian section headed by

[307] I-22, 8.

[308] I-22, 8.

[309] I-150, 9.

[310] I-96, 4; I-150, 3; I-123, 3; I-1, 20.

[311] I-22, 5; 8.

[312] I-36, 3.

[313] I-1, 20.

Major Lenschau, which also had existed for a long time and which at the end of the war contained six people.[314] A desk for Hungary also existed.[315] Finnish may have been worked on in the Scandinavian section. We know, however, no details of German successes against Germany's smaller allies.

k. Scandinavia:

In 1940, Scandinavia became a place of great military importance, and all Scandinavian work was transferred to OKW/Chi.[316] The Scandinavian Desk was headed by Senior Specialist Wevering and contained about six people.[317] The desk read only Swedish unenciphered codes for which the books had been captured.[318] In view of Huettenhain's interest in the Hagelin, it is likely that the research section devoted some attention to the Swedish diplomatic use of this device. He was able to recall a message of more than 5,000 letters sent by the Swedish Attaché in Moscow.[319] No Swedish Hagelin traffic, however, was ever read.

l. Switzerland:

There was apparently a separate desk for Swiss traffic headed by First Lt. Kunze.[320] Traffic enciphered on the Swiss Enigma was regularly read. Huettenhain said that the wiring was changed every three months, but the changes at Washington were not made at the same time as those in London. Cribs thus provided by the Washington Traffic for the London traffic made it possible to solve the London wirings.[321].

[314] I-150, 3; I-123, 3; I-36, 3; I-1, 20.

[315] I-150, 3.

[316] I-22, 21.

[317] I-150, 3; I-123, 3; I-36, 3; I-1, 20.

[318] I-31, 9.

[319] I-31, 7.

[320] From Mettig. The Foreign Office people said a Herr Jung-Fischer was head of desk; Beyreuther, a Studienrat Dr. Peters. Trappe (I-123, 3) says work on Swiss was carried on by Mueller's French desk.

[321] I-31, 14.

m. Vatican, Greece:

Around the beginning of the war, a desk was established for attacks on Vatican traffic. Seifert, a former member of the Austrian Cryptanalytic Bureau, joined OKW/Chi at the time of the Anschluss and broke a Vatican book.[322] A small Greek desk existed under Cpl. Dr. Poetsgens.[323] Seifert also seems to have concerned himself with Greek systems, and is said to have broken one or more Greek books.

n. Spain, Portugal, Latin America:

We do not know what was accomplished by the small desk for Latin America, Spain, and Portugal, headed by Specialist Dr. Kiefer.[324]

o. Agents' Traffic:

Codes and ciphers of enemy and neutral agents were not a regular commitment of OKW/Chi. They were handled by the Agents' Section of In 7/VI, sometimes called Vauck's Section from its head, first Lt. Vauck. Nominally attached to In 7/VI, actually it was detached to Group III of the Radio Defense Corps (Fu III), which, it will be recalled, was concerned with the interception of agents' traffic.[325] Located at Dorf Zinna, near Jueterbog, the group acted more or less independently.[326] It is not clear whether the 6,000 agents' messages, which, deciphered and translated, formed a portion of the production claimed for OKW/Chi in the Kettler report of June, 1944, were actually turned out by OKW/Chi or by Vauck.[327] It is much more likely, however, that Vauck had nothing to do with these messages and that they were actually part of the work of Kettler's own organization. Occasionally more difficult problems were

[322] I-118, 3. He is also stated to have broken Polish, Turkish, and Greek books.

[323] I-150, 3. The Foreign Office informants said Seifert was head of the Greek Desk and that Poestgen, Bruckmann and Ruesing were "also active on a more or less independent footing".

[324] I-150, 3; I-123, 3; I-1, 20.

[325] See above, Chapter III.

[326] I-115, 6.

[327] DF-9, 3.

turned over by Vauck to OKW/Chi. One example of this is the case of the signals from the so-called Rote 3 (Red 3) Network, a Russian agents' network operating from Switzerland. Signals from this source were dealt with by Professor Nowopaschenny, Trappe and Schmidt of OKW/Chi early in 1943. Schmidt succeeded in solving ten of these messages, and Vauck's people then discovered that the encipherment was based on a book. Apparently, however, this was not enough to solve all the traffic passed by the network.[328]

The transfer of work on London-Warsaw traffic from the Agents' Section of In 7/VI to OKW/Chi in the autumn of 1943 has already been mentioned. This transfer was apparently a result of an appreciation of the importance of the traffic and of a desire to give work on it the limited distribution of the regular OKW/Chi VN's.[329] In the autumn of 1944, the whole of the Agents' Section of In 7/VI was subordinated to OKW/Chi. The group remained with Fu III, however, and its work was not affected by this paper change.[330]

8. Cryptanalytic Research, Security, and Development. While the crypto-linguists had a steady and unified mission, the research cryptanalysts of Huettenhain's section in OKW/Chi were pulled in two directions - towards the cryptolinguists whom they could assist in the solution of enemy systems and towards the cryptographers who were interested in security scrutiny of German systems. Research cryptanalytic work in the first field has already been mentioned. In some cases, it was merely a matter of detaching a few people to assist a language section, as for example Weber and his "Digraphic Weight Recorder" Rapid Analytic machine assisted in the solution of the Japanese transposition system. Only a few people seem to have been employed in the unsuccessful attack on the United States enciphered code. Not more than three participated in the study of the later Japanese diplomatic machine.

[328] I-132, 2. See also I-115, 7. T 1620 contains material relating to the "Rote 3" affair.

[329] See above under Poland.

[330] I-115, 6.

How many were employed regularly on the Polish diplomatic stencil we do not know-probably not many. The attack on the United States strip system was perhaps originally a larger effort. The research cryptanalysts seem, in addition, to have made a detailed study of the various Hagelin machines and to have obtained plain text for the linguists, at least in the case of the simplest type, the French C-36. Huettenhain outlined the various methods by which the C-36 could be solved:[331]

from messages in depth

from stereotyped beginnings, where a crib of five or six letters could be confirmed if the cipher text contained more than 323 letters

by statistical means without any cribs when the text was sufficiently long

Their investigations also extended to the more difficult later Hagelin development, the BC-38,[332] and here the general principles of solution were also understood:

solution of messages in depth

solution made possible by errors in wheel setting and consequent retransmission

general statistical solution employing Pearson's X^2 test.

For this last method an artificial message of five thousand letters was used.[333] Results could be checked step by step and the work was brought to a stage where it was apparent that final solution would have been possible. No actual traffic was ever solved by this method, however, despite the fact that a Swedish message of more than five thousand letters was available.[334] The Finnish Hagelin seems never to have been attacked.[335] So far as is known, OKW/Chi did not concern

[331] I-45, 6.

[332] I-45, 7-8.

[333] I-48, 2; I-31, 7.

[334] I-31, 7; I-31, 9.

[335] I-31, 7.

itself officially with the solution of any United States Hagelin traffic. The French B-211, both in the original and in the modified form, and the Russian B-211 were also studied. The section had time for a small amount of purely theoretical work, as for example, Dr. Schulze's study of the X^2 test.[336] Huettenhain was thinking of suggesting "A general theory for the solution of Double Transposition" as a doctoral dissertation. Such work could be kept secret by arrangement with the university authorities.[337]

Probably one of the outstanding achievements of the OKW/Chi cryptanalytic section was the development of various types of rapid cryptanalytic machinery.[338] We have already had occasion to notice the use of this machinery in attacks on cryptographic systems such as the Japanese transposition, the Polish stencil, and the American strip. The section also did a small amount of work in assisting in the development of cipher devices. We hear of a relay mechanism for changing teleprinter letters to digits and thus producing an additive for the use of the Navy.[339] The machinery was extensively used, too, in the security scrutiny of German cipher systems. The machines were shown, as developed, to the other German cryptologic agencies, which could, if they wished, order models for their own use.[340]

Cryptanalytic machinery was first introduced into German signal intelligence work with the adoption of IBM machinery by the Army in 1941.[341] OKW/Chi did not have any IBM machinery[342]

[336] I-84, 2.

[337] I-31, 6.

[338] A detailed discussion of this machinery as well as a more technical treatment of the various cryptographic devices mentioned in this chapter will be found in volume 2 of this report.

[339] I-20, p. 5.

[340] I-31, 10.

[341] I-93, 5.

[342] I-67, 2-3; I-96, 13. Despite this, Huettenhain speaks of using IBM equipment. This must have been the Army's equipment. The Army cryptanalytic agency and OKW/Chi were neighbors. (See below Chapter V.)

and may have made use of the Army's equipment for this purpose. Instead of acquiring IBM machinery for themselves, OKW/Chi established its machine section for the development of special equipment. This equipment was to be used in the first place for security scrutiny of German systems.[343] Huettenhain explained that IBM machinery can be used only for processes which can be reduced to sorting.[344] For processes which could not be so reduced, it was necessary to develop special apparatus. In general, the aim of the section was to build reading and recording apparatus in all conceivable forms in order to put together suitable equipment as soon as a practical problem arose.[345] The machine section was one of the show places of OKW/Chi. Capt. Bigi of the Italian Army saw it in 1942 and was impressed.[346] Certain Army cryptanalysts such as Buggisch made use of the machinery on some occasions.[347] Toward the end of the war, OKW/Chi was empowered to take over the IBM machinery of the Army, but because of the chaotic condition of affairs at that time, this was never actually done.[348]

The energy spent on developing cryptanalytic devices could be used for either cryptanalysis or security scrutiny. An increasing amount of the available expert manpower of the research section, however, was spent on security research and on the resulting problems in the development of cipher devices. The organizational changes expressive of this general tendency have already been traced. The overlapping of security and development work in the Army and OKW/Chi was remedied only at the end of the war when OKW/Chi took over the security and development personnel from the Army. Throughout most of the war there was considerable duplication of effort and a very intimate liaison between Huettenhain and the Army security

[343] I-31, 3.

[344] I-37, p. 2.

[345] I-37, 9.

[346] I-78, 11.

[347] I-58, 7.

[348] D-55, 4.

people.[349] Most security problems were presented to TICOM in the form of joint reports by Huettenhain and Fricke. Fricke, it will be recalled, spent most of the war in Army security research. As a result, it is often difficult to determine what work was done by the Army and what by OKW/Chi.

The chief German cryptographic device was the Enigma. It is possible that OKW/Chi - or rather its predecessor, the Reichswehr Cryptologic Section - was responsible for its adoption. In any case, Fenner had a hand in developing the device.[350] Once adopted, the device was privately produced.[351] The Enigma was produced in three principal models and OKW/Chi had apparently worked on all of them. The simplest form of the machine known as the Commercial Enigma had three wheels with a uniform motion and a fixed end-plate. Huettenhain's research section knew very well that this machine could be solved:[352]

with a depth of twenty to twenty-five messages.

with a short crib.

without a crib by running the cipher text against a catalogue of the results obtained by enciphering the letter E, the most common German letter, in all possible positions of the machine (the so-called E-strip).

The Commercial Enigma was used by the German railways and as a result of OKW/Chi's investigations, new instructions for its use were introduced which required the double encipherment of every message.[353]

A second form of the Enigma, known as the "counter" Enigma, had three wheels with an irregular motion and a movable reflector wheel. This machine was used by military attachés until around the middle of 1943. At that time it was shown that the device could be broken on a ten-letter crib. The machines were withdrawn from the military attachés and replaced by the military type of Enigma. The "counter" Enigmas

[349] See I-67, 2-3.

[350] I-84, 2.

[351] I-84, 3.

[352] I-45.

[353] I-92, 4-5.

were collected by the Radio Defense Corps for use by Military Intelligence (*Abwehr*). *Menzer worked on a new set of instruct*ions for the use of the machine by the Abwehr people.[355]

The most common variety of Enigma, the one used in the field by the Army and Air Force, was the Plugboard Enigma. This was identical with the Commercial Enigma mentioned above except that an additional monoalphabetic substitution was applied to the letters as they entered the wheel-maze and another as they came out, by means of plugs connecting one entry position with another. This plugging was known as the "Stecker". This device was the keystone of the German cipher security structure during most of the war.

Shortly after the beginning of the war, in October 1939, the Germans learned from a captured Polish Officer named Ružek that the Enigma had been worked on in conjunction with the French.[356] Ružek did not say the Enigma had been read. In the remnants of the Polish cryptanalytic bureau files, the plain texts of three German messages known to have been transmitted from a German cruiser in Spanish waters during the Spanish Civil War were found.[357] It is said that there were many interrogations at the time, but the interrogators "drew a blank".[358] They did not find out whether the messages were obtained by cryptanalysis or by physical compromise. At the interrogations in Warsaw in 1942, one of the Poles interrogated was a lieutenant colonel, the head of the Polish cryptanalytic bureau. A second series of interrogations was held in Berlin later in 1942.[359] In 1943 the case was reopened and

[355] I-77; I-92, 4-5.

[356] I-31, 3. This incident became known as the "Fall Wicher" or Wicher Case, from the fact that the Polish cryptanalytic bureau was located at Wicher, Poland. (I-78, p 7). Buggisch, however, (I-92, p 5) thought that Wicher was the Polish cover name for the solution operation.

[357] I-127, 5.

[358] Hentze of the Army Signal Intelligence Service states (I-113, 4); "They had learned from a Polish officer that the Poles had read it [the Enigma] before Stecker was introduced and that Stecker had been brought in in consequence."

[359] The exact date of the interrogations is not stated.

the prisoners interrogated again. No information was obtained. Mettig attributed this lack of success to the stupidity of the Abwehr, which left the prisoners together before the interrogations so that they had an opportunity to agree on a consistent story. Present at the interrogations besides Mettig, who probably attended as Chief of Inspectorate 7/VI (In 7/VI), were Steinberg and Pietsch, two Army cryptanalysts, and a Captain Singer, who represented the Navy. Mettig did not recall whether Huettenhain was present or not.[360]

In the West, the Germans had no better luck. They were able to discover nothing in Belgium that threw any light on the vulnerability of their cryptographic systems. When Paris was captured, the French cryptanalytic agency, the Deuxième Bureau, was visited but it had been moved to Vichy. When Vichy was occupied, no search was made.[361] From interrogations and visits to the cryptanalytic agencies of conquered countries, therefore, the Germans got no conclusive evidence that the Enigma was being broken, but enough was found to arouse their suspicions.

In the interrogations and investigations consequent to the Polish discovery, the Army was primarily concerned. It is quite certain, however, that the doubts which were raised about German security had repercussions in OKW/Chi and that Huettenhain's research people did some work on the Enigma. Their precise responsibility for the change in the indicator technique, which was one of the results of the Polish incident, is not certain. Huettenhain, at least, mentions the possibility of a solution resulting from faulty indicator procedure. He also thought that a general solution might be theoretically possible by the use of an E-strip as in the case of the Commercial Enigma.[362] Such a solution, however, would be slow and would take an enormous assembly of equipment and personnel. It was never actually attempted in Germany. OKW/Chi's final general judgment on the Plugboard Enigma seems to have been that the device was secure if used according to regulations. They

[360] I-127, 5.

[361] I-31, 3.

[362] I-45, 4.

were aware that solution might be possible by means of stereotyped beginnings, stereotyped messages, or a number of messages in depth. No texts of messages actually transmitted in the field were ever made available to OKW/Chi by any branch of the armed forces. The enforcement of cryptographic regulations in the field, however indirectly, was no part of the duty of OKW/-Chi. It is worth noting that early in 1944 the German Navy became concerned about their cryptographic security as a result of heavy U-boat losses in 1943 and early 1944. A naval lieutenant named Frowein was detached from the Signal Intelligence Agency of the Navy High Command (OKM/4 SKL/III) to the Signal Security Agency of the Navy High Command (OKM/4 SKL/II),[363] to study the Naval Enigma. The Naval Enigma was like the army and airforce machines, but it had four wheels instead of three and, therefore, a higher degree of theoretical security. Frowein broke the naval machine with known wheels on a crib of twenty-five letters.[364]

OKW/Chi's cryptanalysts had a generally uneasy feeling about the security of the chief German ciphers. In a lecture given as part of the Chi conferences in the autumn of 1944, Lt. Dr. Stein told the assembled cryptographers that no German system was secure if the cryptographic regulations were violated. Without any authority to monitor actual traffic with a view to finding out how well the regulations were observed, all German cryptographic agencies, including OKW/Chi, were driven from security scrutiny to an attempt to develop cryptographic devices that would have a higher degree of theoretical invulnerability. OKW/Chi's contribution to increased security for the Enigma was a suggestion that the wheels be redesigned so that they could be given an irregular motion. This device, the "Changeable Turnover Rotor" (Lueckenfuellerwalze), was developed by OKW/Chi in conjunction with the Army cryptographers.[366] It meant that every Enigma machine in operation would have to be supplied with

[363] I-38, 2.

