~~TOP SECRET~~ ~~CREAM~~

~~SECRET~~

By Authority of the
Commanding General
Initials Date
WJS OCT 01 1948

ARMY SECURITY AGENCY

Washington, D. C.

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 4--SIGNAL INTELLIGENCE SERVICE OF THE ARMY HIGH COMMAND

Prepared under the direction of the
CHIEF, ARMY SECURITY AGENCY
1 May 1946
WDGAS-14

S-4759 listed on yellow card

~~TOP SECRET~~ ~~CREAM~~

VOLUME 4

The Signal Intelligence Service of the Army High Command

VOLUME 4

Chapter I: The History of the German Army Signal Intelligence Service.

1. The pre-Hitler Period(1919-1933)-- The pre-Hitler period of signal intelligence in the German Army is very obscure. From the scanty and uncertain evidence, however, the following organization may be suggested. A Codes and Ciphers Section of the German Defense Ministry (Reichswehrministerium Chiffrierabteilung), subordinated to an Army Signal Officer, had been maintained in skeleton force from the end of the first World War.[1] The Chiefs were:[2]

Lt. Buschenhagen	1919-1927
Major Schmidt	1927-1931
Major Fellgiebel	1931-1932
Major Oschmann	1932-1934
Major Boetzel	1934-1939

The head of the Codes and Ciphers Section of the German Defense Ministry also controlled the Ministry's intercept network. This network dated from 1923/4 when the first fixed intercept stations (Feste Horchstelle, abbreviated Feste) were established.[3] There is evidence of at least seven such stations operating before 1933.[4] Six of these were devoted primarily to the interception of foreign military traffic; and one to the interception of foreign diplomatic traffic. The six for military traffic were located at Stuttgart, Munich, Muenster, Koenigsberg, Liegnitz, and Breslau; the one for diplomatic traffic, at Treuenbrietzen.[5]

[1] I 96 p 2

[2] I 123 p 4

[3] I 62 p 5; IF 181 p 1

[4] I 85 p 2

[5] I 62 p 6

2. The pre-World War II Period (1933-1939)-- In 1933/34, the German Defense Ministry set up three more intercept stations: one at Hersbruck (later moved to Lauf); the other two, at Striegau and Chemnitz.[6] With these ten intercept stations, the German Defense Ministry intercepted foreign Army, Air Force, and diplomatic traffic. The German Defense Ministry also set up in 1933/4 in Berlin its own military code and cipher section called the Intercept Control Station (Horchleitstelle, abbreviated HLS).[7] For this it drew a few trained cryptanalysts from the Codes and Cipher Section of the German War Ministry (Reichskriegsministerium).[8] Foreign Army traffic intercepted by the German Defense Ministry was sent to the Intercept Control Station (Horchleitstelle); Air Force traffic, to the Signal Intelligence Agency of the Commander-in-Chief of the Air Force (Chiffrierstelle des Oberbefehlshabers der Luftwaffe, abbreviated Chi-Stelle OBdL) established in 1937.[9] Diplomatic traffic was sent to both the Codes and Ciphers Section of the German Defense Ministry (called after 1934 the German War Ministry (Kriegsministerium) and the Foreign Office Cryptanalytic Section (Sonderdienst des Referats Z in der Personalabteilung des Auswaertigen Amts, abbreviated Pers ZS).[10]

3. The early World War II Period (1939-1941)-- During the early years of the war, the main developments within the German Army signal intelligence service were the following:

a. The narrowing of the mission of the intercept service to include only Army traffic. In 1939 a newly formed Signal Intelligence Agency of the Supreme Command of the Armed Forces (Oberkommando der Wehrmacht/Chiffrier-Stelle, abbreviated OKW/Chi) took over the interception of all foreign diplomatic traffic from the German Army Signal Intelligence Service, and for that purpose the Army gave it two of its own intercept stations, at Lauf and Treuenbrietzen.[11]

[6] I 85 p 3

[7] I 78 p 2

[8] The German Defense Ministry was renamed the German War Ministry after 1935.

[9] IF 181 p 15

[10] I 85 p 2

[11] I 85 p 3

b. The expansion of intercept service. In 1939, the Army established two new branch stations for the intercept of foreign Army traffic emanating from the east, one at Graz and the other at Tullin.[12]

c. The establishment of five Signal Intelligence Regiments (Kommandeur der Nachrichten Aufklaerung, abbreviated "KONA"). These regiments were sent into the field as complete intercept and evaluation units, attached to Army Groups.[13] The KONA were given the numbers one through five. KONA 1, 2, 3 were assigned to German Armies on the eastern front: KONA 1 to the Army Group on the southern front, KONA 2 to the Army Group on the central front, and KONA 3 to the Army Group on the Northern front. KONA 4 was not attached to any Army Group but was subordinated to the Commanding Officer who controlled the German Armies in the Balkans (Befehlshaber Suedost).[14] KONA 5 was assigned to the Army Group on the Western front.[15]

d. The introduction of mathematicians and linguists. To cope with the increased amount of enemy Army traffic on all levels, and the increasingly difficult problems of solution, mathematicians and linguists were drafted into the Army in 1939 and were assigned either to the various field units or to the Intercept Control Station.[16]

e. An increased interest on the part of the Army in the security of its own systems. This new interest gave rise to the establishment of an Army Signal Security Agency designated as Group IV of Inspectorate 7 (Inspektion 7 Gruppe IV, abbreviated In 7/IV) which was subordinated to the Chief of Army Equipment and Commander of the Replacement Army (Chef der Heeresruestung und Befehlshaber des Ersatzheeres, abbreviated "Chef H Ruest u. BdE"). In 7/IV was composed

[12] I 85 p 3

[13] I 78 p 4

[14] IF 171 p 1

[15] IF 127

[16] I 78 p 4

of mathematicians and former actuaries whose function was the examination of cryptographic systems used by the German Army, and the preparation, printing and distribution of codes and ciphers.[17]

The German Army signal intelligence service in 1939 consisted of the following parts:

(1) at least 10 intercept stations for the interception of foreign Army traffic called Feste Horchstellen, abbreviated Feste
(2) five Signal Intelligence Regiments attached to Army Groups (each called Kommandeur der Nachrichten Aufklaerung, or "KONA")
(3) an Intercept Control Station (Horchleitstelle, or HLS) for the analysis and evaluation of foreign Army traffic;
(4) an Army Signal Security Agency (Inspectorate 7/IV, or In 7/IV) for testing and issuing codes and ciphers for the Army.

4. The Middle World War II Period (1941-1944)-- When, in 1941, the small staff at the Horchleitstelle was found to be inadequate to cope with the large amount of traffic which had resulted from the increasing pressure of the war, two central agencies were established to replace the station: a central cryptanalytic agency at Berlin designated as Inspectorate 7/VI of the Chief of Army Equipment and Commander of the Replacement Army (Chef der Heeresruestung und Befehlashaber des Ersatzheeres Inspektion 7 Gruppe VI, abbreviated Chef H Ruest u BdE/ In 7/VI or more simply In 7/VI); and a central evaluation agency at Zossen designated as Control Station for Signal Intelligence (Leitstelle der Nachrichten Aufklaerung, abbreviated LNA).

In 7/VI was organized by Major Mang of the German Army, whose aim was not only to increase the cryptanalytic staff of the new agency but also to provide reserves of cryptanalysts to work in key areas in the field. In order to acquire personnel easily, Major Mang subordinated In 7/VI in matters of personnel and administration to the Chief of Army Equipment and Commander of the Replacement Army (Chef H Ruest u BdE)[18]

[17] I 92 p 6

[18] I 78 p 5

In matters of policy, however, In 7/VI was subordinated to the Field Army. This curious form of organization is said to have enabled the cryptanalytic service to recruit sufficient personnel without serious interference while maintaining close operational contact with field units.[19]

During the first few months of the existence of In 7/VI, Russian cryptanalysis was included in the cryptanalytic work done at In 7/VI, and Russian evaluation was included in the evaluation done by LNA. Both these organizations, however, soon felt that the cryptanalysis and evaluation of Russian traffic should be carried on closer to the forward echelon of the German Field Army in East Prussia. In late 1941, therefore, some cryptanalysts and evaluators skilled in Russian traffic were detached from In 7/VI and from LNA respectively, and were sent to Loetzen to work.[20] These cryptanalysts and evaluators became the nucleus of the organization which later became the chief cryptanalytic and evaluation agency for Russian traffic, named Intercept Control Station East (Horchleitstelle Ost, abbreviated HLS Ost). From this point until November 1944 signal intelligence activities were sharply divided into Russian signal intelligence, carried on by HLS Ost, and non-Russian signal intelligence, carried on by In 7/VI and LNA.

In 1942, the responsibility for security testing of existing German Army cryptographic systems had been transferred from In 7/IV to In 7/VI.[21] From that time, the Army Signal Security Agency, In 7/IV, had been confined to the development of new systems for the Army and to the production, printing and distribution of current keys and systems.[22]

[19] I 78 p 5

[20] I 78 p 5

[21] I 78 p 6

[22] I 36 p 2

In the fall of 1943, In 7/VI had been transferred to the newly created Department of Signals of the General Army Office and renamed Signal Intelligence, Department of Signals, General Army Office, Army High Command (Oberkommando des Heeres/Allgemeines Heeres Amt/Amtsgruppe Nachrichten/Nachrichten Aufklaerung, abbreviated OKH/AHA/AgN/NA) Minor changes in internal organization were effected, but the function and operation of the agency was not changed.[23]

Although there was no essential change in the organization of the field units of the German Army Signal Intelligence Service from 1941 to 1944, additional units were placed in the field. In 1942 the eastern KONA (1, 2, and 3) were supplemented by the addition of KONA 6 which was formed to cover the German campaign in the Caucasus.[24] This KONA was not subordinated to any Army Group but was directly under HLS Ost. KONA 7 was established in February 1943 and was subordinated to the Commander-in-Chief South (Oberbefehlshaber Sued) who controlled Army Group C and the German forces in Italy.[25]

The organization of the German Army Signal Intelligence Service in 1944 consisted of:

1) a central cryptanalytic agency for non-Russian traffic, In 7/VI (latterly AgN/NA)
2) a central evaluation agency for non-Russian traffic, LNA;
3) a central cryptanalytic and evaluation agency for Russian traffic, HLS Ost;
4) seven Signal Intelligence Regiments (KONAs);
5) an Army Signal Security Agency for the distribution and development of Army systems (In 7/IV).