[364] I-38, 2. Cf. also I-95, 7 in which Morgenroth of OKM 4/SKL III states that Frowein investigated the Naval Enigma in the summer of 1944.

[366] I-104, p 2-3. It may be noted that the Russians visited the part of the firm of Heimsoeth and Rincke in Russian occupied Territory and removed from it a complete set of drawings for the Lueckenfuellerwalze but did not get a model, according to the members of the firm.

a new set of wheels. The wheels were never produced in great enough quantity so that the system could be changed. Side by side with the attempt to increase the security of the Enigma went an effort to develop entirely new cryptographic devices with the intention of replacing the Enigma entirely. One of the most interesting of these devices, the SG-39, a kind of combination of Enigma and Hagelin principles, was scheduled for production in the year 1939, but because of technical difficulties, lack of clarity in the operational requirements and, finally, the bombing out of factories capable of producing the device, the first experimental models were not ready for delivery before February or March 1945, and they never reached their destination in Berlin.[367] This device seems to have been mainly developed by the Army. The former Army cryptanalyst, Buggisch, was a specialist in the machine.[368] On the part of OKW/Chi, Menzer seems to have had the most fertile mind in the development of cryptographic devices. Between 1937 and 1939 he produced a purely mechanical machine called the M-40 and about thirty models were built. The machine was tested by the Army security people and found "moderately secure", but was actually never used.[369] One variety was to have been adopted for automatic Morse sending.[370] An invention of Menzer's of great practical significance was the SG-41,[371] this was a purely mechanical machine wherein the wheels had an irregular interlocking motion. The machine received the approval of the OKW/Chi cryptanalysts who considered that a fundamental weakness of the Hagelin had been overcome.[372] Like all machines of the Hagelin type, the SG-41 can be read in depth, but the setting of the

[367] I-57, 8. Major Barlow of the United States Army visited the firm which was building the SG 39, Telefonbau und Normalzeit. He reported it completely bombed out (I-52, p 2.)

[368] I-58, 6.

[369] I-118, 5; I-58, 5.

[370] I-84, 5.

[371] I-58, 5.

[372] I-31, 7.

machine cannot be recovered even from a very considerable length of key. The SG-41 was built, and used by German Agents, but it was never finally authorized for the army, largely because of interdepartmental differences of opinion, which seem to have been typical of the German signal intelligence set-up where the link leading from the cryptologic experts to the troops in the field seems to have been unusually long and tenuous. The technical development was in the hands of a Dr. Pupp of Army Ordnance Development and Testing Group, Signal Branch (Wa Pruef 7), and a few engineers from the Wanderer Works at Chemnitz were also concerned. The cryptographers spent a great deal of time in discussion as to whether the order of the letters on the printing wheel should be alphabetical. Gen. Fellgiebel decided that he wanted a machine with a keyboard. Consequently, the alphabetical arrangement on the printing wheel was not required; a mixed alphabet was used instead as adding some slight additional security. Production was started on this basis and a thousand machines were actually built. Then all the officers in the Army Signals Department decided that they wanted a smaller machine without a key board for use below the regiment. On such a machine an alphabetic arrangement of letters on the printing wheel was necessary; if such a machine was to be used with the key board machines, they too would have to have a regular alphabetical arrangement on the printing wheel. As a result of the change-over delay, the machine was never turned out in sufficient quantity for wide use. But a model with ten digits rather than letters was produced for the use of the weather services.[373]

Medium grade and low grade field systems were no concern of OKW/Chi until it took over all Army cryptographic work in the autumn of 1944. Fricke, who joined OKW/Chi along with other cryptographic experts, had, during his career with army security research,[374] shown the weaknesses of the Double Playfair system, which had been the Army medium-grade system at the outbreak of the war. He had been partly responsible for the development of the "Raster" transposition system which replaced it. The transposition system proved awkward for field use because the original metal grilles could not be turned

[373] I-72, 8ff.

[374] I-20, p 2.

out owing to a shortage of material, and paper grilles requiring constant replacement were used. OKW/Chi turned again to Menzer and became interested in a little device he had developed for agents called the "Schluesselkasten" (Literally "key box").[375] This was a device that looked like a slide rule with wheels. T-1620 contains the results of OKW/Chi's security investigation of this device and it was found to be very satisfactory for medium grade use.[376]

The OKW/Chi research section gave considerable attention to the security scrutiny and development of German teleprinting security devices. The Germans produced two series of such devices. The first series, distinguished by the letters SZ, were cryptographic devices separate from the teleprinter and attachable. Encipherment was effected by twelve mechanical (pin) wheels. The second series of devices were actually built into the teleprinter. The teleprinter and the device were designated by a number prefixed by the letter T. Encipherment was obtained by the use of ten wheels with fixed pin patterns.

The SZ series began to be developed in the year 1937 by the Army Ordnance Development and Testing Group Signal Branch (WA Pruef 7) in conjunction with the Lorenz Firm.[377] Originally, no expert cryptologic assistance was sought. In 1937, Menzer and Huettenhain visited Liebknecht, the representative of Army Ordnance Development and Testing Group Signal Branch (WA Pruef 7), and examined the first model, the SZ-40. It was shown that the cipher produced by this machine could be broken on a thousand letters of text without cribs or other assistance.[378] Only about a hundred of the

[375] I-57, 9.

[376] To some extent OKW/Chi concerned itself with the development of ciphers for German commercial firms as Huettenhain states (I-84, 4). The Military Intelligence (Abwehr) Office (possibly III-F) was responsible for the security of commercial firms' ciphers but when there were difficulties, Menzer of OKW/-Chi sometimes helped. Huettenhain himself had advised that when there was little traffic, the firms should use a one-time pad on a commercial book, such as ABC Code or Mosse.

[377] I-45, 16.

[378] I-31, 17.

DOCID: 3560827

machines were consequently produced, and, apparently in consultation with Menzer, a new model, the SZ-42, was designed.[379] This model, in turn, proved to be by no means impervious to cryptanalytic attack, and variations, designated SZ-42 A, B, and C, were developed on consultation with Huettenhain and his assistant, Dr. Stein.

The original models of the T series, the T-52 A and B, were produced by the firm of Siemens. These devices were examined by Huettenhain in 1939, and he showed that they had an extraordinarily low degree of security and could be broken on a hundred letters of cipher text without a crib. Changes in design were suggested to Siemens, including means of producing a non-uniform turning of the wheels, but for engineering reasons Siemens refused to accept these suggestions.[380] Instead, the T-52 was produced, which overcame some of the more obvious disadvantages of the earlier models. There were no short sub-periods in its keying sequence.[381] The T-52 C was studied by the Army cryptanalyst, Doering, in 1942, and he showed that it could be broken on a text of 1,000 letters.[382] In these studies OKW/Chi evidently had a hand because it is known that special cryptanalytic machinery, such as OKW/Chi had and the Army did not have, was used in the solution.[383] These investigations led to the production of the T-52 D. Security work, mainly by Doering, continued, and early in 1943 he

[379] I-31, 16. See I-57 for a paper by Liebknecht on his work at Wa Pruef 7 on the SZ 40, SZ 42, SFM T52 etc.

[380] I-31, 14.

[381] I-45, p 12.

[382] I-58, 6.

[383] I-45, 13 ff. On page 13 Huettenhain states: "Meanwhile the different deciphering machines (Entzifferungs hilfsgeraete) had shown their worth in solving cryptographic problems. Experiences had been gained particularly about the good work of these deciphering aids even at high speeds. With these prerequisites it was possible to give a method with which T 52 C could be solved by employing deciphering machines."

showed that the T-52 D was not secure either, and as a result, the T-52 E was produced.[384] It is likely that Huettenhain's section had some part in these researches, or at least that Huettenhain kept abreast of developments. He knew, for example, that T-52 D and E messages could be read on a depth of ten without a crib.[385] There follows the familiar story about difficulties in getting the Army to introduce and use the improved devices. The original Army position was that security did not make any difference with the teleprinter anyway because the signals went over lines and could not be intercepted. In the summer of 1942, for example, the T-52 A and B, shown to be woefully insecure three years earlier, were still being used, and the T-52 C, with all its faults, was being distributed. Evidence of line tapping found in Paris in the years 1942 and 1943 did something to arouse the Army signal authorities to the necessity for teleprinter security.[386] But again, the Germans were too late with their cipher development. The newly developed machines could not be generally introduced.

Throughout the war there was considerable interest in Germany in ciphony. The authority chiefly interested during most of the war was the war was the Army Ordnance Development and Testing Group, Signal Branch (Wa Pruef 7), which was in these matters represented by Liebknecht, whom we have already met in connection with teleprinter security devices. Liebknecht kept abreast of the experiments being conducted for the Army at the Vierling Laboratories. Various other German firms and individuals, for example, Siemens, which were also concerned with teleprinter security, worked more or less independently on the problem. OKW/Chi was not directly concerned, although Huettenhain and perhaps some of his associates were interested spectators.[387] The first effort at co-ordination was made in the summer of 1943 when all authorities and firms engaged in the development of speech encipherment were called together by Fellgiebel.[388] The aim of the meeting was to eliminate

[384] I-78, 11-12.

[385] I-31, p 14.

[386] I-78, 11 ff.

[387] I-20, par. 30 ff.

[388] I-44, 2.

overlapping work and to make it clear just what the Armed Forces wanted. They wanted: (1) As an immediate development, an improvement in their present ciphony methods. Here they would be willing to accept something very imperfect, if it could be got out quickly - and if interception were difficult; (2) as a long-term project, an absolutely secure system of special encipherment. The Army Ordnance Development and Testing Group, Signal Branch (Wa Pruef 7) had a representative at these meetings, but apparently OKW/Chi did not. Finally, in November 1944, Praun, the new Chief Signal Officer of the Armed Forces (Chef WNV), commissioned OKW/Chi to check developments in ciphony. This move was obviously a part of the program of Praun and Gimmler, whereby OKW/Chi was to be the central authority for all cryptographic materials in Germany. One of the Chi-conferences was devoted to ciphony, but again Chi was too late. "Owing to the general war situation", said Huettenhain and Fricke, "it was no longer possible to do this in such a way that technical details could be reliably reconstructed."[389]

Any arrangement for assuring a high degree of cryptographic security necessarily involves three steps:

the systems actually in use must be put into the hands of skilled cryptanalysts who are able to judge their effectiveness;

they must be thoroughly examined by these cryptanalysts, and if they are accepted as usable, the regulations for their use must be produced by the experts;

the recommendations of the cryptanalysts regarding acceptance or rejection of systems and regarding the use of systems finally accepted must be adequately enforced.

One can arrive at some conclusion regarding the success or failure of the German security effort by examining what they accomplished under these three points:

With regard to point one, the Germans were largely a failure. When the war began, the administration of German cryptographic systems was in a chaotic state. The signal authority of each branch of the armed forces did pretty much as it pleased, at times without regard to the recommendation of the cryptanalytic authorities. It will be recalled that prior to October, 1943, OKW/Chi, the highest-level German

[389] I-44, 2.

DOCID: 3560827

cryptologic agency, had no authority whatever to examine systems used by the branches of the armed forces. The Keitel order of October, 1943, which required at least the opinion of OKW/Chi before any system was adopted by any of the separate branches, was apparently very incompletely observed. Huettenhain states as a general truth, apparently valid for the entire course of the war, that "no compulsion was put on anyone to apply to OKW/Chi for security tests, except where the Army was concerned(to Fricke), and many organizations never thought of doing so."[390] After his accession to office in the summer of 1944, Gimmler seems to have made a real effort to establish OKW/Chi as a security authority for the separate branches. This effort came too late. Conditions were too chaotic for a complete examination of existing German systems, the constant air attacks made the mass production of any new cipher device almost impossible.

In regard to the second point, despite the lack of any real authority in the matter, OKW/Chi did manage to examine fairly thoroughly at least the leading Army and Air Force systems. They appraised correctly the weaknesses of the commercial and "counter" models of the Enigma. They at least saw that the plugboard Enigma was not invulnerable to attack. Huettenhain's early remark to interrogators to the effect that they knew the Enigma to be secure should not perhaps be taken too seriously.[391] One might even suggest that he was trying to trap his captors into some kind of an admission. Huettenhain's later statement, however, is to be taken at its face value: the official judgment of OKW/Chi was that the plugboard Enigma was secure if the instructions were observed. The development of such devices as the changeable turnover rotor, and the Enigma plugboard permuter, as well as the consideration of the various substitutes for the Enigma, such as the SG-39 and the SG-41, was not due to any immediate concern that they felt for the security of the cipher systems, but was intended to provide against future possibilities.

[390] I-31, 16. The translation of the document: "Never thought of doing so" is probably a faulty translation of the German idiom: "Hachten gar nichtdaran."

[391] I-2, p 4.

DOCID: 3560827

In his final decision on the Enigma, Huettenhain betrays a certain academic aloofness and, one is tempted to say, smugness, which may have been his leading flaw as a cryptographer. The standard mathematical tests had been applied to the device and regulations laid down on the basis of these tests. The possibility of other attacks not arising from a standard application of well-known mathematical procedures, but based on new discoveries, never seems to have been seriously considered by him. Allied to this academic attitude is the curious lack of interest which Huettenhain and the other German cryptographers seemed to have shown in the actual size of the Allied cryptanalytic effort against the German systems. The Germans knew of the Deuxième Bureau. They knew nothing, however, of English cryptanalysis - "the English, of course are notoriously stupid." - All they knew about American cryptanalysis they had learned from Yardley's Black Chamber.[392] One prisoner-of-war captured by the Germans in North Africa mentioned a very large park of IBM Machines operated jointly by the British and Americans. This hint was never followed up.[393]

This academic aloofness of OKW/Chi was probably only partly responsible for the almost complete German failure with regard to point three. It was only with the greatest difficulty that devices demonstrably insecure like the T-52 A and B were actually withdrawn from use, or new and secure devices introduced. The regulations for the use of cipher devices, once they had left the hands of OKW/Chi, were entirely outside their competence.[394] The Army refused to submit live traffic to the cryptanalysts for analysis or monitoring from a security point of view. Gimmler's insistence on a more vital connection between the security center and the troops in the field, a connection, it will be recalled, that was to be carried out through Capt. Bernsdorff's sub-section, was amply justified. But the scheme, though good, was too late. By January, 1945, conditions were too chaotic to put it into effect. The chance for effective security control had passed.

[392] I-48, 2.

[393] I-84, 6.

[394] I-20, par. 11. Fricke (I-20 par. 28) states that Oberpostrat Halder in the office of the Military Attaché at Stockholm astonished OKW/Chi by asking that T 52 keys be sent in clear !

DOCID: 3560827

9. Miscellaneous Operations. a. Broadcast Monitoring: The department located at the Fehrbelliner Platz, in Berlin, (finally called Section VI) put out its findings in a daily newspaper called the "Chi Nachrichten" ("Chi Reports").[395] These reports were divided into sections devoted to military affairs, economic affairs, and so on, with one section given over to comments. The material for the reports came from the news broadcasts and other plain-language material picked up by the broadcast intercepting system. Originally, these reports had a fairly wide distribution. Every section in OKW/Chi got a copy, and probably many of the higher ups. After Stalingrad, when the news became less favorable from the German point of view, the Chi Reports received increasingly narrow distribution until finally Keitel's approval had to be obtained before anyone could receive a copy. In effect, Keitel became the distribution agency for the Reports. One copy, however, continued to go to the OKW/Chi Archives, and the head of the Archives, Dr. Schaedel, gave Gimmler a daily briefing on the news.

Besides the Chi Reports the monitoring section published special reports which it sent regularly to interested authorities. Russian news, for example, was regularly passed on to the Department of Armed Forces Propaganda which used it as material for its newspaper for the anti-Soviet Russian troops fighting on the German side. For some time, previous to 6 June 1944, all references to the coming invasion were compiled into a single report which was sent daily to the "Department of Foreign Armies West" (Abteilung Fremde Heere West). References to German prisoners-of-war in Allied hands were also included in a special report for separate distribution. The information was probably passed on eventually to the relatives of the prisoners, and thus the effectiveness of the PW broadcasts as bait to the German public to listen to Allied propaganda broadcasts was probably destroyed.

b. Attacks on Ciphony Devices: One of the most interesting items to appear in the Chi Reports was doubtless political conversations between Churchill and Roosevelt, carried on over a radio telephone link between London and Washington. The German informants state that this link was evidently not intended to have any very high degree of security, since an

[395] I-150, 11. For a discussion of the Chi-Nachrichten see also I-96, 16.

DOCID: 3560827

operator warned the conversing parties whenever the talk approached highly secret matters. The transmission, however, was not in clear, but scrambled. The intercept took place at the broadcast monitoring station at Ludwigsfelde by means of a descrambling apparatus developed by the Army Ordnance Development and Testing Group, Signal Branch (Wa Pruef 7). This apparatus is said to have been completely effective, and changes in the key of the scrambler could be easily followed by turning a few knobs.[396]

In June, 1944, the Army cryptanalyst, Buggisch, was assigned to the experimental intercept station at Staats, conducted by the Army Ordnance Development and Testing Group, Signal Branch (Wa Pruef 7). Here his mission was to study the Russian scrambler known as X^2.[397] Apparently at the time of the organizational changes of November, 1944, Buggisch became a member of OKW/Chi. With the exception of a six-weeks stay in Berlin, he continued his work at Staats.[398] He was not successful in solving the scrambler. Some interest at OKW/Chi was aroused by a ciphony device recovered intact from a crashed American Mustang plane. This device was kept on an airfield for six months before it finally was identified as being a cipher device, and it reached OKW/Chi in the spring of 1945. There it was handed over to the Army Ordnance Department (HWA) where it was worked on by Buggisch and a Dr. Lotze.[399] Their investigations are said to have been inconclusive. It was possible to reconstruct the key setting from

[396] I-84, 6; I-118, 4. In I-88 Mr. K. Vetterlein of Abt IIIc of the Research Institute of the Reichspost Ministry revealed that the Germans had constructed apparatus which was used to restore the "scrambled" radio circuits in use between Britain and the United States to complete intelligibility. Vetterlein started work in 1940, by 1942 the equipment was working on a 24-hour basis at Kelheim in the Munich area. The records of the speech were sent to the Propaganda Minister at Berlin. By April 1945 they had also succeeded in deciphering to some extent teletype messages sent over the same circuit. The work of Vetterlein and the Reichspost evidently had no connection with the OKW effort at Ludwigsfelde.

[397] I-73, 2.

[398] I-31, 12. I-58, 4.

[399] I-31, 12; I-118, 4.

intercepted oscillograms. But it was doubtful whether solution could have been rapid enough to be of any use during an actual fighting operation.

c. Training: Training was a regular part of the operations of OKW/Chi. Occasionally, special courses were given. Herold's training tour in 1941 may be recalled in this connection. Kettler's report mentions that, in the Spring of 1944, some Bulgarian officers were given a special course in elementary cryptology, and some German Air Force officers, a special advanced course.[400] Most of the training, however, was for the benefit of OKW/Chi's own personnel. Huettenhain mentions that when he first came to the cipher section, in 1937, he was allocated to a training section for the first six months. There he worked on low-grade Spanish government military systems for practice.[401] For members of the language sections the training procedure, which had been followed since as early as 1930, was somewhat different.[402] These members came to OKW/Chi trained in the language in which they were to work, and it is likely that during the war the military personnel was drawn from such special Army language training units as the Interpreters' Replacement and Training Battalion, in Berlin. Once in OKW/Chi, they were introduced to cryptanalysis gradually, concurrently with their work as linguists. A course was conducted for two days per week during the six winter months. Each new member was expected to attend this course for two winters. During the first winter, substitution ciphers were studied; during the second, transposition. Originally, the course was conducted by Fenner, than by Fenner and Wendland. During the war, it was conducted by Wendland and Huettenhain. Attendance at these courses was about three to twelve persons per winter. This indicates that only the more prominent personnel in the language sections were given the courses. Candidates received into the research cryptanalytic section got two to four months continuous training, at the end of which they were supposed to be able to tackle unsolved problems. In the summer of 1943, Huettenhain started an advanced cryptanalytic course for which eight of the most able cryptanalysts were detached from the language sections.[403]

[400] DF-9, 3.

[401] I-31, 2.

[402] I-118, 2, 3.

[403] Cf. Beyreuther's statement (I-150, 9) that he had heard about Dr. Huettenhain giving lectures about decoding work.

Those who were admitted were expected to be able to break systems independently in the language sections. The scheme was perhaps to relieve pressure on the research section, which was becoming increasingly involved with security problems. The course met for three two-hour periods each week but the total duration was not fixed. The syllabus included mathematical bases for cryptanalytic work, related cryptanalytic problems, machine ciphers, IBM and other cryptanalytic machines, German ciphers, practical work. Members of the course were expected to do a considerable amount of independent research. In November, 1944, because of the general situation, the course was dropped.

Chapter V. Relations with Other Cryptologic Agencies Paragraph

OKW/Chi's Relations with the Signal Intelligence Services of Army, Navy, and Air Force. 10

OKW/Chi and Other German High-Level Signal Intelligence Agencies. 11

Liaison with Foreign Signal Intelligence Agencies. . .12

10. OKW/Chi's relations with the Signal Intelligence Services of Army, Navy, and Air Force. These varied with the field of effort. In the matter of Intercept, and in Security Scrutiny, OKW/Chi actually exercised some control over the other three agencies; but in the field of cryptanalysis the material was divided so that each agency had its own logical assignment. Army cryptanalysts attacked enemy army systems; Navy cryptanalysts attacked enemy naval systems; Air Force cryptanalysts attacked enemy air force systems. OKW/Chi left the Army, Navy, and Air Force systems almost completely alone and worked on diplomatic and military attaché traffic. This is not to say that there was no liaison among the four agencies in cryptanalytic matters; there was both liaison and cooperation. But OKW/Chi did not control the activities of the other Signal Intelligence Services in this field.

In general, no material was passed from the branches to OKW/Chi. Kettler was emphatic on this point.[411] This arrangement seems to have held throughout the war with some apparent exceptions. Dettmann, for instance, told the interrogators that in the years 1942 and 1943 his army unit had passed considerable Russian five-letter traffic to OKW/Chi.[412] The traffic in question was probably diplomatic or at least was suspected of being diplomatic. Capt. Herold, it will be recalled, stated that his air intercept unit at Varna passed material back to Berlin, to OKW/Chi.[413] If Herold was not mistaken,

[411] I-21, p 1.

[412] I-116, 2.

[413] I-130, 13.

this was wholly exceptional. The special direction to the separate branches in the Praun order of 5 September 1944 to pass on diplomatic material to OKW suggests that there may have been some difficulty in keeping the cryptological services of the individual branches from poaching on OKW/Chi's own preserves.

Occasionally Huettenhain seems to have been consulted about the cryptanalytic difficulties of the separate branches. This was, however, a purely informal matter. Even in the case of the M-209 of the United States of America, British Typex, and the "big American Machine", OKW/Chi was not called in by the Agencies working on them. The German Army, Navy, and Air Force worked independently on the M-209 of the U.S. Army, Navy, and Air Force, and constantly exchanged among themselves all technical data, but OKW/Chi took up the study of the M-209 only in passing and because it might be used for diplomatic traffic sometime in the future.

An attempt of OKW/Chi to achieve a certain amount of coordination seems to have been made in the field of intercept. It has already been pointed out that the original plan seems to have been to subordinate all intercept stations in neutral countries to OKW. Herold's experiences at Varna have already been mentioned.[414] Even when that plan was in its early stages, the German Navy refused to participate, and we must assume that OKW/Chi had no real authority to compel its cooperation. The plan was a failure. By the end of the war, only remnants of the original scheme, such as the existence of an OKW and Navy intercept station on the same site near Seville, remained. However, according to Keitel, OKW/Chi was the intercept clearing house, when needed, for all the Services. The intercept systems of the separate branches were apparently never an important source of traffic in OKW's own field. We have already seen that Col. Randewig had a scheme very early in the war for an extensive interservice intercept structure. Randewig's plan remained a dream. His memoranda to the Chief Signal Officer of OKW seem to have been considered a nuisance. No such extensive plan as his was ever even considered by OKW/Chi.

The development of cryptographic devices for use by the troops was originally left entirely to the individual branches. It has already been noted that development was partly taken over from the Army in the autumn of 1944. The other branches kept their right to originate until the end, although OKW/Chi had the right of review.

[414] I-130, 13.

DOCID: 3560827

OKW/Chi's greatest effort to assert its authority as a coordinating agency was made in the field of security scrutiny. The development of this effort is a basic element in the history of the organization of OKW/Chi and has been traced. It is worthy of note that despite Keitel's order of October 1943, little real effort was made by OKW/Chi to assume effective supervision of the security of all branches until Gimmler took office almost a year later.[415] In August 1944, the representatives of the separate branches met those of OKW/Chi at Chi-conferences. After August 1944, there was insufficient time left to overcome the difficulties caused by the neglect of five years. The minutes of some of the Chi-conferences are available, and it is apparent that not very much was accomplished. The first meeting of which we have a record was largely devoted to a discussion of OKW/Chi's authority in matters of security scrutiny. The other meetings were filled with talks of a more or less general nature by OKW/Chi's leading cryptanalysts. No new devices were submitted to OKW/Chi by the separate branches for security testing during this period, because the deterioration of German production made it impossible to introduce any new devices. In the security scrutiny of cryptographic systems already employed by the separate branches nothing seems to have been accomplished. As we have seen, the theoretical limitations of these systems were increasingly apparent to OKW/Chi. The Chi-conferences never succeeded in producing any actual traffic for examination, and apparently left the adherence of the German troops to the cryptographic regulations a matter of pious hope.

We now turn to a separate examination of OKW/Chi's relations to the Signal Intelligence Services of each of the separate branches.

Relations were closest with the Signal Intelligence Service of the Army. This is to be expected in view of the fact that the whole OKW structure was more intimately associated with the Army than with the Navy or the Air Force. The Chief Signal Officer of the Supreme Command of the Armed Forces (Chef WNV) also acted as Chief Signal Officer of the Army (Chef HNW). The officers who controlled OKW/Chi and the Signal Intelligence Service of the Army were drawn from the same set of regular German signal officers. Boetzel, who ended the war as head of the Army Signal Intelligence Service, had once been second in

[415] See I-84, 4.

DOCID: 3560827

command of OKW/Chi. Before he became head of OKW/Chi, Kettler had been associated with an Army Signal Intelligence Unit. For a while, he had been head of the principal Army intercept unit in the east. Mettig, who ended the war as second in command of OKW/Chi, had previously been head of the Army cryptanalytic agency. Furthermore, OKW/Chi and the highest echelon Army cryptanalytic agency were originally located very close to each other in Berlin, in the Tirpitzufer section. So close was the liaison between Army and OKW on command level that an Italian captain, Bigi, who visited the German Signal Intelligence Services in December 1942, seems to have thought that OKW/Chi and the Army cryptanalytic agency were actually one unit. When he was captured much later, this Italian told interrogators that German signal intelligence was under Colonel Kempf, and that subordinate to Kempf was Fenner who was in charge of diplomatic material and Major Mang who was in charge of military material.[416] We now know that Bigi was quite wrong. Kempf was head of OKW/Chi in December 1942; Fenner was subordinate to him, and in charge of cryptanalysis. Mang was head of the Army cryptanalytic agency and in no way subordinate to Kempf. But the fact that Bigi could have made this mistake indicates that the actual cooperation between these two agencies was extremely close. The officers seemed to have been well satisfied with the relations between the Army cryptanalytic agency and OKW/Chi. Huettenhain, on the other hand, who represented the civilian specialist point of view, was not so well atisfied. He told interrogators that "liaison with OKH was not such as the younger men would have wished, nor such as would be natural in scientific work. But the"Higher-ups" had a private war on and liaison among specialists was discouraged."[417] One may perhaps doubt that this statement means much more than that the organizational lines were held and indiscriminate contact between the two services prevented. Actually Huettenhain himself seems to have worked most intimately with the Army cryptanalysts. He knew a great deal about special Army problems, such as the work on Typex, which were no official concern whatever of OKW/Chi. Buggisch, one of the leading Army cryptanalysts, seems likewise to have had a very good knowledge of what went on at OKW/Chi. He mentions conferences with the OKW/Chi specialists on the security of German cryptographic devices and on the

[416] IF-1517 is Captain Bigi's report on German signal intelligence.

[417] I-31, p 10.

DOCID: 3560827

Hagelin machine in the summer of 1943, long before the official Chi-conferences were started.[418] He also speaks of a visit which he paid to the cryptanalytic machine section of OKW/Chi.[419] For a while, Army cryptographic devices seem to have been submitted to a double security check, one by the Army and one by OKW/Chi.[420] This duplication of effort was eliminated when the Army security people were incorporated into OKW/Chi in November 1944. The intimate liaison between the Army and OKW/Chi seems to have existed only on a higher level, particularly with regard to security. OKW/Chi specialists were never permitted to know precisely what was going on in the field. The Army cryptanalysts, moreover, apparently labored under the same difficulties. Fricke says that the Army had been using an amazingly insecure system, (the socalled Barbaraschluessel or "Barbara Keys") for weather traffic from 1939 to 1944. It was not until that late date (1944) that OKW/Chi heard about it.[421] Presumably, the Army cryptanalysts had not heard about it either.

Contact with the Air Force was more lax. The head of the Air Force Signal Intelligence Service, Lt. Col. Friedrich, a prisoner of TICOM, was asked about his relations with OKW/Chi. Although he was an extraordinarily communicative prisoner, on the subject of OKW he could give very little information. Apparently this was because he knew very little about the organization and was rather bored by it. He remembered that decoded traffic had been sent to him by OKW/Chi but said it was of no use whatever to him and he stopped reading it.[422] His cryptanalysts, he said, "got nothing from OKW."[423]

[418] I-58, 3; I-72, 6.

[419] I-58, 3.

[420] Buggisch states (I-72, 6), "The types of small Hagelin known in the year 41 (C 36 and BC 38) did not satisfy the security demands set by OKW/Chi and OKH/In 7."

[421] I-20, p 7.

[422] I-13, 6.

[423] I-13, 1.

(Friedrich made it very clear that he did not think very much in general of cryptanalysts or of cryptanalysis). There was a little more contact than he implies. Mettig told his first interrogator that he had had some liaison with Dr. Voegele, chief cryptanalyst of the German Air Force.[424] Voegele himself was interrogated later and gave some details of what this liaison actually amounted to. He had worked in the early part of the war on the British Government Telegraph Code and later got a photo copy of it from OKW.[425] In 1940 and 1942, he had exchanged traffic in the Interdepartmental Cypher, results of the reconstruction of the recipher book used with it with OKW as well as with the Navy.[426] In 1945, messages and items in a United States code were exchanged with OKW and the Army.[427] He also had on order from OKW a cryptanalytic machine employed for an attack on the American strip cipher.[428] Apparently he never received the machine; but he was rather dubious about its efficiency in any case. He said he could get along well enough on American strip with IBM machinery. Voegele showed OKW as well as the Foreign Office the method of attack on the American strip cipher which his organization had developed.[429] He did not know what use, if any, OKW/Chi had made of this method. Huettenhain says that he gave some assistance to the GAF weather service in their attack on an English meteorological system.[430] This assistance consisted in putting at their disposal a cryptanalytic device which Huettenhain called the Bigrammsuchgeraet (digraph "weight" recorder). Even with the assistance of Huettenhain and his machine, however, the weather service failed to solve

[424] I-17, 2.

[425] I-112, 6.

[426] I-119, 4.

[427] I-112, 9.

[428] I-112, 4.

[429] I-119, 3.