5. The Late World War II Period (1944-1945).-- In October 1944, the organization of the German Army signal intelligence service was completely changed through the amalgamation of the three central agencies, In 7/VI (latterly AgN/NA), LNA, and HLS Ost, into one central cryptanalytic and evaluation agency, (the Signal Intelligence Agency of the Army High Command, the Oberkommando des Heeres/General der Nachrichten Aufklaerung, abbreviated OKH/GdNA). This amalgamation was the logical result of the retreat of HLS Ost together with the German Army, from East Prussia to Zossen, where In 7/VI and LNA were situated.[26]

[23] IF 190 B p 4

[24] DF 18 p 81

[25] IF 172 p 2

[26] IF 123 p 5

The Signal Intelligence Regiments (KONAs) were not greatly affected by the amalgamation of the central agencies into the GdNA, although the KONAs did come "under closer centralized control in matters of administration and signal intelligence policy."[27]

The main changes in the Army's signal intelligence field organization in 1944-1945 were necessitated by the Allied invasion of France in June 1944. To cope with this situation, KONA 6 was moved from the eastern front to the western;[28] and a Senior Commander of Signal Intelligence (Hoeherer Kommandeur der Nachrichten Aufklaerung, abbreviated Hoeh Kdr d NA) was set up to coordinate and control KONA 5 and 6.[29] In late 1944 and early 1945, two additional KONAs were formed in the east, KONA 8 and KONA Nord,[30] but it is noteworthy that these KONAs were largely composed of units borrowed from other eastern front Signal Intelligence Regiments, and the creation of these last two KONA was thus not so much a mark of expansion as of redeployment to areas under stress.[31]

Colonel Boetzel, chief of the Signal Intelligence Agency of the Army High Command (OKH/GdNA) stated that KONA 4 was transferred to the West at the end of the war.[32] A captured document[33] indicated that KONA 4 had been succeeded by a signal battalion Nachrichten Aufklaerung Abteilung, abbreviated NAA) 16, in February 1945 but did not mention its transfer to the West. It is probable that the KONA disintegrated and that various parts were sent to the different fronts.

The organization of the German Army signal intelligence service at the end of the war consisted of:

1) the Signal Intelligence Agency of the Army High Command(OKH/GdNA) a central cryptanalytic and evaluation agency for all traffic.
2) a Senior Commander of Signal Intelligence,(Hoeh Kdr d NA) with control over the KONA stationed in the west and responsibility for all signal intelligence activities of the German Army in the West;
3) nine Signal Intelligence Regiments (KONAs) which were attached to Army Groups or Commanders in the field.

[27] IF 123 p 5

[28] I 76 Appendix, Chart I

[29] IF 123 p 5

[30] T 1402

[31] See below Chapter IV

[32] I 76 p 7

[33] T 1402

VOLUME 4

Chapter II: Organization of Central Agencies of the German Army Signal Intelligence Service.

6. Organization of the Intercept Control Station 1933-1941.-- Not much is known of the organization of the Intercept Control Station (Horchleitstelle, abbreviated HLS), before 1941. The existence of sections for the cryptanalysis and evaluation[35] of Belgian, Polish, Russian, and British traffic may be surmised from Mettig's account of its activities.[36] Nothing specific, however, is known from TICOM sources. The small staff was commanded by Major Dr. Jung.[37]

7. Organization of In 7/VI.--

a. Inspectorate 7/VI (Inspektion 7/VI, abbreviated In 7/VI) in the autumn of 1941 was headed by Major Mang, and was divided into the following sections with heads as shown:[38]

Personnel Section	Captain Herbrueggen
British Section	Senior Inspectors Zillman and Liedtke
French Section	Senior Inspector Kuehn
Italian Section	Captain Fiala

[35] Evaluation is a free translation of the German word "auswertung" which to the Germans meant traffic analysis, the interpretation of news broadcast and plain text transmissions, the interpretation of radio telephone intercept, and the interpretation of the results of successful cryptanalysis. All these things taken together resulted in fully evalusted intelligence.

[36] I 78 p 3

[37] I 78 p 2

[38] IF 190 B App. 3

Balkan Section.....	Senior Specialist Bailovic
Mathematical Section.....	1st Lt. Lueders and Technician Dr. Pietsch
Russian Section.....	1st Lt. Dettman
Linguistic Section.....	Technician Koehler
Training Section.....	Senior Inspector Kuehn

Between 1941 and 1943 the following changes in the Organization of In 7/VI took place:

a) the Russian section was sent to Loetzen, East Prussia[39]
b) a section for cryptanalysis of USA systems was formed with the entry of the USA into the war[40]
c) a section for cryptanalysis of traffic of agents (foreign and internal) was added in 1942[41]
d) the investigation of the security of current German Army systems was transferred from In 7/VI, the former Army Signal Security Agency, to the mathematical section of In 7/VI[42]
e) an IBM section together with its machinery from In 7/IV was added[43]

b. In 7/VI in the spring of 1943 was divided into the following sections:[44]

Chief.....	Major Mettig
British Section.....	Senior Inspector Zillmann
USA Section.....	Technician Dr. Steinberg
Balkan Section.....	Senior Specialist Bailovic
French Section.....	Technician Kuehn
Italian Section.....	Corporal Manaigo
Mathematical Section.....	Technician Dr. Pietsch
Linguistic Section.....	Technician Koehler
Training Section.....	Senior Inspector Kuehn
Agents Section.....	1st Lt. Vauck
IBM Section.....	Specialist Schenke

[39] I 78 p 8
[40] I 78 p 10
[41] I 115 p 3
[42] I 78 p 6
[43] I 78 p 6
[44] IF 190 B App 4

The sections of In 7/VI were housed during this period in buildings near the Bendlerstrasse in Berlin. The headquarters Training Section and sections for USA, French and Agents' traffic were located at Matthaekirchplatz 4;[45] the British and Balkan section, at Schellingstrasse 9; the IBM section, on Viktoriastrasse. Location of the Mathematical section is not known.[46]

In November 1943, the first large RAF raid on Berlin destroyed a great part of the offices of the Army High Command on Bendlerstrasse in Berlin, among which were those of In 7/VI. In 7/VI was thereupon moved to Jueterbog, where it was located until its amalgamation in November 1944 into GdNA.[47]

No estimate is given of the number of people employed in In 7/VI.

c. Organization of AgN/NA. When In 7/VI was reorganized as the Signal Intelligence Section of the Department of Signals of the General Army Office, of the Army High Command, the internal organization was somewhat changed. The previously independent sections were organized into a main section (Hauptreferat) for mathematics, and a main section for languages. The IBM section retained its autonomy.

The Main Section for Languages, with the exception that one section was added for Swedish traffic, covered the same field as had been covered by the individual language sections of In 7/VI. The organization of AgN/NA is outlined thus:[48]

Chief	Major Lechner
Main Section A for Mathematics	1st Lt. Lueders
Main Section B for Languages	Senior Specialist Bailovic
British Section	Senior Inspector Zillmann
USA Section	Technician Steinberg
French Section	Technician Kuehn
Balkan Section	Senior Specialist Bailovic
Swedish Section	Pfc. Rohden

[45] I 58 p 2

[46] IF 126 pp 6-7

[47] IF 126 p 6

[48] IF 190 B App 5

Linguistic Section..... Technician Koehler
Training Section..... Senior Inspector Kuehn
IBM Section..... Specialist Schenke

8. Organization of the Control Station for Signal Intelligence (LNA).-- The organization of the central evaluation agency for non-Russian traffic, the Control Station for Signal Intelligence (Leitstelle der Nachrichten Aufklaerung, abbreviated LNA) is obscure.

According to Krause, a member of LNA, there were sections for evaluating British, USA, Italian, Balkan, Greek, Turkish, Tunisian, Near Eastern, Portuguese, and Spanish traffic. Evaluation was made both of traffic and of the contents of decoded messages passed to these sections from In 7/VI. The staff of LNA was comparatively small, consisting of about seventy-five persons who were housed in one building for which the ground plan is given in a CSDIC publication.[49]

9. Organization of HLS Ost.-- The Intercept Control Station East (Horchleitstelle Ost, abbreviated HLS Ost) was the central cryptanalytic and evaluation center for Russian traffic located at Loetzen, East Prussia from late 1941 to late 1944. The exact size of the station is not known, but the organization is outlined as follows:[50]

Section "Z".....Personnel problems
Section 1.....Supply, maintenance, evaluation of captured documents and general research into wireless procedures.
Section 2.....Evaluation, compilation of intercept situation report
Section 3.....Russian cryptanalytic section.
Section 4.....Monitoring of inter-Soviet State traffic; Russian radio broadcasts and Reuter and Tass News Agency broadcasts.

[49] IF 111 Annexes 1 and 2

[50] IF 123 p 4

In the winter of 1942-43, the Baudot Reception Station was moved from Minsk to Loetzen and subordinated to HLS/Ost, Section 4.