[430] I-31, 4; I-84, p 2, p 7.

the cipher. One cryptographic achievement of the German Air Force was the development of the Enigma plugboard permuter. This device seems to have been developed entirely by the Air Force and initial research on the mathematical aspects of the machine was carried out by them. Later on, however, OKW/Chi did give some help in mathematical research on the device.[431]

The Navy was the most aloof of the services. It had worked on the Interdepartmental Cypher and sent representatives to the Chi-conferences, but otherwise, it had little connection with OKW/Chi. The chief cryptanalyst of the Navy, Tranow, stated that OKW/Chi was kept informed of the cryptanalytic work carried out by the Navy cryptanalytic agency.[432] This was required, it will be recalled, by the Praun order of 5 September 1944. Tranow is emphatic, however, in his statement that no naval research problems were referred to OKW/Chi.[433] The Navy received some raw traffic intercepted by OKW, which had been passed over commercial circuits. They had adopted at least one of the cryptanalytic devices developed by OKW/Chi, the so-called Roller apparatus.[434] One of the Navy ratings had devised some improvements for the apparatus and was ordered to cooperate with OKW/Chi in developing these.[435] Otherwise, contact seems to have consisted of informal conversation between Tranow and Huettenhain. It was in one of these conversations that Tranow learned from Huettenhain that the exiled Polish Government in London used a stencil system somewhat similar to the British Naval System.[436]

[431] I-57, 8.

[432] I-93, 4.

[433] I-93, 4.

[434] I-37, 3.

[435] D-45, 5. From a report of 4/SKL, dated 6/3/44. "FK. Gfr. Zimmermann, of Section III Fq, submitted within the last few weeks a proposal for a printing synthetic producing machine [Rollmaschine]. Zimmermann was instructed by OKW/Chi, where new developments are worked out for the branches of the armed forces, to have a prototype ready within 3 weeks in order to fix the final model."

[436] I-93, 25.

11. OKW/Chi and other German High-Level Signal Intelligence Agencies. When attacks on enemy service systems were assigned to the separate branches and OKW/Chi assumed responsibility for enemy and neutral diplomatic systems, OKW/Chi definitely became the competitor of two other German high-level signal intelligence agencies, Goering's Research Bureau (hereafter indicated by FA, the abbreviation for Forschungsamt), and the Foreign Office Cryptanalytic Section (Pers ZS).

Since 1933, Goering's Research Bureau (the FA) had apparently given some attention to diplomatic material as well as dabbled in a great many other things. Since World War I, the German Foreign Office had maintained a cryptanalytic bureau whose main commitment was attack on diplomatic traffic. One of the problems of OKW/Chi was, consequently, to establish its position in the face of these agencies which had been longer in the field.

Goering's Research Bureau (the FA) had started in a fashion likely to prejudice its relations with OKW/Chi. It will be recalled that the FA owed its existence to the fact that Schapper and other members of the Abwehr Cipher Section had gone to Goering and proposed a new intelligence organization. They said at the time that the older organization was inefficient and involved in departmental politics.[437] They apparently kept this opinion until the end of the war. Schapper's remarks on OKW/Chi have already been noted. His colleague, Seifert, had an equally low opinion of OKW/Chi and told the interrogators that Goering's Research Bureau (the FA) had been established "to provide diplomatic and commercial intelligence of an absolutely reliable kind... and to insure..the elimination of all bias which might have resulted from association with the old established ministries.[438] Hermann Goering expressed particular scorn for OKW/Chi "the most junior member of the family".[439] The personnel of OKW/Chi, on the other hand, seem to have returned scorn for scorn. Mettig stated that Fenner, who seems to have been in charge of liaison with other cryptologic agencies,

[437] IF-15, p 20.

[438] I-54, 3.

[439] I-143, 15.

felt particularly strongly on the subject of Goering's Research Bureau (the FA), probably because it had been established by his former subordinate, Schapper.[440] Huettenhain also refers to Fenner's particularly violent "prejudice". He further said that some personnel of OKW/Chi had gone over to Goering's Research Bureau (the FA) and that they were regarded in OKW/Chi as people who had "deserted the ship". He knew Paetzel and had discussed cryptanalytic work with him. His personal impression was that Goering's people knew little in the field of cryptanalysis. "They employed no mathematicians".[441] Fricke denied that he had ever known any of the personnel of Goering's Research Bureau (the FA) until he was brought together with them as a prisoner at the end of the war. They had a bad name, he said, at OKW/Chi. His personal opinion was that they were a big name with nothing behind it. The interrogators told Fricke that Goering's Research Bureau (the FA) employed twenty-five hundred people. He replied, "For their deciphering they should have needed a handful. They must have had other work to do, but what the devil could they have been doing with twenty-five hundred people?".[442]

The chiefs of both services professed a willingness to cooperate, but each accused the other of failing to do so. Schapper told his interrogators that at the beginning of the war he wished his work to become a general intelligence bureau but that his competitors, the Foreign Office and OKW/Chi, refused.[443] He was quite willing, he said, to work with Col. Kettler, but this willingness was not reciprocated. Kettler, on the other hand, said, "the Forschungsamt monitored Press traffic. It carried out cryptographic work but I do not know what it was. We tried to work together but the Forschungsamt refused for reasons unknown to me.[444]

[440] I-131, 3.

[441] I-31, 10.

[442] I-20, p 8.

[443] IF-15, p 17.

[444] I-21, p 1.

In view of this mutual feeling, it is surprising to find that there actually was considerable cooperation with Goering's Research Bureau (the FA). The most conclusive evidence of this is that, according to Kettler's report, one-third of the raw traffic reaching OKW/Chi in the Spring of 1944 came from Goering's Research Bureau (the FA). It is probable that a similar proportion came during the other periods for which we have no record. Goerings Research Bureau (the FA) was probably not interested in cryptographic development but, despite this fact, it was represented at Gimmler's Chi-conferences. Their representative was Kroeger, a leading machine specialist, who had, according to Paetzel, broken the Finnish Hagelin.[445] In cryptanalysis, however, cooperation was non-existent.[446] On the other hand, the cryptanalytic machines developed by OKW/Chi were made available to all German cryptanalytic agencies except the FA.[447] Intelligence obtained by Goering's Research Bureau (the FA) from cryptanalytic and other activity was passed on to the OKW directly by the liaison officer.[448] OKW/Chi was by-passed.

The Foreign Office Cryptanalytic Section (Pers ZS) was senior to OKW/Chi. There is no doubt that OKW/Chi had intruded on its domain when it took over diplomatic traffic. This aspect of the relations between the two organizations is particularly stressed by Specialist Karstien, who of all the Foreign Office Cryptanalytic Section (Pers ZS) personnel seems to have felt most strongly against OKW/Chi.[449] The attitude of the other members of the Foreign Office Cryptanalytic Section (Pers ZS) was one of mild contempt. They definitely felt that they were an older organization, that they had a greater number of able people, and that they were in general more competent. This feeling of superiority was tinged with a certain bitterness because they felt that their efforts were unappreciated in higher quarters and that they were discriminated against in such matters as

[445] I-54, 2.

[446] I-54, 4.

[447] I-31, p 10.

[448] Klautschke, liaison officer to OKW, OKM, OKL, OKH was concerned solely with passing intelligence and intelligence requests. There was no liaison on cryptanalytic matters as far as he knew (I-54, 4).

[449] I-[illegible], 9.

procurement of additional personnel. Prof. Rohrbach, who was the principal spokesman for the captured Foreign Office Cryptanalytic Section (Pers ZS) people, was at great pains to point out that Rave, Hierer, Grosse, and Schroeder, who were OKW/Chi personnel working with the Foreign Office Cryptanalytic Section (Pers ZS) and captured with them, were people of an inferior type who had been sent to the Foreign Office Cryptanalytic Section (Pers ZS) for training. "He spoke of them", the interrogator remarked, "with obvious distaste."[450] Rohrbach was careful to point out that when Zastrow, the expert on U.S.A. systems, was detached from the Foreign Office Cryptanalytic Section (Pers ZS) to OKW/Chi his status was entirely different. He had gone to OKW/Chi not for training but to lend his expert assistance to the junior organization. It is noteworthy that this mild contempt was not reciprocated by OKW/Chi. As spokesman for the OKW/Chi party detached to the Foreign Office Cryptanalytic Section (pers ZS), Rave spoke in the most flattering terms of his hosts. OKW/Chi, he said, had neither the long experience nor the "expertise" which the Foreign Office Cryptanalytic Section (Pers ZS) possessed although Fenner and a small party had been engaged on this work in time of peace.[451] Huettenhain had seen the papers which Schauffler of the Foreign Office Cryptanalytic Section (Pers ZS) had written on the mathematical aspects of cryptanalysis.[452] Although he did not speak of them with a high regard, he at least does not hold them in contempt. At one time Huettenhain seems to have considered contributing papers on cryptologic subjects to the Foreign Office Cryptanalytic Section (Pers ZS) publication. Nothing came of this, however, because Fenner discouraged it for reasons of security.

Kettler stated that he considered the relations of OKW/Chi with the Foreign Office Cryptanalytic Section (Pers ZS) good,[453] and there is considerable evidence that a high degree of cooperation was achieved and the delicate problems arising

[450] I-22, 7, 11.

[451] I-22, 8.

[452] I-31, 11.

[453] I-21, p 2.

DOCID: 3560827

from the fact that both organizations were committed to the same material were partly met. In the case of the American strip system, for example, the Foreign Office Cryptanalytic Section (Pers ZS) worked on circular traffic, OKW/Chi on point to point traffic.[454] When both organizations were breaking the older Japanese cipher machine, OKW/Chi worked on odd days, the Foreign Office Cryptanalytic Section (Pers ZS) on even.[455] Results were exchanged. There was also a division of labor among the language sections on some book-breaking problems and there were occasionally some exchanges of personnel. Huettenhain and his mathematicians had worked with the Foreign Office Cryptanalytic Section (Pers ZS) research party. He felt that a satisfactory division of labor had been achieved.[456] Fenner directed liaison for OKW/Chi and Senior Specialist Paschke for the Foreign Office.[457] The head of the Foreign Office Cryptanalytic Section (Pers ZS), Minister Selchow, is said to have been opposed to too intimate a relationship.[458] It is known that he refused to permit the cryptographic system developed by his department for Foreign Office use to be turned over to OKW/Chi for security scrutiny. The actual debt of OKW/Chi to the Foreign Office Cryptanalytic Section (Pers ZS) cryptanalysts is hard to assess, particularly in view of the fact that the leading members of the OKW/Chi language sections, Fenner, Wendland, and Nowopaschenny, were not captured and interrogated. On the basis of the material available, however, it seems that that debt is considerable. The Foreign Office Cryptanalytic Section (Pers Z S) gives the impression of being old, conservative, slow-moving but able. It was a cipher party of the old type such as Fenner's had been previous to the outbreak of the war. It had never been subject to the dynamic and somewhat feverish expansion that had been the lot of OKW/Chi, where emphasis had been changed from intelligence to security, and

[454] I-31, 10.

[455] I-31, p 11.

[456] I-31, 10.

[457] I-22, 8.

[458] I-22, 8.

where a great many of the leading cryptanalytic personnel had been taken into purely cryptographic research. In the Foreign Office Cryptanalytic Section (Pers Z S), the mathematicians existed solely to assist the crypto-linguists. The linguists themselves were apparently more carefully selected, older, and better trained than those of OKW/Chi. It is very likely that in the exchange of results, OKW/Chi received more than it gave. It is known that the initial break into the older Japanese machine was made by the Foreign Office Cryptanalytic Section (Pers ZS).[459] It is possible that they also were the first to break the American strip system, as Rohrbach so emphatically claims.[460] Two South African codes were worked on jointly by OKW/Chi and the Foreign Office Cryptanalytic Section (Pers Z S), with the latter taking the lead. On the other side of the ledger is the loan by OKW/Chi to the Foreign Office Cryptanalytic Section (Pers Z S) of a Brazilian, a Mexican, and a Portuguese compromised code for photographing. Prior to the compromise of the Portuguese code, the two agencies had regularly exchanged group meanings.[461] Where quality and expertness were primary considerations as in initial attacks on cipher systems, and in more difficult book breaking problems, the Foreign Office Cryptanalytic Section (Pers Z S) was superior to its military colleague. When a problem had reached the mass production stage, however, OKW/Chi was able to profit by the comparative ease with which it could obtain partly trained, medium-grade personnel.[462]

12. Liaison with Foreign Signal Intelligence Agencies. In the matter of liaison with the signal intelligence agencies of Germany's allies, the authority of OKW/Chi seems to have been partly recognized. Fenner had been working for a number of years previous to the outbreak of the war to establish

[459] I-22, p 2, 7, 16.

[460] I-89.

[461] D 16 Report 2 P 3; Report 4 P 3, 5.

[462] Cf. Also the statement (I-22, 13) "If when a new system was broken, it was discovered that traffic dealt mainly with matters outside the diplomatic field, it was handed over to OKW for exploitation."

DOCID: 3560827

firm relationship between OKW/Chi and Germany's probable future allies. There is some evidence that the signal intelligence agencies of the Army, Navy, and Air Force were expected to approach their allied counterparts through OKW/Chi. Thus Friedrich, head of the Air Force signal intelligence, told interrogators that he had no liaison with the Japanese authorities and that such liaison took place only through OKW/Chi.[463] Voegele, the chief cryptanalyst of the Air Force, stated that he visited Berlin once in January and again in February 1942 for cryptographic discussions with Hayashi, the Japanese representative, but that the meeting never actually took place. Voegele believed that the discussions were prevented by Kempf, who was the head of OKW/Chi at the time.[464] To be sure, the Army had independent relations with the more reliable axis allies, the Italians and particularly the Finns. It is clear from the case of Bigi, however, that insofar as these relations were conducted on a high level, OKW/Chi had a hand in them. Bigi, it will be recalled, was never clear as to whether his relations were with OKW/Chi or the Army.[465] It is noteworthy, too, that the members of OKW/Chi were well acquainted with the Finnish liaison officers stationed with the army cryptanalytic agency.

a. Austria:

Before the annexation, Austria is said to have had a small but efficient cryptologic office. This was located in Vienna and headed by a Mr. Seifert. It had a small staff which dealt with the traffic of Italy, Rumania, Greece, Jugoslavia, Bulgaria, Turkey, Poland, and Czechoslovakia.[466] It is said that these organizations had close contact with OKW/-Chi even during the period of tension preceding the Anschluss. Huettenhain, from whom this information is derived, does not know precisely what this contact amounted to. At the time of the Anschluss, Gen. Fellgiebel and Fenner paid a visit to the

[463] I-29, 3.

[464] I-119, 6.

[465] See above, page ___.

[466] I-118, 3.

DOCID: 3560827

Austrian cipher office and brought the best personnel to Berlin where they were incorporated into OKW/Chi. Seifert became a high ranking civil servant (principal specialist, Ministerialrat) and specialist in book-breaking.[467]

b. Japan:

With representatives of the Japanese signal intelligence, a more or less astute sparring went on from the time of Japan's entry into the war. In 1942, one of the leading Japanese cryptanalysts, Colonel (later General) Hayashi, happened to be in Berlin. Unable to return home, he became Japanese Military Attaché in Budapest. During his stay in Berlin, he arranged for an exchange of material with OKW/Chi and a relationship was started between the head of OKW/Chi and the Japanese representative in Berlin which lasted throughout the war.[468] From cream sources, we know that Kempf was a favorite of the Japanese and that a proposal was made that he be decorated by Japan. What became of this proposal is unknown. Kettler maintained the relationships established during Kempf's regime. He admitted that he knew Japanese officers in Berlin well. Rave says that he remembered a Japanese naval attaché paying a visit to Col. Kettler.[469] There was, however, no regular Japanese liaison officer at OKW/Chi, and no Japanese worked there. Just what the Japanese got out of the relationship is difficult to say. Kettler stated that various book recoveries were passed on to them. Some of these were probably American,[470] although Huettenhain said that he was convinced that no United States strip material had ever been passed to the Japanese by OKW.[471] Some unworked traffic was exchanged, but there was never any exchange, so far as is known, of information on cryptologic procedures. In short, the Germans

[467] Cf I-118, 3. I-84, 4 in which it is stated that "Sieffert" head of the bureau, came to work at OKW/Chi with other members of the Austrian bureau: Dr. Mauler, Dr. Locker ORR Bailovic. This is not the man of the same name who headed the evaluation section of Goering's Research Bureau.

[468] I-21, p 2-3. I-31, 9.

[469] I-22, 8.

[470] I-21, p 3.

[471] I-31, 10. Cf. also Buggisch's statement (I-64, 3) that he had never heard of any Japanese cryptanalytic relations with OKW/Chi.

gave the Japanese very little cryptanalytic assistance and got nothing in return. In the cryptographic field, the Germans were apparently even more reticent. "We did not tell the Japanese," says Kettler, "that we considered their systems bad".[472] Huettenhain, however, knew of a proposal to sell to the Japanese some Enigmas, probably for naval use in the far east. He says that when the cryptanalysts of OKW/Chi found that the non-plugboard Enigma was readable, it was suggested to Fellgiebel that the Japanese should have plugboard machines. Fellgiebel vacillated. Huettenhain does not know what was finally done about the matter.[473]

There was to have been a last minute attempt to improve cryptologic relations with Japan. A plan existed to send a cryptographic delegation by submarine from Germany to Japan in the winter of 1944-45.[474] This delegation was to include Capt. Opitz and First Lt. Schubert, Army signal intelligence personnel, and Lt. Morgenroth, one of the Navy cryptanalysts. So little was known about Japanese cryptanalytic activity that the delegation did not know where they were to go in Japan or to whom they should announce their arrival. The first contact was to be with the German Military Intelligence (Abwehr) in the far east. The Military Intelligence (Abwehr) presumably would have further contacts.[475] According to Mrs. von Nida, only one of the delegates was able to speak Japanese[476] and it is perhaps true, as Mettig said, that the delegation did not plan to reveal or hope to get much. Mettig added that, in general, German liaison with the Japanese was not considered good, and that the German officers who visited Japan had to wear civilian clothes so that they would not embarrass their Axis partners.

[472] I-21, p 3.

[473] I-84, 7.

[474] I-105, 5.

[475] From Mettig I-127, 2, I-48, 3.

[476] I-49, p 2.

[477] I-127, 2.

c. Italy:

Despite the fact that cryptologic liaison with Italy had gone on for some time, and is said to have been started by General Gamba at the time of the Abyssinian war, it does not seem to have been much closer than liaison with the Japanese.[478] Bigi's visit to OKW/Chi in 1942 has already been mentioned.[479] An Italian proposal for a similar visit in December of that year was refused by the Germans.[480] A deal, however, was made and carried out whereby certain Italian IBM equipment was exchanged for German IBM equipment in order to enable the Italians to use IBM machinery in their cryptanalytic work. Huettenhain mentions exchanges of book groups. He also tells a story of how the Germans broke an Italian cipher and told the Italians, who refused to believe it. "To prove it to them we finally sent a cryptographer to Rome and he was locked in a room until he had done so!"[481] After the surrender of the Italian government, the Italian Fascist Republic set up a new signal intelligence service. With this service Kettler refused to have any dealings whatever, "since we did not know what they would do with it".[482] Kettler was instrumental in obtaining a German order that the Fascist Republic cryptologic bureau be dissolved. This occurred on 25 February 1944.

d. Hungary:

Liaison with the Hungarian cryptanalysts had existed since the early twenties, and there was a regular exchange of material throughout the war.[483] In the report of June 1944, Kettler stated that, during the Spring of '44, he received one-eighth of his raw traffic from the Hungarians. The exchange took place through the Hungarian embassy. There was no

[478] I-21, p 3, from Huettenhain.

[479] I-1517 Appendix A. See above p 73. Cf. also I-78, 11.

[480] I-21, p 3.

[481] I-21, p 3.

[482] I-21, p 3.

[483] I-21, p 2.

DOCID: 3560827

regular exchange of liaison officers although Wendland, Fenner's under-study, was sent to Hungary.[484] A few weeks before the entrance of Hungary into the war, Hungarian General Petrikovic visited OKW/Chi when he passed through Berlin, probably on his way to Helsinki. This was during Kempf's term of office.[485] Kettler, moreover, made two good-will visits to Hungary. In return for the traffic which they received, the Germans gave the Hungarians methods of solution for Italian, Rumanian, and Polish systems, the only countries whose systems were of interest to the Hungarians.[486] Huettenhain tells an odd story which indicates that relations were not always quite so happy as the above details suggest. In the summer of 1944, OKW/Chi broke a Turkish code and gave it to the Hungarians. The Hungarians sold the code to Himmler's Security Service, the RSHA, which brought it proudly back to OKW/Chi.[487] At the beginning of 1945, liaison with the Hungarians was terminated. Kettler sent a liaison officer to the German border at Steinamanger but he returned after having exchanged courtesies with the Hungarians. Nothing further is heard.[488]

e. Finland:

Liaison with the Finnish cryptanalysts began around the year 1938 and was intensified just after the first Russo-Finnish war.[489] In 1942, a Lieutenant Mikkoja arrived to act as liaison officer at army headquarters. He may also have had some contact with OKW/Chi. In any case, OKW/Chi had liaison with a Colonel Hallimaa from the beginning of the second Russo-Finnish war.[490] Traffic was exchanged in both the military and diplomatic fields. The Finns were said to have been interested

[484] p 2 Ibid.

[485] p 2 Ibid.

[486] p 2 Ibid.

[487] I-132, 2.

[488] I-21, p 1.

[489] I-96, p 5; I-29, p 3.

[490] I-111, 4.

DOCID: 3560827

principally in the traffic of Russia, Poland, Rumania, and Sweden.[491] There was close liaison with the Finns on the solution of an American strip system, but no exchange was made on any other system since OKW/Chi had nothing to offer. It is probable that the Finns were given to driving sharp bargains with their allies. We know that the German solution of the American strip system depended partly on the traffic for March 1943, and that it was not broken by them before that date.[492] We know, too, that on the tenth of March 1943, the Finns gave their solution of the American cipher system to the Japanese. It seems that the Finns had broken the American cipher system previous to March 1943, and withheld this information from their German allies. They started to exchange only when the Germans had something to offer. What the Finns got from the Japanese in return for the information on the American strip, we do not know from TICOM.

In his report for Spring 1944, Kettler states that German relations with the Hungarian and Finnish cryptanalytic organizations were of great assistance to the Germans in restoring the Archives of OKW/Chi which had been destroyed by the air raid of November 1943.

f. Bulgaria:

The only evidence of any connection of OKW/Chi with Bulgarian signal intelligence is the statement in the Kettler report for Spring 1944: that several Bulgarians were given a course in elementary cryptography at OKW/Chi.[494]

g. Spain:

The extent of OKW/Chi's relations with the Spanish Signal Intelligence has been covered in the discussion of the intercept systems of OKW/Chi in Spain. There is no doubt that the head of the Spanish signal intelligence service, Colonel Sarmiento, cooperated with the Germans. He received French traffic and military traffic in general sent to North Africa. In return, he gave the cablegrams about ship movements probably originating

[491] I-31, 9.

[492] I-89.

[494] DF-9, 3.

DOCID: 3560827

with commercial attachés.[495] About cryptanalytic materials, he told the Germans nothing. Mettig believes that this was because he knew nothing.[496]

[495] I-111, 4. It is not clear whether these cablegrams were given, however, to OKW or to OKH.

[496] I-111, 4.

DOCID: 3560827

TAB A

VOLUME 3

Tab A

A-13. "Consolidated List of Documents received from: I. A.F.H.Q., Italy; II. Feuerstein; III. Japanese Embassy, Berlin; IV. Lisbon; V. M.I.8; VI. N.S.VI; VII.OSS, Wiesbaden." A TICOM publication.

Abwehr.-- Military Intelligence.

Adler, Walter, First Lt. Dr. Member of Subsection of OKW/Chi working on China, Japan.

Agents' Section.-- "Referat Vauck," named for its head, Lt. Vauck.

Ag/WNV (Amtsgruppe Wehrmachtnachrichtenverbindung).-- Armed Forces Communications Group.

Aigner,_____, Dr. (of Medicine). Member of Section IVc of OKW/Chi (initial breaking of more difficult systems; cryptanalytic theory).

Amberg, Hans Contact man for OKW/Chi in Spain.

Amtsgruppe Wehrmachtnachrichtenverbindung (Ag/WNV).-- Armed Forces Communications Group.

Andrae,_____, Lt. Col. Chief of Group I of OKW/Chi (intercept) until replaced by von NIDA. Chief of Staff of the Signal Intelligence Agency of the Army High Command (OKH/G d NA).

Armed Forces Communications Group.-- Amtsgruppe Wehrmachtnachrichtenverbindung (Ag/WNV).

Armed Forces High Command.-- Oberkommando der Wehrmacht (OKW).

Armed Forces Signal Communications.-- Wehrmachtnachrichtenverbindung (WNV).

Armed Forces Signal Officer for Special Employment # 700.-- Wehrmachtnachrichtenfuehrer zu besonderer Verwendung 700 (Wehrmachtnachrichtenfuehrer z. b. V. 700).

Armed Schutzstaffel (Waffen-SS).-- Components of Elite Guard serving at front.

Army Ordnance, Development and Testing Group, Signal Branch.-- Waffenpruefung 7 (Wa Pruef 7).

Army Ordnance Office.-- Heereswaffenamt (HWA).

Aumann,_____, Prof. Dr. Member of Section IVc of OKW/Chi (initial breaking of more difficult systems; cryptanalytic theory).

DOCID: 3560827

Baechle, Friedhelm. Radio operator with Military Intelligence (Abwehr), Department I-i in Madrid, Spain, Jul 1940 - Nov 1944. This department was responsible for radio operation, telegraphy, teletype, and cryptography of Military Intelligence (Abwehr).

Ballovic, _____, Senior Specialist. Former member of Austrian cryptanalytic bureau, transferred at the time of Germany's annexation of Austria to Goering's Research Bureau (FA). After a short time, went to the Signal Intelligence Agency of the Army High Command (OKH/G d NA) and in Oct 1944 joined Balkan Section of Group V of OKW/Chi.

Barlow, _____, Maj. U.S. Army officer who tried to trace personnel and plant of the firm of Telefonbau und Normalzeit of Frankfurt/Main, which was responsible for the development of SG 39.

Berndt, _____ Mr. Chief of Polish part of Subsection V 6 of OKW/Chi.

Bernsdorff, _____ Capt. Chief of Section IIa of OKW/Chi (liaison between OKW/Chi and field units); in 1945 replaced Metzger as chief of Group III.

Beyreuther, Heinz W., Cpl. Member of Subsection of OKW/Chi working on China, Japan.

Boetzel, _____, Col. Chief of Code and Cipher Section of German War Ministry, 1934 - 1939. Chief of the Signal Intelligence Agency of the Army High Command (OKH/G d NA).

Bruckmann, _____. Mentioned (I-1, p. 20) as being "active on more or less independent footing" in OKW/Chi. Specialty: Greek.

Buck, _____, Senior Inspector. Chief of Section Ic of OKW/Chi (telecommunications).

Buggisch, Otto, S/Sgt. Dr. Cryptanalyst in Inspectorate 7/VI (In 7/VI). Expert on Russian ciphony.

Buschenhagen, _____, First Lt. Chief of the Defense Ministry Cipher Section, predecessor to OKW/Chi (1919).

Chi (Chiffrierabteilung).-- Cipher section.

Chiffrierabteilung (Chi).-- Cipher section.

Chiffrierstelle des Oberbefehlshabers der Luftwaffe (Chi-Stelle Ob d L).-- Signal Intelligence Agency of the Commander in Chief of the Air Force.

Chi-Stelle Ob d L (Chiffrierstelle des Oberbefehlshabers der Luftwaffe).-- Signal Intelligence Agency of the Commander in Chief of the Air Force.

Clifton, _____, Col. USA officer in command of units which captured some of the OKW/Chi personnel.

DOCID: 3560827

Cryptanalytic Section of the German Foreign Office.-- Sonderdienst des Referats Z in der Personalabteilung des Auswaertigen Amtes (Pers Z S).

D-16. "Translation of Annual Progress Reports by Pers Z S covering 1927, 1941, and 1942." A TICOM Publication.

D-55. "Translation of Order concerning Cryptanalytic and Cypher Production Work promulgated by OKW/WFSt/Chef WNV, taken from Papers of Major Nielson." A TICOM publication.

D-57. "Notes and Minutes of High-Level Meetings held at OKW/Chi." A TICOM publication.

Defense Ministry.-- Reichswehrministerium.

Dettmann, Alex, Lt. Head of cryptanalysis at Intercept Control Station East (HLS Ost); later head of Section 3, Group IV of the Signal Intelligence Agency of the Army High Command (OKH/G d NA). Specialty: machine cipher and research.

DF-8. Captured Wehrmacht Sigint Document: Statement of Order of Battle of OKW/Chi based on document dated April 1945. A TICOM publication.

DF-9. Captured Wehrmacht Sigint Document: Translation of Activity Report of OKW/Chi for the period 1st January, 1944 to 25th June, 1944. A TICOM publication.

Doenitz, Karl, Grand Admiral. Commander in Chief, German Navy; Reich Chancellor after Hitler's death.

Doering, _____, S/Sgt. Dr. Mathematician of Inspectorate 7/VI (In 7/VI); later with the Signal Intelligence Agency of the Army High Command (OKH/G d NA). Specialty: machine cipher and research.

Eckert, _____, First Lt. Liaison Officer from OKW/Chi to the Signal Intelligence Agency of the Commander in Chief of the Air Force (Chi-Stelle Ob d L).

Eichner, _____, Second Lt. Officer in charge of OKW/Chi's "Section Spain" office in Sevilla, Spain.

Elite Guard of the Nazi Party.-- Schutzstaffel (SS).

Felgiebel, Erich, Lt. Gen. Chief Signal Officer of Army and Armed Forces High Commands from beginning of war until he was executed in 1944.

Fenner, Wilhelm, Principal Specialist. Chief of Division B of OKW/Chi (Cryptanalysis).

Flicke, _____, Specialist. In charge of technical matters at OKW Intercept station at Lauf.

Foreign Security Service.-- Sicherheitsdienst Ausland (SD Ausland).

DOCID: 3560827

Franke, _____, Senior Specialist. In charge of work on Swedish BC 38 in OKW/Chi, 1940.

Franz, _____, Prof. Dr. Chief of Section IVc of OKW/Chi (initial breaking of more difficult systems; cryptanalytic theory).

Fricke, _____, SS First Lt. Liaison Officer from the Reich Main Security Office (RSHA) to OKW.

Fricke, Walther, Technician (Lt. Grade) Dr. Chief of Section IIb of OKW/Chi (development of German systems).

Friedemann, _____. One of chief members of Joint Intelligence (Abwehr) in Spain.

Friedrich, _____, Lt. Col. Chief of Division III of Chief Signal Office (Gen NaFue III) and of the Signal Intelligence Agency of the Commander in Chief of the Air Force (Chi-Stelle Ob d L).

Frowein, _____, Lt. (Navy). Member of the Signal Intelligence Agency of the Navy High Command (OKM/4 SKL/III).

Fu (Funkueberwachung).-- Radio Defense Corps.

Funkueberwachung (Fu).-- Radio Defense Corps.

Gamba, Vittorio, Gen. Head of Italian Cryptanalytic Department.

Gimmler, _____, Maj. Gen. Chief of Army Ordnance Development and Testing Group, Signal Branch (Wa Pruef 7), 1939 - 1943. Chief Signal Officer to Commander in Chief West, 1943 - 1945. Chief of Armed Forces Communications Group (Chef Ag WNV).

Goering, Herrmann, Reichsmarschall. Commander in Chief of German Air Force, German Air Minister, etc.

Grosse, Arthur, Mr. OKW/Chi employee detached to Foreign Office Cryptanalytic Section (Pers Z S) for training. Specialized in Chinese and Japanese.

Grotz, _____ Capt. Chief of Group I of OKW/Chi (control of intercept stations).

Hagen, Ursula, Miss. Head of the group in the Foreign Office Cryptanalytic Section (Pers Z S) which worked on English and British Empire, Spanish, Portuguese, and Latin-American Systems.

Hallimaa, _____, Col. Head of Finnish Cipher Section. Had liaison with OKW/Chi.

Hatz, Heinrich, Staff Director, in charge of administration of OKW intereept station at Lauf.