HLS Ost was first directed by Col. Kettler, who later became chief of the Signal Intelligence Agency of the Supreme Command of the Armed Forces (OKW/Chi). In the summer of 1942, Kettler was succeeded by Baron Col. von der Osten-Sacken, who remained its chief until July 1944, when he was implicated in the plot on Hitler's life and committed suicide.[51]

10. Organization of Signal Intelligence Agency.-- The three agencies, In 7/VI (latterly AgN/NA), HLS Ost and LNA were amalgamated in November, 1944, into the Signal Intelligence Agency of the Army High Command (Oberkommando des Heeres General der Nachrichten Aufklaerung, abbreviated OKH/GdNA) almost intact.[52] In 7/VI (latterly AgN/NA), with some slight depletion of personnel, became Group IV of GdNA, which was assigned the responsibility for all cryptanalysis on foreign military traffic. LNA was transferred as a unit to Group II of OKH/GdNA, except for those sections which had been dealing with wireless and news agency traffic. These sections were assigned to Group I at OKH/GdNA. The various sections of HLS Ost were absorbed into the appropriate sections of OKH/GdNA as follows:

Section Z.....	into Group Z
Section 1.....	into Group V
Section 2.....	into Group III
Section 3.....	into Group IV
Section 4.....	into Group VI (except the wireless and news agency which went to Group I)

The organization of the OKH/GdNA which is explained in the following pages is outlined on Chart 4-2. It was in effect from November 1944 to the capitulation. Approximately 700 people were employed by the OKH/GdNA.[53]

[51] IF 123 p 4

[52] IF 123 pp 5-6

[53] All material concerning the organization of the GdNA is derived either from IF 123 pp 6-14 or I 113 pp 5-12, the account by Major Hentze, head of Group IV of the GdNA.

a. Headquarters unit. The Headquarters unit of OKH/GdNA consisted of the Chief, Signal Intelligence Service (Chef, General der Nachrichten Aufklaerung, abbreviated Chef/GdNA), Colonal Boetzel; his Chief of Staff, Lt. Col. Andrae; the Adjutant, Lt. Moravec, and the Chief of the Understaff, Lt. Koebe.

The staff controlled the signal intelligence work of all units of the GdNA, Groups I through VI. It also controlled two intercept stations, Feste 6 and Feste 11. These had been subordinated to HLS Ost before being attached to the GdNA. They specialized in intercepting high frequency traffic of the Red Army and NKVD.[54]

The Understaff of the OKH/GdNA supervised the intercept coverage of the Signal Intelligence Regiments (Kommandeure der Nachrichten Aufklaerung, abbreviated KONA) and their subordinate units: directly, in the case of KONA 1,2,3,7, and 8; and through the Senior Commander of Signal Intelligence (Hoeherer Kommandeur der Nachrichten Aufklaerung, abbreviated Hoeh, Kdr. d NA) for KONA 5 and 6.[55]

b. Group I. Group I was under the supervision of Bodenmueller. It had two main tasks:

1) the maintenance of communications between the units of the GdNA;
2) press monitoring.

For internal communications, teleprinter was used until the final debacle, when it became necessary to resort to radio. To carry out the second task of Group I, press monitoring, there were four subsections: the monitoring of eastern wireless, western wireless, plain text monitoring, and evaluation. The evaluation sub-section (4) was responsible for collating all information from the other three sub-sections and consolidating it into reports. The collated reports were divided into separate parts for political, economic, or military news. They were circulated within the departments of the Army High Command, sometimes with the classification SECRET (Geheimkommandosache, abbreviated GKdoS). Because of the personnel shortage, the BBC London Service and the Reuter Agency were the only news agencies monitored for western traffic.

[54] IF 123 p 6

[55] IF 123 p 6

c. Group II. Group II which had cannibalized LNA and consisted of about 50 people, produced radio situation reports correlating the information from KONAs 5, 6, and 7. Capt. Thiel, who was head of this group, had been with LNA for a long time and was said by Hentze to have been thoroughly familiar with the problems of western evaluation.

d. Group III. This group, under the supervision of Capt. Gorzolla, was responsible for the evaluation of traffic and cryptanalytic work emanating from the Russian front. The department was divided into the following sections:

Traffic Sorting Office
Northern Sector Evaluation
Central Sector Evaluation
Southern Sector Evaluation
Russian Special Police (NKVD) Evaluation
Partisan traffic evaluation
Swedish traffic evaluation

e. Groups IV. Group IV, under Major Hentze, was responsible for all cryptanalytic work done at GdNA. It was one of the largest groups of the OKH/GdNA, having been built up from parts of three former agencies, In 7/VI, LNA and HLS Ost. The group was divided into separate sections according to the origin of the material.

Section I, headed by the mathematician, Dr. Pietsch, was the former Mathematical Section of In 7/VI. It was responsible for the security of German Army Systems. Sub-section 1a, headed by Marquardt, was engaged in research on German Army hand systems; sub-section 1b, under Dr. Pietsch handled research on German Army machine systems.

Section 2, headed by Kneschke, dealt with the cryptanalysis and deciphering of non-Russian traffic. There were three sub-sections:

2a: British and USA systems;
2b: French systems;
2c: Balkan systems

Section 3, headed by Lt. Dettmann, was composed of the cryptanalytic sections of HLS Ost. It dealt with Russian systems and had four sub-sections:

3a: Russian Special Police traffic (NKVD);
3b: Russian Army traffic;

3c: Russian Partisan traffic;
3d: Research on Russian systems.

Section 4 was the former IBM section of In 7/VI. According to Major Hentze, this section performed mainly statistical work. Most of the members were women used to run the machines. The section maintained its own repair shop for the machines.

Section 5 was the training department of the GdNA, where cryptographic and cryptanalytic courses were given under the direction of Inspector Kuehn, who had headed the Training Section of In 7/VI. During the last months of the war, the once flourishing section dwindled to a group of forty students every three months.

f. Group V. Group V was a mixed group containing three sections all of which carried out unrelated activities.

Section 1. This section headed by Inspector Zipper, was engaged in reconstructing Russian, British, and USA call signs and call signs systems, and deducing units therefrom. It covered various procedures of enemy wireless and the allocation of wave lengths.

Section 2. This section under Specialist Block was responsible for the exploitation of captured Russian documents of signals interest. Captured manuals were translated and descriptions of Russian equipment examined.

Section 3. This section was engaged in supplying the KONAs with necessary intercept equipment and in maintaining a workshop to service the needs of the OKH/GdNA itself.

g. Group VI. Group VI, located at Potsdam under Capt. Roeder, was responsible for intercepting and evaluating special high-grade machine systems, Russian systems were handled by Section 1, with three sub-sections:

1a: interception and evaluation of Inter-Soviet State traffic;
1b: intercepting and evaluation of Russian Baudot;
1c: intercepting and evaluation of Russian Army traffic.

Western teleprinter and automatic morse traffic was handled by Section 2. (Interception was done in sub-section 2b, evaluation in sub-section 2a).

h. Group Z. Group Z (which is not shown on the chart) was responsible for general administrative control of all departments within the OKH/GdNA. The work was divided into four types: personnel, communications, pay, and drawing. A central card index was kept of all personnel employed in the OKH/GdNA and the personnel section was responsible for all transfers, either inter-departmental or outside the OKH/GdNA. The section for communications registered all incoming and outgoing correspondence and was responsible for all courier communications between the OKH/GdNA and its subordinate units. For local communications, this section had its own runners; but for long distances, the courier services of the Army High Command were used. All personnel of OKH/GdNA were paid by the "pay" section. In the drawing section, all situation maps and radio networks were reproduced. A certain amount of photostat and book-binding activity was also carried on here.

Because of the lack of detailed information concerning German signal intelligence at the end of the war, it is difficult to appraise the effectiveness of the final reorganization of November 1944. In large measure, the logical simplicity of outline was disrupted in the last months. The full organization existed as an integrated unit only from November, 1944 to February, 1945. From that time until the surrender, the OKH/GdNA was almost continously on the move seeking refuge in southern Germany. Most of the groups moved from Zossen to Bad Reichenhall either directly or by way of Erfurt. Somewhere between Erfurt and Bad Reichenhall in the Weimar area, the IBM section was lost. Group VI which had been located at Potsdam went first to Stuttgart and then to Rosenheim.[56]

[56] IF 123 p 6-13

VOLUME 4

Chapter III: Organization of the German Army Field Signal Intelligence Service

11. The organization of the typical Signal Intelligence Regiment.-- The basic element of the field organization of the German Army signal intelligence service was the Signal Intelligence Regiment (Kommandeur der Nachrichten Aufklaerung, abbreviated KONA). Each Army Group was provided with a Signal Intelligence Regiment (KONA), which had control over all signal intelligence units in the area governed by the Army Group. If, as was the case with KONA 4 and KONA 7, the Signal Intelligence Regiment was attached to a Commander of the German Armies stationed in an area, the Signal Intelligence Regiment had control of all signal intelligence units within the area of that command.

There were, of course, variations in the organization and manner of operation of the various Signal Intelligence Regiments corresponding to differences in personnel, equipment, and operational responsibilities. The typical component parts of a Signal Intelligence Regiment, however, were: [60]

[60] I 190 p 5

One Signal Intelligence Evaluation Center (Nachrichten Aufklaerung Auswertestelle, abbreviated NAAS), designed to work with KONA headquarters at Army Group level; usually one Stationary Intercept Company (Feste Nachrichten Aufklaerungsstelle, abbreviated Feste), designed to work at Army level; usually two Long Range Signal Intelligence Companies (Nachrichten Fernaufklaerung Kompanie, abbreviated FAK), designed to work at Army level; usually two Close Range Signal Intelligence Companies (Nachrichten Nahaufklaerung Kompanie, abbreviated NAK), designed to work at Army Corps level; each Close Range Company usually had two or three Close Range Signal Intelligence Platoons (Nachrichten Nahaufklaerungszug, abbreviated NAZ), designed to work below the NAK but still at Army Corps level.