Hayashi, _____, Col. (later Gen.). Head of Japanese military cryptographic organization, caught in Germany at outbreak of war; became Japanese Military Attaché at Budapest. Had some liaison with OKW/Chi.

DOCID: 3560827

Heereswaffenamt (HWA).-- Army Ordnance Office.
Heimsoeth & Rincke. Firm which made the changeable turnover rotor (Lueckenfuellerwalze) for the Enigma cipher machine. Address of the firm: Uhlandstrasse 138, Berlin-Wilmersdorf.
Hein, _____, Maj. Commander of Transport in move of part of OKW/Chi to South Germany, 1945.
Hentze, Rudolf, Maj. Dr. Head of Group IV, Signal Intelligence Agency of the Army High Command (OKH/GdNA).
Herold, Wadim, Capt. German Air Force Officer detached to OKW/Chi in Jan 1940 to be intercept officer in the field.
Hierer, _____, Mr. OKW/Chi employee detached to Foreign Office Cryptanalytic Section (Pers Z S) for training.
Himmler, Heinrich. Reichsfuehrer SS, Minister of Interior, Chief of German Police.
Hoepfner, _____, Col. Took command of OKW/Chi after it moved to Halle, 1945.
Huettenhain, Erich, Specialist Dr. Chief cryptanalyst of OKW/Chi from 1937 to end of war. Chief of Group IV (cryptanalytic research); also chief of Section IVd (training).
HWA (Heereswaffenamt).-- Army Ordnance Office.
I-1. "Report of TICOM reporting team number three, which uncovered the Foreign Office Cryptanalytic Section (Pers Z S)." A TICOM publication.
I-2. "Interrogation of Dr. Huettenhain and Dr. Fricke at Flensburg, 21 May 1945." A TICOM publication.
I-13. "Composite Report on Two Interrogations of Oberstlt. Friedrich, Chief of the G.A.F. Sigint Service, 18/5/45 and 9/6/45." A TICOM publication.
I-17. "Extracts of SHAEF Interrogations of Maj. Gen. Boner, Colonel Grube, Lt. Col. Mettig, and Major Rottler." A TICOM publication.
I-20. "Interrogation of Sonderfuehrer Dr. Fricke of OKW/Chi (Formerly of OKH/Chi)." A TICOM publication.
I-21. "Preliminary Interrogation of Oberst Kettler, R.R.Dr. Huettenhain, Sdf. Dr. Fricke and Oblt. Schubert (OKH/Chi), 15 June 1945." A TICOM publication.
I-22. "Interrogation of German Cryptographers of Pers Z S Department of the Auswaertiges Amt." A TICOM publication.
I-27. "Preliminary Interrogation of Fraeulein Hagen, Head of English Section of Pers. Z S, Auswaertiges Amt." A TICOM publication.
I-29. "Third Interrogation of Oberstltn. Friedrich, Chief of the G.A.F. Signals Intelligence Service." A TICOM publication.

DOCID: 3560827

I-31. "Detailed Interrogations of Dr. Huettenhain, formerly head of research section of OKW/Chi, 18th-21st June 1945." A TICOM publication.
I-36. "Translation of Paper Written by Reg.Rat.Dr. Huettenhain and Sonderfuehrer Dr. Fricke on the Development of OKW/Chi, Sections A.III and B.V." A TICOM publication.
I-37. "Translation of Paper Written by Reg.Rat.Dr. Huettenhain of OKW/Chi on Special Apparatus used as aids to cryptanalysis." A TICOM publication.
I-38. "Report on Interrogation of Lt. Frowein of OKM/4 SKL/III, on his work on the Security of the German Naval Four-Wheel Enigma." A TICOM publication.
I-39. "Organization of OKW/Chi." A TICOM publication.
I-44. "Memorandum on Speech Encipherment Apparatus by O.R.R. Huettenhain and Sdf. Dr. Fricke." A TICOM publication.
I-45. "OKW/Chi Cryptanalytic Research on Enigma, Hagelin and Cipher Teleprinter Machines." A TICOM publication.
I-46. "Preliminary Report on Interrogation of Dr. Otto Buggisch (of OKH/Gen.d.NA) and Dr. Werner Liebknecht (employed by OKH and OKW as tester of cryptographic equipment) 23 June 1945." A TICOM publication.
I-47. "P/W Situation Report." A TICOM publication.
I-48. "Report on Special Interrogation of Drs. Huettenhain and Fricke, Oberst Mettig, and Lt. Morgenroth carried out on 29th July 1945." A TICOM publication.
I-49. "Notes on OKW/Chi and on Intercept Organization under K.O. Spain." A TICOM publication.
I-53. " Construction of "Schluesselgeraet 39." A TICOM publication.
I-54. "Second Interrogation of Five Members of the RLM/Forschungamt." A TICOM publication.
I-57. "Enciphering Devices worked on by Dr. Liebknecht at Wa Pruef 7." A TICOM publication.
I-58. "Interrogation of Dr. Otto Buggisch of OKW/Chi." A TICOM publication.
I-61. "Interrogation Report on Friedhelm Baechle, W/T Operator with KO Spain." A TICOM publication.
I-62. "Field Interrogation of Paul Ratz of the German Army Signals Intelligence (1933-1945)." A TICOM publication.
I-64. "Answers by Wm. Buggisch of OKH/Chi to Questions sent by TICOM." A TICOM publication.
I-65. "Interrogation Report on Four Members of the G.A.F. Sigint Service." A TICOM publication.

DOCID: 3560827

I-66. "Paper by Dr. Otto Buggisch of OKH/In 7/VI and OKW/Chi on TYPEX." A TICOM publication.
I-67. "Paper by Dr. Otto Buggisch of OKH/In 7/VI and OKW/Chi on Cryptanalytic Machines." A TICOM publication.
I-68. "Consolidated Report Based on Two Interrogations of Oberst Randewig, of Hoeh. Wehrmachts Nafue z.b.V. 700, carried out at CSDIC on approx. 1 Aug. and 10 Aug. 1945."
I-69. "Summary of Cipher Information on Jugoslav Traffic Provided by Uffz. Herzfeld (Appendices to TICOM I-52)." A TICOM publication.
I-72. "First part of the Report by Wm. Buggisch on S.G. 41." A TICOM publication.
I-73. "Translated Version of Homework done by Wm. Buggisch." A TICOM publication.
I-75. "Interrogation Reports on German Field Sigint Personnel carried out at BUFFER - Ltn. August Schroeder, Ltn. Starke, Obgefr. Heudorf, and Hptm. Holetzke." A TICOM publication.
I-76. "Interrogation Reports on Lehwald, Haupts, Klett and Lauerbach. Also I/76 Supplement (Diagrams).." A TICOM publication.
I-77. "Translations of Joint Report made by Drs. Huettenhain and Fricke on the "Zaehlwerk" Enigma Machine." A TICOM publication.
I-78. "Interrogation of Oberstlt. Mettig on the History and Achievements of OKH/AHA/In 7/VI." A TICOM publication.
I-79. "Supplementary Paper by Drs. Huettenhain and Fricke on the Solution of the Hagelin Machine." A TICOM publication.
I-84. "Further Interrogation of R.R. Dr. Huettenhain and Sdf. Dr. Fricke of OKW/Chi." A TICOM publication.
I-85. "P.W. Interrogation Report on Reg. Rat Flicke, Techn. Insp. Pokojewski, Stabsintendant Hatz of OKW/Chi." A TICOM publication.
I-86. "Interrogation of Oberstlt. Mettig of OKH and OKW/Chi on the higher direction of German cryptanalytic work." A TICOM publication.
I-88. "Report on Interrogation of Mr. K. Vetterlein of the Reichspost Laboratorium on German Interception of Transatlantic Speech Circuits." A TICOM publication.
I-89. "Report by Prof. Dr. H. Rohrbach of Pers Z S on American Strip Cipher." A TICOM publication.
I-90. "Interrogation of Herr Reinhard Wagner (OKW/Chi) on Japanese Systems." A TICOM publication.
I-91. "P.O.W. Interrogation Report - General Major Robert K.H. Schlake, Chief of Communications in the Main Office of the Ordungspolizei, Ministry of the Interior." A TICOM publication.

DOCID: 3560827

I-92. "Final Interrogation of Wachtmeister Otto Buggisch (OKH/In 7/VI and OKW/Chi)." A TICOM publication.
I-93. "Detailed Interrogation of Membersof OKM/4 SKL/III at Flensburg." A TICOM publication.
I-95. "Interrogation of Lt. Morgenroth on organization of OKM/4 SKL/III." A TICOM publication.
I-96. "Interrogation of Oberstlt. Mettig on the Organization and Activities of OKW/Chi." A TICOM publication.
I-98. "Interrogationof Oberst Randewig on German Deception Plans." A TICOM publication.
I-103. "Second Interrogation ofReg.Rat Hermann Scherschmidt of Pers Z S Auswaertiges Amt, on Turkish and Bulgarian Systems." A TICOM publication.
I-104. "Report on Berlin Targets by Major Heller of G.S.I.(s), 21 A.G., B.A.O.R." A TICOM publication.
I-105. "Interrogation Report on Frau von Nida (wife of Major Wolfgang von Nida, one-time Deputy Head of OKW/Chi)." A TICOM publication.
I-111. "Further Interrogation of Oberstlt. Mettig of OKW/Chi on 14th September 1945." A TICOM publication.
I-112. "Preliminary Interrogation of Reg.Rat. Dr. Ferdinand Voegele (Chi Stelle, Ob.d.L) and Major Ferdinand Feichtner (O.C. of LN Regt. 352, etc.)" A TICOM publication.
I-113. "Interrogation of Major Dr. Rudolf Hentze, Head of Gruppe IV (Cryptanalysis) General der Nachrichtenaufklaerung." A TICOM publication.
I-115. "Further Interrogation of Oberstlt. Mettig of OKW/Chi on the German Wireless Security Service (Funkueberwachung)." A TICOM publication.
I-116. "Report of Interrogation of Ltn. Alex Dettmann and Oberwachtmeister Sergius Samsonow of OKH (Gen.d.NA) at Oberursel, Germany, during August 1945." A TICOM publication.
I-118. "Joint Reports by Reg.Rat. Dr. Huettenhain and Sdf. Dr. Fricke, written at CSDIC on or about 28th August 1945." A TICOM publication.
I-119. "Further Interrogation of Reg.Rat Voegele and Major Feichtner on G.A.F. Sigint." A TICOM publication.
I-123. "Interrogation Report on Rudolf Trappe (Civilian) of OKW/Chi." A TICOM publication.
I-124. "Interrogation Report on Dr. Werner Weber of OKW/Chi." A TICOM publication.
I-127. "Interrogation of Oberstlt. Mettig of OKW/Chi." A TICOM publication.

I-128. "Deciphering Achievements of In 7/VI and OKW/Chi." A TICOM publication.
I-130. "Homework by Hauptmann Herold, O.C. Ln. Regt. III/353." A TICOM publication.
I-143. "Report on the Interrogation of Five Leading Germans at Nuremberg on 27th September 1945." A TICOM publication.
I-150. "Report by Uffz. Heinz W. Beyreuther on the Organization of OKW/Chi." A TICOM publication.
I-161. "Further Statements on Typex by Huettenhain, Fricke, and Mettig." A TICOM publication.
IF-15 "Final Report of TICOM Team 1 on the exploitation of Kaufbeuren and the Berchtesgaden area." From TICOM.
IF-130. Copy of MIS dossier on Fellgiebel. From Captured German Army Official Dossier, now in MIS files in Pentagon.
IF-164. "Report on Interrogation of Walter Schellenberg."
IF-165. Special report by Kirby, on TICOM Team 6's relation with OKW/Chi personnel. Original.
IF-166. Special report by Kirby on Sdf. Dr. Fricke. Nov 23, 1946. Original.
IF-167. "Final report on the visit of TICOM Team 5 to the Schliersee area." TICOM, but not registered.
IF-1517. "First detailed Interrogation of Augusto Bigi, who worked in the Cryptographic Section of SIM before the Armistice and in SID afterward." CSDIC/CMF/Y 4.
Inspectorate 7/VI of the Army High Command.-- Oberkommando des Heeres/Inspektion 7/VI (OKH/In 7/VI)
Jensen, _____, Graduate Engineer. Member of Section IVb of OKW/Chi (development of cryptanalytic machinery).
Jeschol, _____. Intercept operator in OKW Section Spain substation on Canary Islands.
Jodl, Alfred, Gen. Chief of Operations Staff, Armed Forces High Command (Chef OKW/Ia).
Jung-Fischer, _____, Mr. According to I-1, p. 20, chief of Swiss subsection of OKW/Chi.
Kaehler, _____, Lt. Col. Chief of Group VI of OKW/Chi (broadcast and press monitoring).
von Kalkstein, _____, Lt. Col. Chief of Group VII of OKW/Chi (intercept reports and their distribution; evaluation).
Karstien, Hans, Specialist Dr. Cryptanalyst with Foreign Office Cryptanalytic Section (Pers Z S). Specialist in Slavonic Languages. Headed the group which worked on Yugoslav, Bulgarian, Croatian, and Polish systems, as well as systems originating from the Baltic States. During the evacuation period (Dec 1943 - Mar 1945) headed that portion of the Section which was located in Hirschberg in the Riesengebirge. Also worked on Chinese problems 1930-1938.

DOCID: 3560827

Keitel, Wilhelm, Field Marshal. Chief of Armed Forces High Command (Chef OKW).

Kempf, _____, Col. Chief of OKW/Chi prior to 1943.

Kern, _____, Lt. Dr. Chief of Turkish Subsection of OKW/Chi.

Kettler, Hugo, Col. Chief of OKW/Chi, 1943 - 1945.

Kiefer, _____, Specialist Dr. Chief of subsection of OKW/Chi working on Spain, South America, Mexico.

Klautschke, Heinz, Specialist Dr. Liaison Officer with the Supreme Command of the Armed Forces (OKW not just OKW/Chi). Stated that he had "university training in economics and politics." Gives examples of information he supplied in the OKW and mentions offices he had dealings with. (I 25, IF 135, D 22, especially I 54).

Klett, Werner, Cpl. Member of Control Station Signal Intelligence West, located in Berlin.

Klinger, _____, Mr. Chief of Section Ia of OKW/Chi (liaison with intercept stations).

Koehler, _____, Technician (1.t. Grade). Head of linguistics at Inspectorate 7/VI (In 7/VI); later member of Signal Intelligence Agency of Army High Command (OKH/G d NA); finally (from Nov 1944) chief of Section Va of OKW/Chi (technical assistance for language work).

Korn, Willi, Graduate Engineer. Employee of firm of Heimsoeth & Rincke, who manufactured the Enigma. Collaborated with Fenner in developing the Enigma.

Krause, _____, Mr. Chief of Section VIc of OKW/Chi (foreign broadcasts).

Kriegsministerium.-- War Ministry.

Kroeger, _____, Specialist. The "cipher machine" specialist of Goering's Research Bureau (FA). Was said to have broken Finnish Hagelin. Was the representative of his organization in Huettenhain's Cipher Security Committee.

Kunze, _____, First Lt. Chief of Swiss Subsection of OKW/Chi.

Lenschau, _____, Maj. Dr. Chief of Subsection V 3 of OKW/Chi (Rumania). Worked with Mueller of French Subsection.

Liebknecht, Werner, Graduate Engineer Dr. Chief of Section IIIh of Army Ordnance Development and Testing Group, Signal Branch (Wa Pruef 7), research agency for developing voice scramblers.

Lober, _____, Maj. Chief of Group Z of OKW/Chi (personnel).

Locker, _____, Specialist Dr. Formerly member of Austrian cipher bureau; later chief of subsection on Turkish military systems of OKW/Chi.

Lotze, H., Graduate Engineer. Member of Army Ordnance Development and Testing Group, Signal Branch (Wa Pruef 7), Section e. Specialty: ciphony.

Lufthansa.-- German commercial airline.

Mang, _____, Maj. Chief of Inspectorate 7/VI (In 7/VI), 1941-1942.

Mauler, _____, Dr. Former member of the Austrian cryptanalytic bureau transferred at time of annexation to OKW/Chi, where he was deputy chief of Italian Subsection.