In 1944, the Signal Intelligence Battalion (Nachrichten Aufklaerung Abteilung, abbreviated NAA) was introduced into the organization of the KONA. These battalions were small administrative units, which acted as coordinating units at Army level.

Major Hertzer, CO of KONA 1, stated that the NAA commanders were generally elderly supervisors whose chief duty was to make the rounds of the units forming the NAA gathering opinions and effecting small adjustments in the use of close range signal intelligence platoons. Colonel Boetzel, head of OKH/GdNA, stated that the NAA was not considered an effective improvement.[61]

This chapter will deal with each Signal Intelligence Regiment separately and will give in some detail the organization and history of the components of each.

[61] I 19g p 5

12. Organization of KONA 1.-- KONA 1 was organized in the following way. To KONA headquarters were subordinated:[62]

1 Signal Intelligence Evaluation Center, NAAS 1
1 Stationary Intercept Company, Feste 10
1 Close Range Signal Intelligence Company, NAK Preuss
2 Signal Intelligence Battalions, NAA 3 and NAA 4

To NAA 3 were subordinated:

1 Long Range Signal Intelligence Company, FAK 623
1 Close Range Signal Intelligence Company, NAK 953 (later NAK Benold)

To NAA 4 were subordinated:

1 Long Range Signal Intelligence Company FAK 617
1 Close Range Signal Intelligence Company, NAK 954

a. Headquarters Unit. The headquarters units of KONA 1, which worked at Army Group headquarters, consisted of the commandant of the KONA, his Adjutant, a Chief of Operations (S-3), a paymaster, a technical inspector, clerks, and truck drivers. The following statistics show the breakdown of the headquarters unit.[63]

	Officers	Enlisted Men	Women
Co	1	-	-
Adj.	1	-	-
S-3	1	-	-
Paymaster	1	-	-
Technical Inspector	1	-	-
Clerks	-	4	2
Truck drivers	-	9	-
	5	13	2

[62] I 198 p 5

[63] IF 40 p 12

b. NAAS 1. The NAAS of KONA 1 had two major operational subdivisions: a section engaged in evaluation and traffic analysis, and a section for cryptanalytic activities. There were also a headquarters section, a communication line section, and a section of truck drivers. The personnel, totalling eight officers, one hundred sixty enlisted men, and fifty enlisted women were thus divided among the section: 64

Section	Officers	Enlisted Men	Women
Headquarters	1	18	2
Evaluation	6	66	25
Cryptanalysis	1	42	-
Communication	-	21	23
Truck Drivers	-	13	-
	8	160	50

c. Feste 10 and the Long Range Intercept Companies. The Stationary Intercept Company, Feste 10, and the Long Range Signal Intelligence Companies, FAK 617 and FAK 623, were similar in their organization and operation. Each had a headquarters section, monitoring platoons, an evaluation section, a cryptanalytic section, and a communication line platoon. The differences between Feste 10 and the FAK were minor. Feste 10 was less mobile than the FAK, having eight truck drivers instead of the twelve and sixteen assigned to FAK 617 and FAK 623 respectively.

64 IF 40 p 12

The following lists show the subsections and strength of Feste 10, FAK 617, and FAK 623:[65]

Feste 10

Section	Officers	Enlisted Men	Women
Headquarters	1	18	2
Monitoring Plt.	-	32	61
Evaluation	1	25	8
Cryptanalysis	1	15	2
Communication Ln. Plt.	-	10	-
Truck Drivers	-	8	-
Enemy Radio Station Locators	-	50	-
	3	158	73

FAK 617

Section	Officers	Enlisted Men	Women
Headquarters	1	15	3
Monitoring Plts.	1	91	-
Evaluation	1	33	-
Cryptanalysis	-	20	-
Communication Ln. Plt.	-	23	-
Truck Drivers	-	16	-
	3	198	3

[65] IF 40 p 13

FAK 623

Section	Officers	Enlisted Men	Women
Headquarters	1	14	4
Monitoring Plts.	1	83	-
Evaluation	1	34	-
Cryptanalysis	-	16	-
Communication Ln. Plt.	1	17	-
Truck Drivers	-	12	-
	4	176	4

d. NAK 954. The Close Range Signal Intelligence Company, NAK 954, was divided into sections comparable to those of Feste 10 and the long-range intercept companies, as the following chart indicates: [66]

Section	Officers	Enlisted Men	Women
Headquarters	1	41	-
Evaluation	-	30	-
Radio Receiving	-	25	-
Communication Ln. Plt.	-	18	-
4 Monitoring Plts.	4	112	-
	5	226	-

The NAK operated by platoons, one platoon attached to each Army Corps.[67] The strength of a platoon was from twenty to thirty men, of which approximately twelve were engaged in radio telephone intercept, two in radio intercept, five in direction finding, and three in evaluation. The rest of the platoon comprised clerks, drivers, cooks, etc.

[66] IF 40 p 13

[67] I 19b p 2

e. NAK 953. Up to September, 1944 NAK 953 was subordinated to NAA 3 of KONA 1; but at that time it was moved to the west, leaving behind only its interpreters and cryptanalysts, who continued to serve on the eastern front.[68]

f. NAK Benold. NAK Benold, named after its CO, was composed of specialists of various kinds who had been drawn from the signal intelligence companies subordinate to KONA 1. As a company it formed part of NAA 3.

g. NAK Preuss. NAK Preuss, taking its name as did NAK Benold, from its CO, was formed from forces withdrawn from other units of KONA 1. This close range signal company was, in contrast to the other companies, subordinated directly to KONA Headquarters.

13. Organization of KONA 2. -- The organization of KONA 2 is not known in detail. As far as can be determined from TICOM sources, there were subordinated to this KONA in 1944:[69]

1 Signal Intelligence Evaluation Center, NAAS 2
3 Signal Intelligence Battalions, NAA 6, 7, and 8
1 Stationary Intercept Company, Feste 7
3 Long Range Signal Intelligence Companies, FAK 610, 619, 622
3 Close Range Signal Intelligence Companies, NAK 951, 955, 958

In February 1945, these components of KONA 2 were split: part of them remained with KONA 2, which was reassigned from Army Group North to Army Group Weichsel; part of them were attached to KONA Nord, which took the place of KONA 2 with Army Group North. The original components were divided between the two KONA in the following way:[70]

KONA 2:

2 Long Range Signal Intelligence Companies, FAK 610, 622
1 Close Range Signal Intelligence Company, NAK 958
1 Stationary Intercept Company, Feste 7

[68] I 19b p 1

[69] DF 9; I 76 Appendix

[70] DF 9

KONA Nord:

1 Long Range Intercept Company, FAK 619
1 Close Range Signal Intelligence Platoon, NAZ Brutus
2 Close Range Signal Intelligence Company NAK 951, 955
1 Signal Intelligence Evaluation Center, NAAS 2

This remained the general organization until 28 March, 1945, when by order of General Praun, Chief Signal Officer, Armed Forces (Chef Wehrmacht Nachrichtenverbindungen, abbreviated Chef WNV) and Chief Signal Officer, Army (Chef Heeres Nachrichtenverbindung's wesen, abbreviated Chef HNW.) KONA Nord returned to KONA 2 all its units except the Close Range Signal Intelligence Companies, NAK 951 and 955. [71]

14. Organization of KONA 3.-- KONA 3 was composed, insofar as is known, of one NAA (10),[72] one FAK, one NAK and one Feste. (The FAK may have been Number 611, which was transferred to the west under KONA 6 in October 1944) [73] Nothing further isknown about KONA 3, which was caught by the Russians in a pocket in Kurland at the end of the war.[74]

15. Organization of KONA 4.-- KONA 4, was subordinated to the Commanding Officer Southeast (Befehlshaber Suedost), who controlled the German Armies in the Balkans.[75] The responsibility of these armies appears to have been essentially that of and occupational force; and KONA 4, therefore, added to its normal task of intercepting long range traffic emanating from the Middle East and Africa that of monitoring the traffic of the occupied Balkan countries. This circumstance may account for the fact that the organization of KONA 4 included no mobile Long Range Signal Intelligence Companies and only two mobile Close Range Signal Intelligence Platoons. The other units of KONA 4 were the Signal Intelligence Evaluation Center NAAS 4, and two Stationary Intercept Companies (Feste 5 and 6)[76]

[71] DF 9

[72] I 76 Appendix

[73] I 76 Appendix

[74] I 116 p 8

[75] IF 171 p 1

[76] IF 171

a. NAAS 4. The code name for NAAS 4 was the abbreviation HASSO, which stood for Horchauswertestelle Suedost, Intercept Evaluation Station Southeast.[77] NAAS 4 was divided into a cryptanalytic section, a direction finding section, a tactical evaluation section, and a final evaluation section.[78] The strength of NAAS 4 was about 80-100 men, including interpreters, decoders, cryptanalysts, evaluating personnel, draughtmen, drivers and switchboard operators.[79]

b. Feste 5. Feste 5 was the former Army Fixed Intercept Station at Graz. It had the following sections:

1) headquarters
2) radio intercept section
3) radio operation and maintenance section, operating a radio transmitter
4) decoding and cryptanalytic section
5) evaluation section for direction finding.

Feste 5 had a strength of 150-170 men and operated fifty radio intercept sets. Its personnel was composed of radio intercept operators, code clerks, cryptanalysts, interpreters, drivers, radio operators, typists, and switchboard operators.[80]

c. Feste 6. Feste 6 was the former Army Fixed Intercept Station at Tulln. It had the same subordinate sections as Feste 5, with a strength of about 130 men:[81]

1) headquarters
2) radio intercept section
3) radio operations and maintenance section, operating a radio transmitter
4) decoding and cryptanalytic section
5) evaluation section for direction finding

[77] IF 171 p 1

[78] IF 171 p 2

[79] IF 171 p 2

[80] IF 171 p 3

[81] IF 171 p 3

d. NAZ T. The Close Range Signal Intelligence Platoon, NAZ T, consisted of about forty-two men; among these were Turkish decoders who also acted as interpreters. Its organization was as follows:[82]

1) platoon headquarters
2) radio intercept station with 10 sets
3) radio operation and maintenance section
4) direction finding platoon
5) decoding section for Turkish only
6) final evaluation section for direction finding

e. NAZ W. The signal intelligence platoon, NAZ W, consisted of about eighty men who specialized in monitoring internal Balkan radio traffic. Its organization was as follows:[83]

1) platoon headquarters
2) radio intercept station
3) radio operation and maintenance section
4) direction finding platoon
5) decoding section
6) final evaluation section

f. Radio Control Station. The Radio Control Station (Rundfunkueberwachungstelle) which had been part of the organization of KONA 4 was dissolved in 1942. [84]

16. Organization of KONA 5.--

a. Organization through 1944. KONA 5 was the only Signal Intelligence Regiment on the western front until the establishment of KONA 7 in February 1943. It remained throughout the war preeminent on this front.

[82] IF 171 p 3

[83] IF 171 p 3

[84] IF 171 p 3

Before February 1944, the organization KONA 5 consisted of a Signal Intelligence Evaluation Center, NAAS 5, four Stationary Intercept Companies, Feste 2, 3, 9, and 12; and two Long Range Signal Intelligence Companies, FAK 613 and 624.[85]

Some time after February 1944, the organization of KONA 5 was changed.[86] The reorganization of KONA 5 parallels changes in the German order of battle which took place on the western front in early 1944. Prior to this time the western armies had been under the command of Army Group D, to which KONA 5 was attached as the Signal Intelligence Regiment of the West. In early 1944, however, Army Group D was absorbed into the Commander-in-Chief West (Oberbefehlshaber West), who took control of three newly formed Army Groups on the western front, Army Groups B, H, and G. KONA 5 therefore modeled its organization so that it controlled three Signal Intelligence Battalions, NAA 12, 13, and 14. Each battalion was attached to a separate Army Group: NAA 12 to Army Group D, NAA 13 to Army Group B, and NAA 14 to Army Group G.[87]

In regard to the subordination of the six component parts of KONA 5 to the three Signal Intelligence Battalions, there is disagreement between a Combined Services Detailed Interrogation Centre publication[88] and a TICOM interrogation report.[89-90]

[85] IF 127

[86] IF 127 p 2

[87] I 76 Appendix

[88] IF 127

[89] I 76

[90] The CSDIC report describing the grouping of the six component parts indicate that FAK 624 combined with signal intelligence platoon 12 to form NAA 12; Feste 2 and 12 combined to form NAA 13; Feste 613 combined with a short range intercept company, NAK 965, to form NAA 14. Feste 3 and 9 were left as independent units administered by the Kommandeur.

Chart 4-3 shows the distribution of the six elements according to the TICOM report. Feste 12 combined with Feste 3 to form NAA 12; Feste 2 and 9 combined with FAK 613 to form NAA 13. There is no indication whether FAK 624 combined with other companies when it formed NAA 14.

b. After 1944. The organization of KONA 5 as outlined above remained constant throughout most of 1944. In late 1944, however, an attempt was made to centralize and to strengthen the western field organization. Accordingly, a senior Commander of Signal Intelligence (Hoeherer Kommandeur der Nachrichten Aufklaerung, abbreviated Hoeh Kdr d NA) was established. This Senior Commander, Col. Kopp, was attached to the Commander-in-Chief West (Oberbefehlshaber West) and was made responsible for all signal intelligence activities in the west. [91] The strengthening of the western field signal intelligence was effected by moving KONA 6 from the eastern front to the western front to join KONA 5. Both KONAs were subordinated to the Senior Commander: KONA 5 was assigned to Army Group D, which controlled the German armies on the southern end of the western front; and KONA 6 was attached to Army Group B, which controlled the German armies on the northern end of the western front.[92]

With the move of KONA 6 to the west, the organization of KONA 5 was modified. The Signal Intelligence Battalions of KONA 5 were reduced to two, NAA 12 and NAA 14. NAA 13, which had been composed of two Stationary Intercept Companies (Feste 2 and 9) and one Long Range Signal Intelligence Company (FAK 613), was taken from KONA 5, broken up, and its components reassigned. Feste 2 was placed under the direct supervision of the Hoeh Kdr d NA; Feste 9 was shifted from Norway to Italy, where it fell under KONA 7; and NAA 13 with FAK 613 was assigned to KONA 6. KONA 5 was compensated for the loss of FAK 613 by the addition of FAK 626, which was taken from one of the eastern KONA (perhaps KONA 8) and brought to the western front.[93]

[91] IF 123 p 6

[92] I 76 Appendix

[93] I 76; IF 127

c. Organization of component parts: The organization of KONA 5, therefore, in the spring of 1945 was, as Chart 4-3 indicates: one evaluation center (NAAS 5) with two battalions (NAA 12 and 14); subordinated to NAA 12, one Stationary Intercept Company (Feste 12), and one Long Range Signal Intelligence Company (FAK 624); subordinated to NAA 14, one Signal Intelligence Company (FAK 626). This was the organization of KONA 5 until the capitulation.

1) NAAS 5. NAAS 5, the Signal Intelligence Evaluation Center of KONA 5, was located near Paris at St. Germaine-en-Laye. The strength of the organization was about 150 men, consisting of interpreters, cryptanalysts, evaluators, draughtsmen, switchboard operators, drivers, etc. In addition, some women auxiliaries were available, particularly for switchboard work. The internal organization of NAAS 5 is not known.[94]

2) Feste 12. Feste 12 was the Stationary Intercept Company which was subordinated to NAAS 5 until early 1944, when it joined with Feste 3 to form NAA 12.

The organization of Feste 12 consisted of a radio intercept platoon, and a telephone communications unit. When it was attached to NAAS 5, Feste 12 had no cryptanalytic or evaluation personnel since this work was being done at NAAS 5, it is probable that this type of personnel was added. The strength of Feste 12 was estimated at 120 men and 30 women auxiliaries.[95]

3) Feste 2. According to a prisoner's account,[96] the organization of Feste 2, the former Army intercept station at Muenster, closely approximated that of Feste 3. It had a radio intercept platoon, a direction finding platoon, and an evaluation platoon consisting of two sections: one for the evaluation of content of messages (Inhaltsauswertung) and one for the evaluation of traffic. (Verkehrsauswertung).

[94] IF 127 p 2

[95] IF 127 p 4

[96] IF 127 p 4

In 1944, Feste 2 combined with Feste 9 and FAK 613 to form NAA 13. When NAA 13 was broken up in November 1944, Feste 2 was subordinated directly to the Senior Commander of Signal Intelligence in the West.

4) Feste 3. Feste 3 was the original Army intercept station at Euskirchen. Early in the war it had been subordinated to KONA 5. At first administered independently, in 1944 it combined with Feste 12 to form NAA 12. When KONA 5 was reorganized in the fall of 1944, Feste 3 was combined with the Long Range Signal Intelligence Company, FAK 626, which had been brought from the eastern front to form NAA 14. This organization was valid until the end of the war.[97]

The internal organization of Feste 3 is described by a liaison officer, Lt. Hans Lehwald, attached to it as consisting of a radio reception platoon of approximately 70 receivers, and an evaluation platoon of 25-30 men. The evaluation platoon was broken down into sections for traffic analysis, cryptanalysis, evaluation, direction finding, and filing section for diagrams of the nets, call signs, personalities, code names, and direction finding results.[98]

5) Feste 9. Feste 9 was a Stationary Intercept Company formed in Frankfurt/Main in the spring of 1942 and sent to Norway in July of that year. It was first stationed at Trondhiem, later at Bergen, and in the spring of 1944 at Ski near Oslo. (Between the summer of 1944 and the following winter, most of the personnel were moved to Italy; by Christmas of 1944, there was nothing left of the unit in Norway.)[99]

[97] IF 127 p 3

[98] I 76 p 2

[99] IF 120 p 6

While in Norway Feste 9 was organized along the lines of a Long Range Signal Intelligence Company, with a headquarters platoon, an intercept platoon of 80-120 men, a direction finding, a radio platoon of about 20 men, and an evaluation section of about 30 men. The evaluation section had one subsection for the evaluation of message contents, one for traffic, and one for cryptanalysis.[100]

When in Norway, Feste 9 was subordinated to KONA 5. It can be surmised, however, that its connection with KONA 5 was always more flexible than that of the other units because of its geographical position in Norway. When NAA 13 was broken up, Feste 5 remained under the supervision of KONA 5 until, it was shifted to Italy under KONA 7.[101]

6) FAK 624. FAK 624 was formed at Montpellier on 16 April 1943 and attached to KONA 5.[102] In February 1944, FAK 624 was subordinated to NAA 14 of KONA 5, and in late fall of that year it combined with Feste 3 to form the reorganized NAA 14.[103]

The company was composed of an intercept platoon with an advanced listening post, a communications platoon, and an evaluation platoon. For transport, FAK 624 is said to have had approximately 85 vehicles with six special French radio trucks and trailers with direction finding equipment. The strength of the company was approximately 250 men including interpreters, code clerks, cryptanalysts, radio intercept operators and ninety drivers.[104]