Menzer, _____, Senior Inspector. Chief of Section IIc of OKW/Chi (development and production of special ciphers for government departments, industry, and the Reich Main Security Office ((RSHA)), developing of deciphering aids for agents).

Mettig, _____, Lt. Col. Second in command of OKW/Chi, Dec 1943 - 1945. Chief of Division A (cryptography).

Mertz, _____, S/Sgt. Chief of Section IIIb of OKW/Chi (paper supply).

Metzger, _____, Maj. Chief of Group III of OKW/Chi (production and distribution of keys) until injured (early in 1945) and replaced by Bernsdorff.

Mihailovic, Draha. Yugoslav patriot leader.

Mikkoja, _____, Lt. Finnish liaison officer to OKW/Chi, 1942 - ?

Military Intelligence.-- Abwehr.

Morgenroth, _____, Lt. (Navy). A Navy cryptanalyst.

Mueller, _____, Senior Specialist. Chief of Subsection V5 (France, Switzerland) of OKW/Chi toward end of war.

von Nida, Wolfgang, Maj. Officer in charge of OKW intercept network in Spain, Jan 1940 to Apr 1942. From Apr 1942 to his death, Nov 1943, second in command of OKW/Chi.

von Nida, Mrs. Wife of Maj. Wolfgang von Nida.

Nielsen, _____, Maj. (Gen Staff) Operations Officer on staff of Chief Signal Officer of the Armed Forces.

Novopaschenny, _____, Professor. Chief of Russian subsection of OKW/Chi.

Oberkommando des Heeres/General der Nachrichten Aufklaerung (OKH/G d NA).-- Signal Intelligence Agency of the Army High Command.

DOCID: 3560827

Oberkommando des Heeres/Inspektion 7/VI (OKH/In 7/VI)-- Inspectorate 7/VI of the Army High Command.
Oberkommando der Marine/4 Seekriegsleitung II(OKM/4 SKL II).-- Signal Security Agency of the Navy High Command.
Oberkommando der Marine/4 Seekriegsleitung III (OKM/4 SKL III).-- Signal Intelligence Agency of the Navy High Command.
Oberkommando der Wehrmacht (OKW).-- The German Armed Forces High Command.
OKH/G d NA (Oberkommando des Heeres/General der Nachrichten Aufklaerung).-- Signal Intelligence Agency of the Army High Command.
OKH/In 7/VI (Oberkommando des Heeres/Inspektion 7/VI).-- Inspectorate 7/VI of the Army High Command.
OKM/4 SKL II (Oberkommando der Marine/4 Seekriegsleitung II).-- Signal Security Agency of the Navy High Command.
OKM/4 SKL III (Oberkommando der Marine/4 Seekriegsleitung III).-- Signal Intelligence Agency of the Navy High Command.
OKW (Oberkommando der Wehrmacht).-- The German Armed Forces High Command.
OKW/Chi (Oberkommando der Wehrmacht/Chiffrierabteilung).-- Signal Intelligence Agency of the Supreme Command, Armed Forces.
Operations Staff.-- Waffenfuehrungsstab, (WFSt).
Opitz, Carl Heinz, Capt. An Army Signal Intelligence Officer, member of a cryptographic delegation which was supposed to go from Germany to Japan by submarine in the winter of 1944-1945.
Ordnungspolizei (Orpo).-- Regular Police.
Orpo (Ordnungspolizei).-- Regular Police.
Oschmann, Maj. Chief of the Defense Ministry Cipher Section, predecessor to OKW/Chi (1932).
Oshima. Japanese Ambassador to Germany, 1943.
Paetzel, Martin, Senior Specialist Dr. Head of the research section, section 6, of Goering's Research Bureau (FA).
Paschke, Adolf, Senior Specialist Dr. Co-head of the Foreign Office Cryptanalytic Section (Pers Z S). Also headed the Linguistic-Cryptanalytic Subsection, his language specialties being Italian, Greek, and Russian. Was principally responsible for the Section's successes with Italian diplomatic codes 1935 to 1943.

Pers Z S (Sonderdienst des Referats Z in der Personalabteilung des Auswaertigen Amtes).-- Cryptanalytic Section of the German Foreign Office.

Peter or Peters, -----, Assistant Schoolmaster Dr. According to Beyreuther (I-150, p. 2), chief of Swiss Subsection of OKW/Chi.

Petrikovic, _____, Gen. Head of Hungarian cryptanalytic bureau.

Pietsch, _____, Specialist. Head of mathematical section of Inspectorate 7/VI (In 7/VI).

Plankert, _____, First Lt. In April 1943, succeeded Major von Nida as officer in charge of German intercept system in Spain, which was conducted by OKW.

Poetsgens, _____, Cpl. Dr. Chief of Greek subsection of OKW/Chi.

Pokojewski, Kurt, Technical Inspector. Subordinate to Flicke, civilian in charge of OKW intercept station at Lauf; later became civilian in charge.

Praun, Albert, Maj. Gen. Succeeded Fellgiebel as Chief Signal Officer of Armed Forces, 1944.

Pupp, _____, Dr. Member of Army Ordnance Development and Testing Group, Signal Branch (Wa Pruef 7), Section IV.

Raatz, Paul, Non-commissioned Officer. Member of various German Army Radio Intelligence Units.

Radio Defense Corps.-- Funkueberwachung (Fu).

Raffel, _____, Senior Specialist. Chief of Subsection V 6 (Italy) of OKW/Chi.

Randewig, _____, Col. Chief of Western intercept stations in 1939. In 1944, Armed Forces Signals Officer for Special Employment # 700 (Hoeherer W NaFue z. b. V. 700).

Rave, Kurt, Mr. OKW/Chi employee detached to the Foreign Office Cryptanalytic Section (Pers Z S) for training.

"Referat Vauck". Agents' Section, named for its head, Lt. Vauck.

Regular Police.-- Ordnungspolizei (Orpo).

Reichswehrministerium.-- Defense Ministry.

Rohen, _____, Senior Specialist. Chief of USA subsection of OKW/Chi.

Rohrbach, Hans, Prof. Dr. Member of Foreign Office Cryptanalytic Section (Pers Z S). Mathematician, and professor at the Charles University in Prague. Worked in Dr. Kunze's Mathematical-Cryptanalytic Subsection. Awarded the War Service Cross Grade 2 (KVK II) in September 1944, probably for his achievements in solution of the US Diplomatic Strip Cipher 0-2.

DOCID: 3560827

Rotscheidt, _____, Graduate Engineer. Chief of Section IVb of OKW/Chi (development of cryptanalytic machinery).

Rotter, _____, Senior Specialist. Chief of Czechoslovak Subsection of OKW/Chi; later chief of Bulgarian Subsection.

Ruesing, _____. Mentioned (I-1, p. 20) as being "active on more or less independent footing" in OKW/Chi. Specialty: Greek.

Rust, _____, Capt. Dr. Commanding Officer of OKW intercept station at Treuenbrietzen.

Ružek, _____. Captured Polish officer interrogated by Germans late in 1939 with regard to Polish work on German Enigma.

Salzbrunn, _____, Specialist Graduate Engineer. Chief of Section VIa of OKW/Chi (interception and recording equipment). In charge of Ludwigsfelde outstation.

Sarmiento, Rafael, Col. Chief Signal Officer of the Spanish Army.

Sato, _____. Counterintelligence man for Oshima, Japanese Ambassador to Germany.

Schaedel, _____, S/Sgt. Dr. Chief of Section VIIb of OKW/Chi (archives).

Schapper, Gottfried, Ministerial Director. A captain in Signals Intelligence in World War I. A member of the cipher section of the Defense Ministry, he resigned and joined Schimpf and others in forming Goering's Research Bureau (FA) for Goering in 1933. He was the third (and last) head of this organization and claims to have held a rank equivalent to that of a Generalleutnant in the Air Force.

Schauffler, Rudolf, Senior Specialist. Cryptanalyst, Co-head of the Foreign Office Cryptanalytic Section (Pers Z S) with Dr. Paschke. Head of the Research Subsection, head of the Japanese-Chinese cryptanalytic group, and adviser on cipher and code security to the Foreign Office Cryptographic Section.

Schellenberg, Walter, SS Brig. Gen. Head of Amt VI of the Reich Main Security Office (RSHA) which took over Joint Intelligence (the Abwehr) in Spring 1944. Schellenberg claimed to have arranged to take over Goering's Research Bureau and to have reached an understanding with Kettler to control OKW/Chi.

Scherschmidt, Hermann, Senior Specialist. Cryptanalyst, who headed at various times the work on Bulgarian, Turkish, and Polish systems in the Foreign Office Cryptanalytic Section (Pers Z S). Turkish was his language specialty, and this was the section which he headed in 1945.

DOCID: 3560827

Schlake, Robert K. H., Brig. Gen. Chief of radio and communications in the ministry of the Interior, 1933 - 1945.
Schmidt, _____, Maj. Chief of the Defense Ministry Cipher Section, predecessor to OKW/Chi (1927).
Schmidt, _____, First Lt. Chief of Section VIb of OKW/Chi (news agency transmissions, including pictures; international commercial radio traffic; multiplex).
Schnueckel, _____, T/Sgt. Chief of Section Ib of OKW/Chi (call sign and frequency study).
Schroeder, _____. OKW/Chi employee detached to the Foreign Office Cryptanalytic Section (Pers Z S) for training.
Schubert, _____, First Lt. Cryptanalyst with the Signal Intelligence Agency of the Army High Command (OKH/G d NA).
Schultze, _____, Dr. Member of Section IVc of OKW/Chi (initial breaking of more difficult systems; cryptanalytic theory).
Schutzstaffel (SS).-- Elite guard of the Nazi Party.
SD Ausland (Sicherheitsdienst Ausland).-- Foreign Security Service.
Seifert, _____, Principal Specialist. Formerly a member of the Austrian Cryptanalytic Bureau, joined OKW/Chi upon annexation of Austria, 1938.
Selchow, _____, Minister. Head of Z Branch (Referat Z), the Foreign Office Branch which handled cryptography, cryptanalysis, and Foreign Office Communications.
Seyfarth, _____, First Lt. Dr. Chief of Section VId of OKW/Chi (evaluation of Group VI's material; publication of reports).
SHAEF.-- Supreme Headquarters Allied Expeditionary Forces.
Sicherheitsdienst Ausland (SD Ausland).-- Foreign Security Service.
Signal Intelligence Agency of the Army High Command.-- Oberkommando des Heeres/General der Nachrichten Aufklaerung (OKH/G d NA).
Signal Intelligence Agency of the Commander in Chief of the Air Force.-- Chiffrierstelle des Oberbefehlshabers der Luftwaffe (Chi-Stelle Ob d L).
Signal Intelligence Agency of the Navy High Command.-- Oberkommando der Marine/4 Seekriegsleitung III (OKM/4 SKL/III).
Signal Security Agency of the Navy High Command.-- Oberkommando der Marine/4 Seekriegsleitung II, (OKM/4 SKL II).
Signal Intelligence Agency of the Supreme Command, Armed Forces.-- Oberkommando der Wehrmacht/Chiffrierabteilung (OKW/Chi).

DOCID: 3560827

Singer, _____, Capt. German naval officer who attended interrogations of captured Polish cryptanalytic personnel, 1942.

Sonderdienst Des Referats Z in Der Personalabteilung Des Auswaertigen Amtes (Pers Z S).-- Cryptanalytic Section of the German Foreign Office.

SS (Schutzstaffel).-- Elite guard of the Nazi Party.

Stein, _____, Lt. Dr. Chief of Section IVa of OKW/Chi (security investigation of new systems, new inventions). Machine specialist.

Steinberg, _____, Technician Dr. Member of mathematical section of Inspectorate 7/VI (In 7/VI), later in Section 1, Group IV of the Signal Intelligence Agency of the Army High Command (OKH/G d NA). Transferred in Nov 1944 to OKW/Chi. Worked on Japanese machine. Expert on solution of M-94 and M-209.

Supreme Headquarters Allied Expeditionary Forces. Abbreviated SHAEF.

T 782. Frankreich [German translations of decodes of French diplomatic traffic, dated Aug - Oct 1944.]

T 788. Chungking-China [German translations of decodes of Chinese diplomatic traffic, dated Aug - Oct 1944].

T 789. Chile [German translations of decodes of Chilean diplomatic traffic, dated Aug - Oct 1944].

T 791. Brasilien [German translations of decodes of Brazilian diplomatic traffic, dated Aug - Oct 1944].

T 803. Japan [German translations of decodes of Japanese diplomatic traffic, dated Aug - Oct 1944].

Target Intelligence Committee (abbreviated TICOM).-- A joint combined committee organized in the fall of 1944 in England for the exploitation of European Axis signal intelligence centers of special interest.

Telefonbau & Normalzeit. Firm in Frankfurt/Main which was constructing the SG 39 at the end of the war.

Teischmueller, _____. Member of Section IVc of OKW/Chi (initial breaking of more difficult systems; cryptanalytic theory). Worked with Weber in 1941 on a USA system.

Thiele, _____, Grig. Gen. Chief of Staff to Chief Signal Officer of Army.

Thielen, _____, First Lt. Succeeded Capt. Grotz as head of OKW intercept station at Sofia.

TICOM.-- Target Intelligence Committee. A joint combined committee organized in the fall of 1944 in England for the exploitation of European Axis signal intelligence centers of special interest.

TICOMMA. TICOM Materials.
Tito. Yugoslav Patriot leader.
Tranow, _____, Senior Specialist Dr. Head of Subsection IIIf (Britain and USA) of the Signal Intelligence Agency of the Navy High Command (OKM/ 4 SKL III).
Trappe, Rudolf, Mr. Member of OKW/Chi. Translated French and English military manuals, news items, etc.
Vauck, _____, First Lt. Dr. Member of Inspectorate 7/VI (In 7/VI); later member of Section IV, Signal Intelligence Agency of the Army High Command (OKH/G d NA); still later member of Section V of OKW/Chi. Chief of Subsection dealing with agents' traffic, called "Referat Vauck."
Verlaessliche Nachricht (VN).-- Translation into German of decoded diplomatic message. "Reliable Report"
VN (Verlaessliche Nachricht).-- Translation into German of decoded diplomatic message. "Reliable Report"
Voegele, Ferdinand, Specialist Dr. Chief of Section E (Referat E) of the Signal Intelligence Agency of the Commander in Chief of the Air Force (Chi-Stelle Ob d L) and principal cryptanalyst in the German Air Force.
Waffenfuehrungsstab (WFSt.).-- Operations Staff.
Waffenpruefung 7 (WA Pruef 7).-- Army Ordnance, Development and Testing Group, Signal Branch.
Waffen-SS (Waffen-Schutzstaffel).-- Armed Elite Guard. Components of Elite Guard serving at front.
Wagner, Reinhard, Acting Cpl. Member of Japan-China Subsection of OKW/Chi. Specialty: Japanese. Cryptanalyst as well as linguist.
Wa Pruef 7 (Waffenpruefung 7).-- Army Ordnance, Development and Testing Group, Signal Branch.
War Ministry.-- Kriegsministerium.
Weber, Werner, Prof. Dr. Member of Section IVc of OKW/Chi (initial breaking of more difficult systems; cryptanalytic theory).
Wehrmachtnachrichtenfuehrer z. b. V. 700 (Wehrmachtnachrichtenfuehrer zu besonderer Verwendung 700).-- Armed Forces Signal Officer for Special Employment #700.
Wehrmachtnachrichtenfuehrer Zu Besonderer Verwendung 700 (Wehrmachtnachrichtenfuehrer z. b. V. 700).-- Armed Forces Signal Officer for Special Employment #700.

DOCID: 3560827

Wehrmachtnachrichtenverbindung (WNV).-- Armed Forces Signal Communications.

WFSt. (Waffenfuehrungsstab).-- Operations Staff.

Wend, _____, Reserve Maj. Dr. Commanding officer of OKW intercept station at Lauf from 1 Dec 1939 to end of war.

Wendland, _____, Principal Specialist. Chief of Group V of OKW/Chi (routine breaking and translation); also chief of Balkan Subsection of Group V. Interested in Russian.

Wevering, _____, Senior Specialist. Chief of Scandinavian Subsection of OKW/Chi.

Witt, _____, Prof. Dr. Member of Section IVc of OKW/Chi (initial breaking of more difficult systems; cryptanalytic theory).

WNV (Wehrmachtnachrichtenverbindung).-- Armed Forces Signal Communications.

Yardley, Herbert Osborne. Author of book: The American Black Chamber (Indianapolis, the Bobbs-Merrill Co., 1931) which dealt with cryptanalysis in USA Military Intelligence Department.

Zastrow, Karl. Cryptanalyst in the Foreign Office Cryptanalytic Section (Pers Z S); specialist on USA systems. Lent to OKW as visiting specialist.

Zeimer, _____, Lt. Cmdr. Head of D/F station of Signal Intelligence Agency of the Navy High Command (OKM/4 SKL III) in Spain.

DOCID: 3560827

TAB B

TAB "B"

OKW/Chi and the beginning of Cryptologic Work in the German Army.

The pre-war relation between OKW/Chi and the Army's early signal intelligence agency called the Intercept Control Station (Horchleitstelle) is very obscure and into this obscurity the following remark of Mettig throws only a little light: "Before the war, cryptography in the German Army was carried out by OKH/In 7 Horchleitstelle.[1] This organization originated in the cipher section of the German War Ministry, and grew up parallel with the cipher section of the OKW (OKW/-Chi). Before the war, In 7 Horchleitstelle was merely a small department."[2] Now the War Ministry (Kriegsministerium) is simply the name the Defense Ministry (Reichswehrministerium) acquired after 1934. The organizations are identical. Since it is unlikely that this ministry had two cipher sections, one in Military Intelligence and one elsewhere, it is probable that the cipher section mentioned here as the parent of the Intercept Control Station (Horchleitstelle) is identical with the cipher section of the Defense Ministry which Mettig said elsewhere was the parent of OKW/Chi.

It may be suggested further that the officer in charge of the cipher section also controlled the fairly extensive intercept network which it is known that the Defense Ministry and later the War Ministry operated.[3] This suggestion is based on the remarks of Mr. Trappe who stated:

[1]An early designation of the Army Cryptanalytic Service. See Chapter II

[2]I-78, 2.

[3]See Chapter II

DOCID: 3560827

(1) That he was "employed by the Chiffrierstelle[4] office [sic]... at first of the Reichswehr Ministerium and later OKW from 1919" until he was captured by the Americans.

(2) That from 1919 to 1933, presumably while employed by the Chiffrierstelle, he served at intercept stations in Munich, Kassel (Niederzwehren), and Stuttgart before coming to the Reichswehr Ministerium in Berlin.[5]

The fact that an employee of the Cipher Section was physically located at the intercept stations implies a unified control of the two organizations.

Further, Trappe gives the following list of "Chiefs of the Chiffrierstelle":

1919: 1st Lt. Buschenhagen
1927: Major Schmidt
1931: Major Fellgeibel [sic]
1932: Major Oschmann
1934: Major Boetzel
1939: Major Kempff [sic]
1943: Major Kettler.[6]

Fellgeibel is probably identical with the Fellgiebel who was Chief Signal Officer both of the OKW (Chef WNV) and of the OKH (Chief of Army Signals), (Chef HNW) from the beginning of the war until he was dismissed in disgrace and executed for his part in the attempt on Hitler's life in July 1944. The German official file on Fellgiebel is available, and he is known to

[4] There is other evidence that the cryptologic section of the Reichswehr and later the OKW was known as the Chiffrierstelle. (Cipher Office). According to A-22 B, 7 a folder stamped Reichswehrministerium, Heeresleitung (Army Directorate), Chiffrierstelle, has been found among the Schliessee documents. A collection of correspondence of the German Navy signal intelligence service (TICOM Document 514 in film 49) contains a letter dated 23/9/36 and headed "Chiffrierstelle/Abw. II" (Abw. is probably for Abwehr). In a report from Huettenhain to Fenner dated November 1939, a reference is also made to the Chiffrierstelle of OKW. (Letter in T-1620).

[5] I-123, 2.

[6] I-123, 4.

have been a major in 1932.[7] Major (later Col.) Boetzel is well known as an expert in intercept. He ended the war as chief of the Signal Intelligence Agency of the Army High Command (OKH/ G d NA). It is very unlikely that these signal officers would have been in charge of the Cipher Section if the Cipher Section had been organized wholly separately from the intercept network.

Trappe is not a wholly trustworthy witness. That he was connected with Chi from an early date is undoubtedly true. He is mentioned in a letter from Huettenhain to Fenner as one who had worked on French codes in 1939, before the outbreak of the war.[8] Later on he seems to have worked on agents' ciphers,[9] and it may be in this connection that he made the trips abroad mentioned by Beyreuther. Beyreuther was unquestionably wrong when he stated that "Mr. Trappe .. has nothing to do with OKW/Chi.[10] He was, however, too far down in the organization to be a wholly reliable witness as to the niceties of organization at the top. His list of chiefs of the Cipher Section of the Defense Ministry (Chiffrierstelle) may be nothing more than a list of individuals whom at one time or another Trappe had considered the "big boss".

On the basis of the above material, the following development may be suggested, with the caution that the evidence is scanty and uncertain. The Cipher Section of the Defense Ministry (later the War Ministry) was subordinate to a signal officer who also controlled the Ministry's intercept network. When the War Ministry was replaced by the Supreme Command of the Armed Forces (OKW) and a separate Army High Command (OKH) set up to control the Army, the intercept organization was subordinated to the Army High Command. At the same time the Army drew on the Ministry's Cipher Section for a few trained

[7] IF-130, p 3. In 1932, the file declares Major Fellgiebel was Commander of Signal Battalion 2 (Kdr. Nach. Abt. 2). If Trappe is right, then this battalion must have controlled intercept operations.

[8] T 1620 (Film ES)

[9] I-132, 2.

[10] I-150, 9.

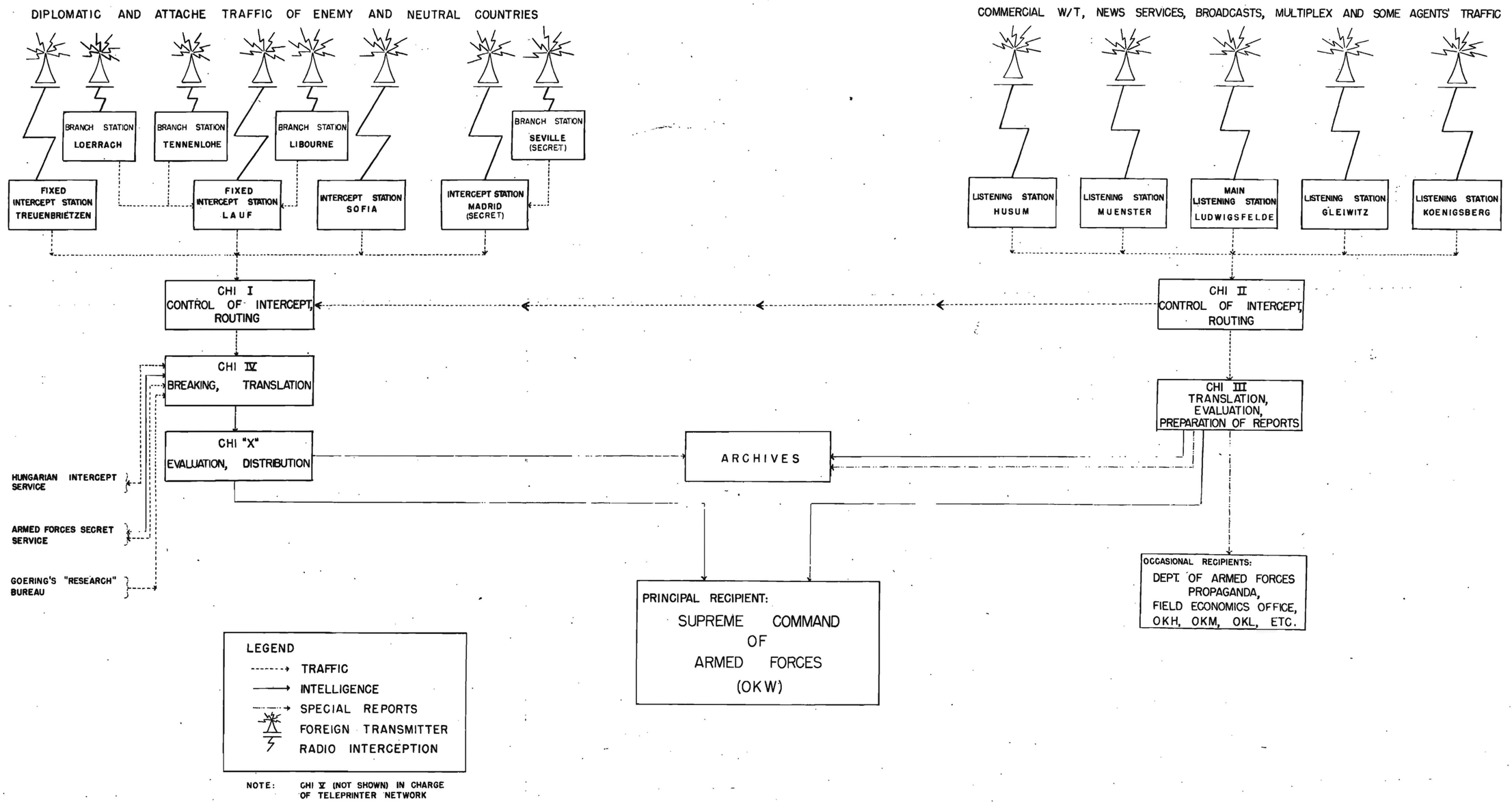
cryptanalysts and used them to work on foreign military traffic, which now became the exclusive sphere of the Army. Meanwhile, the main body of the Cipher Section came under the OKW, took over diplomatic traffic as a definite commitment, and remained for a while without an intercept organization of its own. Finally in 1939 the two Army intercept stations at Lauf and Treuenbrietzen were subordinated to the OKW and commissioned to intercept diplomatic traffic for OKW/Chi. The split between Army and Armed Forces signal intelligence services was then complete.[11]

[11] OKW/Chi's intercept operators, however, continued to be trained in the Army Signal School at Halle, according to Mrs. von Nida. (I-105, 5).

DOCID: 3560827

SIGNAL INTELLIGENCE AGENCY OF SUPREME COMMAND ARMED FORCES (OKW/CHI)

OPERATIONS CHART AS OF SPRING 1944



NOTE: CHI V (NOT SHOWN) IN CHARGE OF TELEPRINTER NETWORK

CHART NO. 3-2

DOCID: 3560827

DOCID: 3560827

TOP SECRET

SIGNAL INTELLIGENCE AGENCY OF SUPREME COMMAND ARMED FORCES

(OKW/WFST./AG. WNV/CHI)

ORGANIZATION AS OF APRIL 1945

CHIEF OF SERVICE
OBERST KETTLER

GROUP Z
PERSONNEL OFFICER, POLITICAL COMMISSARIAT
MAJOR LOBER
(4 + 9)

GROUP I
CONTROL OF INTERCEPT STATIONS
HPTM. GROTZ
(1 + 1)

- **SECTION I a**
  LIAISON WITH INTERCEPT STATIONS
  AMTMANN KLINGER
  (1 + 1)
- **SECTION I b**
  STUDY OF FOREIGN CALL SIGNS AND FREQUENCIES
  OWTM. SCHNÜCKEL
  (1 + 1)
- **SECTION I c**
  MAINTENANCE OF SIGINT - SERVICE TELECOMMUNICATION

INTERCEPT STATIONS
(DIPLOMATIC & MILITARY ATTACHE)
ABOUT 400 PERSONS

DIVISION A
CRYPTOGRAPHY
OBERSTLTN. METTIG
(1 + 1)

GROUP II
DEVELOPMENT AND ALLOCATION OF GERMAN SYSTEMS
(VACANT)

- **SECTION II a**
  KEY ALLOCATION POLICY, LIAISON WITH NAVY, AIR FORCE, AND POLICE ON CRYPTOGRAPHIC SECURITY
  HPTM. BERNSDORF
  (4 + 2)
- **SECTION II b**
  DEVELOPMENT OF GERMAN SYSTEMS
  SONDERFUEHRER DR. FRICKE
  (8 + 6)
- **SECTION II c**
  CODES AND CIPHERS FOR SECRET AGENTS
  REG. OBERINSP. MENZER
  (10 + 15)

GROUP III
PRODUCTION AND DISTRIBUTION OF KEYS
MAJOR METZGER
(25 + 215)

DIVISION B
CRYPTANALYSIS
MIN. RAT. FENNER
(1 + 2)

GROUP IV
CRYPTANALYTIC RESEARCH
REG.RAT. DR. HUETTENHAIN
(1 + 1)

- **SECTION IV a**
  TESTING OF GERMAN CRYPTOGRAPHIC PROCEDURES & DEVICES
  LT. DR. STEIN
  (10 + 1)
- **SECTION IV b**
  DEVELOPMENT AND CONSTRUCTION OF CRYPTANALYTIC MACHINERY
  REG.BAURAT ROTSCHEIDT
  (26 + 2)
- **SECTION IV c**
  INITIAL BREAKING OF MORE DIFFICULT SYSTEMS. CRYPTANALYTIC THEORY
  PROF. DR. FRANZ
  (10 + 38)
- **SECTION IV d**
  TRAINING
  DR. HUETTENHAIN

GROUP V
ROUTINE BREAKING AND TRANSLATION
MIN. RAT. DR. WENLAND
(1 + 1)

- **SUBSECTIONS V, 1-22**
  DESKS FOR VARIOUS COUNTRIES
  (190 + 130)
- **SECTION V a**
  TECHNICAL ASSISTANCE FOR LANGUAGE WORK
  SONDERFUEHRER (Z) KOEHLER

GROUP VI
MONITORING OF PRESS, BROADCASTS AND COMMERCIAL TRAFFIC
OBERSTLTN. KAEHLER
(1 + 1)

- **SECTION VI a**
  CONTROL OF GROUP VI'S INTERCEPT EQUIPMENT.
  REG. BAURAT DIPL. ING. SALZBRONN
  (30 + 30)
- **SECTION VI b**
  NEWS AGENCY TRANSMISSIONS (INCLUDING PICTURES) INTERNATIONAL COMMERCIAL RADIO TRAFFIC, MULTIPLEX
  OBLTN. SCHMIDT
  (30 + 30)
- **SECTION VI c**
  FOREIGN BROADCASTS
  ANGESTELTER KRAUSE
  (15 + 15)
- **SECTION VI d**
  EVALUATION OF GROUP VI'S MATERIAL, PUBLICATION OF REPORTS
  OBLTN. DR. SEYFARTH
  (6 + 6)

INTERCEPT STATIONS
(COMMERCIAL, NEWS SERVICES, BROADCASTS, MULTIPLEX, AGENTS)

GROUP VII
EVALUATION
OBERSTLTN. VON KALKSTEIN
(1 + 1)

- **SECTION VII a**
  EVALUATION AND DISTRIBUTION OF BROKEN MATERIAL & REPORTS BASED THEREON.
  (1 + 2)
- **SECTION VII b**
  ARCHIVES
  WTM. DR. SCHAEDEL
  (5 + 12)

ABBREVIATIONS:

DIPL. ING.	= DIPLOMINGENIEUR
HPTM.	= HAUPTMANN
LT.	= LEUTNANT
MIN. RAT.	= MINISTERIALRAT
OBERSTLTN.	= OBERSTLEUTNANT
OBLTN.	= OBERLEUTNANT
OKW/WFST/AG.WNV/CHI	= OBERKOMMANDO DER WEHRMACHT/ WEHRMACHTFÜHRUNGSSTAB/AMTS-GRUPPE WEHRMACHTNACHRICHTEN-VERBINDUNGEN/CHIFFRIERABTEILUNG.
OWTM.	= OBERWACHTMEISTER
REG.	= REGIERUNGS
WTM.	= WACHTMEISTER

NOTE: FIGURES IN PARENTHESES GIVE NUMBER EMPLOYED (SPECIALIST + CLERICAL). TOTAL PERSONNEL: 1606 (383 SPECIALIST + 423 CLERICAL + 800 INTERCEPT).

TOTAL PERSONNEL — ESTIMATED 1606

CHART NO. 3-1