[100] IF 120 p 6

[101] IF 144 p 2

[102] IF 127 p 3

[103] I 76 Appendix

[104] IF 127 p 3

7) FAK 613. FAK 613 belonged to KONA 5, in so far as is known, from its inception. In February 1944, FAK 613 combined with Feste 2 and 9 to form NAA 13. When this battalion was broken up in late 1944, FAK 613 was reassigned to KONA 6, with which it remained until the end of the war.[105]

Very little is known of the organization of FAK 613; according to IF 127, its organization paralleled that of FAK 624.[106]

8) FAK 626. FAK 626 was established in August 1943, trained until January 1944 and formally activated at that time at Winniza. It was subordinated to one of the eastern KONA (perhaps KONA 8) and was stationed in the Ukraine area. In October 1944, FAK 626 was sent to Landau where it was schooled in western traffic and reorganized. In November 1944, it met FAK 624 at Landau; and both units were sent west to KONA 5 with which they remained until the end of the war.[107]

The original strength of FAK 626 on the Russian front is said to have been 250-300 men of whom 80-100 were intercept operators, 10-15 direction finding operators, 10-15 cryptanalysts, 5-7 translators, 10 traffic analysts. The unit, however, was greatly under strength on the western front.[108]

17. Organization of KONA 6.-- KONA 6 was activated as an eastern KONA at Frankfurt/Main in 1941 and stationed in the Crimea to [109] work in the Caucasian campaign.[110] After that campaign, its assignment was the interception of Russian partisan traffic.[111] This remained its task until the KONA was detached in early 1944 and reassigned to work on the western front.[112]

[105] I 76 Appendix

[106] IF 127 p 4

[107] I 76 p 3

[108] I 76 p 4

[109] IF 195

[110] DF 18 p 81

[111] DF 18 p 81

[112] I 76 Appendix

There is no statement in TICOM documents about the organization of KONA 6 while it was in the east. The organization after it was assigned to the west, however, is clear from I 76 Appendix. As a western KONA, KONA 6 had two Signal Intelligence Battalions: NAA 9 and NAA 13. NAA 9 had been brought from the east in November 1944. Subordinated to it were the Close Range Signal Intelligence Company, NAK 956, which was established in October 1944, and the Long Range Signal Intelligence Company, FAK 611, which had been brought from the east at that time. NAA 13, it will be recalled, had been given to KONA 6 by KONA 5 with the Long Range Signal Intelligence Company, FAK 613. Subordinated to NAA 13 were also FAK 610, which had been brought from the east in November, 1944; and NAK 953, which had been brought from the east in October, 1944.[113]

a. FAK 613. FAK 613 was given by KONA 5 to KONA 6 in late 1944. As has been stated under the material on KONA 5, nothing is known of the organization of FAK 613. It was probably parallel to that of other Long Range Signal Intelligence Companies such as FAK 624.[114]

b. FAK 611. FAK 611 was active on the eastern front during the Russian campaign from June 1941. It was also stationed in Poland, where it was attached to Army Group Center.[115] In November 1944, FAK 611 was moved to the western front and subordinated to KONA 6, NAA 9.[116]

Nothing is known of the size of FAK 611 on the eastern front. On the western front it was small enough to occupy a house in Zutphen, Holland, near the Vandyk church, and consisted of 30-40 radio and radio telephone operators, 10 decoders and cryptanalysts, and 25 evaluators.[117]

[113] I 76 Appendix

[114] IF 127 p 4

[115] I 55 p 4

[116] I 76 Appendix

[117] I 74 p 2

c. FAK 610. FAK 610 was activated in 1940 for operations on the eastern front.[118] Subordinated to KONA 2, it worked at Tilsit in September 1940 and later settled at Volkhov, where it intercepted Russian traffic. In November 1944 it was transferred to the western front. Nothing is known of FAK 610 on the western front except that it was subordinated to NAA 13 of KONA 6.[119]

18. Organization of KONA 7.-- KONA 7 was established in February 1943 as the Signal Intelligence Regiment subordinated to the Commander-in-Chief South (Oberbefehlshaber Sued) who controlled the German Armies in Italy. In 1944, the component parts of KONA 7 were: [120]

Headquarters unit
1 Signal Intelligence Evaluation Center, NAA 7, with covername Krimhilde
2 Stationary Intercept Companies, Feste 1 and 9, with covernames Monika and Astrid
1 Long Range Signal Intelligence Company, FAK 621, with covername Erika

a. NAAS 7. NAAS 7 was organized into sections for cryptography, cryptanalysis, and evaluation. The evaluation sections included immediate, tactical, Direction Finding, traffic, content, and final evaluation. The strength of the evaluation center was about 150 men.[121]

b. Feste 1. Feste 1, the former Army intercept station at Stuttgart, which had been stationed at Strasbourg in 1940, Brittany in 1941, and later that year at Montpellier, moved to Italy and was attached to KONA 7 in 1943.[122]

The main task of Feste 1, was interception. No evaluation was done by the personnel who consisted of radio intercept operators, telegraph and telephone operators, and direction finding operators.[123]

[118] I 62 p 3

[119] I 76 Appendix

[120] IF 172

[121] IF 172 p 2

[122] IF 172 p 2

[123] IF 172

c. Feste 9. The origin and organization of Feste 9 has been described under KONA 5.

d. FAK 621. FAK 621 was organized in 1942 from the former intercept (Horch) company 3 (H) NA 56.[124] Its original commander was Seebohm, who was captured with most of FAK 621 in the African campaign on 10 July, 1942. The remnants of this company continued to work on Allied systems under Captain Habel until May 1943, when the Allies completed the capture of the unit at Tunisia.[125] Nothing is known of the organization of the company and interrogations of the prisoners are not available for this report.

19. Organization of KONA 8.-- KONA 8, which was formed in October 1944 and assigned to the Eastern front, Army Group South, had one Signal Intelligence Evaluation Center, NAAS 8; two Signal Intelligence Battalions, NAA 1 and 2;[126] one Long Range Signal Intelligence Company, FAK 620; one Close Range Signal Intelligence Company whose identity is unknown; and one Stationary Intercept Company (either 4 or 8). It is known that Feste 8 attempted in the winter of 1942-3 to intercept Russian radio telephone traffic at Koenigsberg; but it is not certain to what eastern KONA this Feste was assigned.[127] FAK 620 had monitored western traffic on the Norderney Island from August 1939 until it was sent to the eastern front and subordinated to KONA 8.[128] Nothing more is known of the units.

[124] IF 126 p 10 See I 55 p 4 for a list of the seven intercept companies (Horchkompanie) in the German Army.

[125] I 78 p 9

[126] I 76 Appendix

[127] IF 123 p 3

[128] I 76 p 3

20. Organization of KONA Nord.-- KONA Nord was organized in February 1945 to serve Army Group North when KONA 2, which had been attached to that group, was transferred to Army Group Weichsel. From KONA 2, KONA Nord received NAAS 2, FAK 619, NAK 951 and 955, and NAZ Brutus. This organization was valid only until 28 March, when by order of General Praun, KONA Nord was ordered to return to Army Group Weichsel all its components except the two Close Range Signal Intelligence companies, NAK 951 and 955. These probably remained with KONA Nord until the capitulation.[129]

21. Organization of NAA 11.-- NAA 11 was a field unit unique in the German Army Signal Intelligence organization. Although it was assigned to the 20th Mountain Army (XX Gebirgsarmee), in matters of signal intelligence it was an independent unit subordinated directly to HLS Ost acting in all respects like a Signal Intelligence Regiment.[130]

The original core of NAA 11 was the Long Range Signal Intelligence Platoon designated North (Nachrichten Fernaufklaerungszug Nord, abbreviated FAZ Nord) which operated in Finland after 1941. On 1 March 1944, FAZ Nord was merged with the Close Range Signal Intelligence Company, NAK 961, to form NAA 11. In the fall of 1944, after Finland's capitulation, NAA 11 retreated to Norway.[131] In May 1945, when it was at Gjovik, Norway, it was ordered to turn over all documents and papers to the 20th Mountain Army and to organize a group which would incorporate the experience and knowledge of the unit.[132] The interrogations of this group which became known as the "The Norway Party" are published as I 55 and I 106.

[129] DF 9

[130] I 55 p 5

[131] I 55 p 5

[132] I 55 p 3

The major function of NAA 11 was interception, although it was also responsible for direction finding, evaluation, cryptanalysis, and communications. The division of personnel gives an estimate of the comparative importance of these functions. Of the 475 men, from 200 to 250 were assigned to intercept and operated seventy-five sets; thirty men were assigned to direction finding, forty to evaluation, twenty-five to cryptanalysis, and thirty to communications. One hundred men were needed for driving, cooking, etc.[133]

22. Feste Loekken.-- The Feste Loekken was the Stationary Intercept Company attached to the German military commander in Denmark. Nothing is known of its organization.

[133] I 55 p 8

VOLUME 4

Chapter IV: German Army Intercept Operations

23. Intercept operations, 1923-1933-- Assignment of intercept coverage from 1923-1933 was made by the Codes and Ciphers Section of the Defense Ministry, (Reichwehr-ministerium Chiffrierabteilung). The division of intercept tasks was established on a geographical basis. Munich monitored Italy (including her colonies), Yugoslavia, Greece, Turkey, Bulgaria, Rumania, Hungary, Austria, and Czechoslovakia. Stuttgart monitored France (including her colonies), Belgium, Holland, and Spain. Munster monitored England (including her colonies) and Dominions. (There is no record in TICOM sources of intercept of United States traffic before 1941. With the entry of the United States into the war, a USA section was formed within In 7 VI.) The station in Koenigsberg intercepted Russian traffic, and that at Breslau monitored Polish, Czechoslovakian (and Russian) communications. The station at Liegnitz had twice the personnel of the other stations, and its cover was directed by the Codes and Ciphers Section of the German Defense Ministry.[140]

The personnel of each intercept station consisted of one officer (chief of the station), one radio mechanic, eighteen or twenty enlisted men, and six or eight civilian employees used as clerks, interpreters, etc. In 1933,

[140] IF 181 p 2

five technicians were added to the personnel. Major Feichtner of the German Air Force, Air Signals Regiment 352 (LN Regt. 352) stated that these units had no tables of organization, their personnel being detached from signal battalions and signal platoons of the Infantry, Cavalry, etc. Not until 1932 did the Fixed Intercept Stations (Feste Horchstelle, abbreviated Feste) receive their tables of organization. The quality of the personnel of the Fixed Intercept Stations was certain to be of best because the stations received the direct support of the German Defense Ministry.[141]

The material intercepted daily was studied by the traffic analysis section of the Feste, and the results were incorporated into a daily traffic analysis report. The deciphered radio messages were then evaluated. All radio messages which could not be decoded by the intercept stations were sent daily to the Codes-Ciphers Section of the German Defense Ministry. On one occasion, when the maneuvers of one of the large foreign powers were being monitored, Feichtner stated that the head of the Sub-section dealing with the country in question was sent from the Codes and Ciphers Section to the appropriate intercept station for the duration of the maneuvers.[142]

The first real military activity was the monitoring of the Riff War in the middle 1920's (Feichtner said 1930). The deployment and operational tactics of the Spanish and French were learned in detail through the decoding of radio messages, and the German HQ was regularly serviced with reports. In recognition of the fine performance of the Munich intercept station, its chief was given leave to pursue technical studies at the expense of the state.[143]

Major Feichtner made it clear that the period prior to 1933 was one of training for the German intercept units.

24. Intercept operation, 1933-1939-- In 1933, the Army High Command (OKH) assumed general control of the

[141] IF 181 p 3

[142] IF 181 p 4

[143] IF 181 p 5

intercept organization[144] and the Intercept Control Station[145] (HLS) directed intercept coverage. A program of expansion and improvement was instituted, with establishment of three new Fixed Intercept Stations at Striegau, Hersbruck, and Chemnitz.[146] All Army intercept stations were improved. By 1934, for instance, each had its own building outside the city limits where it was free from electrical interference, and each was equipped with the latest technical improvements.[147] In 1935, the first mobile Signal Intelligence Companies were activated, for the greater part from Signal Corps recruits. Officers, non-commissioned officers, and privates from the Fixed Intercept Stations acted as instructors.[148]

At this time the Army was intercepting all Army, diplomatic, and Air Force traffic. The Army traffic was sent for analysis to the Army cryptanalytic and evaluation agency[149] the Intercept Control Station (HLS) at Berlin. Diplomatic traffic was passed either to the Codes and Ciphers Section of the German Defense Ministry or to the Foreign Office.[150] Sergeant Jering of the Signal Intelligence Agency of the Air Force High Command (OKL/LN Abt 350) noted that during this period the Army intercepted and evaluated foreign Air Force traffic but did not give it so much attention as it gave the ground force traffic.[151] The Air Force was becoming increasingly dissatisfied with the Army intercept work and in 1935 began to organize its own Signal Intelligence Service. For three years however (1935-1938), the Air Force maintained close relations with the Army. Air Force employees underwent familiarization training at Army Fixed Intercept Stations and the Air Force radio intercept stations, Wetterfunkenpfangstelle, (W-stellen) were set up according to the Army prototypes.[152] By 1939, the break between the Signal Intelligence Service of the Army High Command and that of the Air Force High Command was complete.

[144] I 78 p 2
[145] See Chapter II, Volume IV
[146] I 85 p 3
[147] IF 181 p 9
[148] IF 181 p 10
[149] I 78 p 2
[150] I 85 p 2
[151] IF 181 p 13
[152] IF 181 p 14

At this time the Supreme Command of the Armed Forces also set up its own intercept service for diplomatic traffic. The Army gave to the Armed Forces two of its intercept stations, Lauf (formerly at Hersbruck) and Treuenbrietzen, for the interception of this traffic.[153] From this period on, the Army intercept service confined itself exclusively to the interception of foreign Army traffic.

The activities of the Army intercept service from 1933 to 1939 centered around the various crises of the international situation. In 1934, at the time of the Austrian revolt, Munich was given the task of monitoring all Austrian traffic including internal communications.[154] At the same time it monitored Italians communications and through its discovery that the Italians were massing troops at the Brenner pass brought about the timely withdrawal of Germany from the affair.[155] In 1935, Munich was monitoring French traffic at the time of the occupation of the Rhineland; and, as a result of the intelligence derived German troops marched in without fear of reprisal.[156] From 1933 to 1936, the period of the Abyssinian War, intercept stations of the Army High Command monitored Italian traffic without cessation.[157] From 1936 to 1939, Munich and Stuttgart monitored the traffic of both factions in the Spanish Civil War.[158] During this period, the first mobile signal intelligence company went into the field attached to the Legion Condor. Feichtner stated that, in spite of the opposition of some of the regular Army officers to a mobile organization of this type, this company quickly assumed its role as a most important instrument of intelligence to the Legion Command.[159]

[153] I 85 p 3

[154] IF 181 p 6

[155] IF 181 p 6

[156] IF 181 pp 6-7

[157] IF 181 p 7

[158] IF 181 p 8

[159] IF 181 p 8

25. Intercept operations 1939-1944-- Before 1939, the German General Staff had placed very little emphasis upon intercept in the field. Nearly all intercept had been carried on by the Fixed Intercept Stations (Feste). With the approach of mobile warfare, however, German Army intercept operations also became mobile. The new emphasis on field intercept resulted in the establishment of Signal Intelligence Regiments (KONA) whose mobile component parts were designed to work with units of the Army from Army Group to Army Corps level. The adaptation of the Signal Intelligence Regiments to meet the needs of the Field Army is one of the chief accomplishments of the Army signal intelligence service.

a. Control of Intercept Coverage 1939-1944-- Control of intercept coverage during the war stemmed from the Intelligence Officers of the Eastern Armies Branch and the Western Armies Branch.[160] As Jodl stated, these officers were thoroughly familiar with the general signal intelligence picture.[161] The chain of command is very clear during the last year of the war. The Intelligence officers of the Eastern Armies Branch and the Western Armies Branch briefed the chief of the Understaff of OKH/GdNA, who had control over all the Signal Intelligence Regiments (KONA) and who issued to them their directives for intercept coverage.[162] In the west, the Understaff worked through the Senior Commander of Signal Intelligence (Hoeh Kdr d NA) whose function it was to coordinate the intercept coverage of KONAs 5 and 6.[163] With the other KONA, the chain of command from the Understaff was direct. The Signal Intelligence Evaluation Centers (NAAS) of the KONAs issued the directives for intercept coverage to all units subordinate to the KONA.

In 1941-1944, previous to the establishment of the GdNA, the chain of command appears to have been the following: non-Russian intercept coverage was directed by the Western Armies Branch through the Control Station of Signal Intelligence of the Army High Command (OKH/LNA);[164] Russian

[160] I 86 p 2

[161] I 143 p

[162] IF 123 p 6

[163] IF 123 p 6

[164] I 196 p 10

intercept coverage was directed by the Eastern Armies Branch through the Intercept Control Station East of the Army High Command (OKH/HLS Ost).[165]

b. Assignment of intercept-- Assignment of intercept was established on the geographical basis: eastern, southeastern, western, southwestern. From the beginning of the war eastern interception was given high priority and KONA 1, 2, 3, were assigned to eastern coverage. In 1942 KONA 6 and in 1944/45 two other KONAs, 8 and Nord were formed also for the interception of eastern traffic.[166] In addition, eastern interception was carried on by three independent Stationary Intercept Companies, Feste 7, 8, 11, and one Long Range Signal Intelligence Platoon, FAZ Nord. After 1942, new monitoring of eastern traffic was also done by the Intercept Control Station East (HLS Ost.)[167] In contrast, southeastern, western, and southwestern interception were covered by one KONA apiece, with one central monitoring agency for all three area, the Control Station for Signal Intelligence (LNA).

1. Eastern intercept.-- The mission of all eastern KONA was the interception and evaluation of Russian Army, Air Force, and Partisan (guerrilla troops) traffic. Their intercept coverage differed only in respect to the geographical origin of the traffic. KONA 1, which was attached during the period 1939-1944 to Army Group South Ukraine, covered the southern part of the Russian front. It moved in the vicinities of Lemberg, Winniza, Poltava, Reichshof, and Novy Jicin in Czechoslovakia.[168] KONA 2, which was attached to Army Group Center and covered traffic on the central Russian front, moved in the vicinity of Warsaw, Borisov, Orscha, Vitebsk, Smolensk, Minsk, and Grodno.[169] KONA 3, which was attached to Army Group North, covered

[165] IF 123 p 4

[166] I 19g p 1

[167] IF 123 p 5

[168] I 116 p 8

[169] I 116 p 8

traffic on the northern part of the Russian front and in the Baltic states. It was variously at Riga/Dueneberg, Pskov, and Kurland, where in 1945 it was caught in a pocket by the Russians and captured intact.[170] KONA 6 was formed in 1942 to cover the traffic of the campaign in Caucasus.[171] While in the east the unit was located at Rostov on the Don, Novocherkassy, and Minsk.[172] After that campaign, it was assigned to the interception of Russian Partisan traffic and kept this as its intercept coverage until November 1944, when it was withdrawn from the east and reassigned to the western front.[173]

The four independent Stationary Intercept Companies assigned to work on the eastern front had the following assignments. To Feste 11 was assigned coverage of high-frequency traffic on the Red Army and the NKVD. Originally, this Feste was located at Winniza, latterly at Kiev.[174] The other two Feste, 7 and 8, concentrated on special Russian traffic. Feste 7 was the Russian Baudot reception station at Minsk. In 1942-43 it was moved to Loetzen where it became part of Section 4 of the HLS Ost and continued to intercept Russian Baudot traffic.[175] Feste 8 was the former Army intercept station at Koenigsberg. After 1942, this station concentrated on Russian wireless telephone traffic called by the Germans Russian X-traffic. Attempts were made to pick up this traffic by equipment developed by Army Ordnance, Signal Equipment Testing Laboratory (Waffenpruefung, abbreviated Wa Pruef 7). The channels monitored ran east of Moscow; the traffic was mainly economic. From 1942 to 1944, this traffic was successfully recorded; but after 1944 the Russians scrambled their wireless telephone traffic, and after unsuccessful efforts to intercept this scrambled type had been made, the monitoring was dropped.[176]

[170] I 116 p 8

[171] DF 18 p 81

[172] I 116 p 8

[173] I 116 p 8

[174] IF 123 p 12

[175] IF 123 p 5

[176] IF 123 p 14

The Long Range Signal Intelligence Platoon, FAZ Nord, operated in Finland after 1941. The mission of this unit (which was attached to the 20th German Mountain Army) was the interception of Russian Army traffic.[177] All Russian Army systems were handled by FAZ Nord except five-figure traffic which was sent in an unprocessed state to HLS.[178]

Section 4 of HLS Ost monitored NKVD Inter-Soviet State traffic, and radio broadcasts of the Tass News Agency from Moscow.[179] (Mention has already been made, Chapter II, of the acquisition by the section of the Baudot reception station in 1942-43, when Feste 7 was moved from Minsk).

2. Southeastern intercept-- Southeastern intercept was the task of KONA 4, which was the only Signal Intelligence Regiment in the Balkans during the war. For the task of intercepting traffic in this area, the component parts of the KONA were located in strategic places: NAAS 4, the Signal Intelligence Evaluation Center, was moved in the summer of 1941 to Neon Phaleron near Athens;[180] it remained there until February 1944, when it retreated to Belgrade.[181] From Belgrade it moved to Graz whence it had departed some four years before.[182] Feste 5, the former Army intercept station at Graz, was moved to Epanome, 30 km south of Salonika in the Chalcidice.[183] Feste 6, the former Army intercept station at Tulln, was stationed during this period in Athens, from which it returned to Tulln in 1944.[184] The Close Range Signal Intelligence Platoon NAZ T was located at Kavalla on the Thracian Sea; NAZ W, at Belgrade.[185]

The traffic intercepted by KONA 4 and its component parts was divided into two types:

a) long range traffic emanating from the Middle East and Africa:
b) traffic of the occupied Balkan countries.

Long range traffic of the Middle East emanated from Turkey, from the British Ninth Army in Palestine and the Tenth Army in Iraq, and from the French Armies in Syria.

[177] I 55 p 5
[178] I 55 p 9
[179] IF 123 p 5
[180] IF 171 p 2
[181] IF 171 p 2
[182] IF 171 p 3
[183] IF 171 p 3
[184] IF 171 p 3
[185] IF 171 p 3

Interception of Turkish traffic was carried on from 1941-1944 partly by the NAAS 4 at Neon Phaleron,[186] but chiefly by the close Range Signal Intelligence Platoon, NAZ T, stationed at Kavalla, whose sole mission was the interception and decoding of Turkish traffic.[187] Traffic from the British and French troops in Palestine and Syria was intercepted by NAAS 4 at Neon Phaleron.[188]

Traffic of the occupied countries was covered before 1944 mainly by NAZ W, operating from Belgrade. This platoon covered the traffic of the Croatian terrorists, the Serbian partisans, and Tito.[189] Feste 5 aided by covering Greek partisan traffic.[190] Feste 6 added Hungarian traffic to its intercept coverage in 1943 by sending a plainclothes detail to Slovakia near Pressburg, Hungary to monitor this traffic.[191] When NAAS 4 was moved to Belgrade, it concentrated on the traffic of the occupied countries and covered Yugoslav, Rumanian, Bulgarian, and Hungarian traffic.[192]

3. Western intercept.-- The traffics assigned to western intercept emanated from:

a) The British Isles;
b) USA (including Iceland and American troops in the British Isles), after the entry of the USA into the war; and
c) Spain, Portugal, Brazil.
d) Miscellaneous.

The coverage of these traffics was the task of KONA 5 which, until November 1944, was the only Signal Intelligence Regiment in the western area.

a) Traffic from the British Isles was considered the most important of the western traffics. It had been monitored intensively since August 1939, when a Long Range Signal Intelligence Company, FAK 620, was sent to the Atlantic coast near Norderney Island to monitor British

[186] IF 171 p 2
[187] IF 171 p 3
[188] IF 171 p 3
[189] IF 171 p 3
[190] IF 171 p 3
[191] IF 126 p 10
[192] I 74 p 2

Army maneuvre traffic.[193] Although FAK 620 was sent at a later date to the eastern area,[194] British traffic continued to be monitored by the following units of KONA 5 from 1939 to 1944:

1) Long Range Signal Intelligence Company, FAK 613. This unit stationed at St. Malo monitored exclusively radio traffic from the British Isles:[195]
2) Feste 2, a Stationary Intercept Company located until November 1943 at Husum in Holland, after that at Lille. This unit monitored exclusively traffic of the British Isles:[196]
3) Feste 9, formed in June 1942, at Frankfurt/Main and sent to Norway to monitor British traffic. At first the unit was stationed at Trondhjem; later, at Bergen, where it remained until the spring of 1944 when it moved to Ski near Oslo. The task of the unit was to intercept traffic originated by the British Army in Northern England, Scotland, and Faroes.[197]
4) Feste 12, a Stationary Intercept Company attached to the Evaluation Center of KONA 5 and located at Louveciennes. Until January 1944 this station monitored exclusively traffic from the British Isles.[198]

b) Traffic emanating from the United States and Iceland, and from American troops in the British Isles was monitored chiefly by Feste 3 at Euskirchen and Feste 9 at Bergen, Norway. Feste 3 concentrated on traffic from the USA.[199] After the autumn of 1943, Feste 3 had a special intercept unit for USA non-Morse radio teletype traffic, designated by the Germans as FF5 (Funk Fernschreib 5)[200] From Feste 9 in Bergen, USA traffic from Iceland was monitored. This unit watched for short wave radio traffic from London to Washington via Ireland, but without success.[201]

193 I 76 p 3
194 I 76 p 3
195 IF 127 p 5
196 IF 127 p 5
197 IF 120 p 6
198 IF 127 p 4
199 IF 127 p 3
200 I 149 p 2
201 I 78 p 10

c) The traffic of Spain, Portugal, and the Brazilian Army in Italy was monitored from 1939 to 1942 by Feste 3 at Euskirchen. In early 1943, however, the Long Range Signal Intelligence Company, FAK 624, was formed at Montpellier on the southern coast of France for the interception of this traffic.[202] In January 1944, the interception of Spanish, Portuguese, and Brazilian traffic was shared with FAK 624 by Feste 12.[203]

d) In addition to the three main commitments of the western intercept units, two other minor traffics were monitored: Swedish Army traffic, and French police traffic originating in Corsica. The Swedish Army traffic was intercepted by a subordinate unit of Feste 9 in Norway. This unit, known as out-station Halden (Aussenstelle Halden) was stationed at Halden, Norway, and was attached for administrative purposes to the Halden Police Battalion.[204] The French police traffic from Corsica was monitored by FAK at Montpellier.[205]

4. Southwestern intercept.-- Before 1943, the German Army appears to have had no signal intelligence unit in Italy. In February of that year, however, KONA 7 was established with the task of intercepting traffic from Italy and from North Africa.[206] The traffics consisted of British, American, Polish, French, and Brazilian Army traffic in Italy and North Africa.[207] So far as can be determined, there was no specific division of tasks among the various units of KONA 7: all units intercepted all Army traffic from these countries.

The most southerly location of NAAS 7, the Signal Intelligence Evaluation Center of KONA 7, was Rocca di Papa, 25 km south of Rome.[208] In September 1943, it moved into the neighborhood of Rome, establishing itself at Vallerano. Later it moved to Vicenza in northern Italy.[209] Feste 1, the former Army intercept station at Stuttgart, after sundry moves in France from 1940 to 1943 was ultimately stationed in Italy at Genzano near L'Aquila.[210] Feste 9,

[202] IF 127 p 3
[203] IF 127 p 3
[204] IF 120 p 6
[205] IF 127 p 3
[206] IF 172 p 3
[207] IF 172 p 3
[208] IF 172 p 1
[209] IF 172 p 1
[210] IF 172 p 1

which came to Italy from Norway in November 1944, was located at Breganze and remained there until shortly before the collapse.[211]

The Long Range Signal Intelligence Company, FAK 621, which was attached to KONA 7, had been originally designated as the Army Signal Company 3 (Horch Nachrichten Aufklrg. H NA 56).[212] This unit, which was particularly active in North Africa during the campaigns there, was captured (in part) in July 1942. In May 1943, the entire company was captured at Tunisia.[213] Until the time of its final capture, this unit intercepted traffic of the British, French, and American troops in North Africa and of the Egyptian Army and Camel Corps.[214]

26. Intercept service 1944-1945--

a. Intercept operations of OKH/GdNA. The years 1944-1945 saw the centralization of the German Army Signal Intelligence Service and its catastrophic dissolution in the months prior to the capitulation. As part of the movement to centralize the service, OKH/GdNA assumed responsibility for the intercept and evaluation of the following types of traffic:

1) foreign press;
2) special high grade machine ciphers;
3) wireless photography.

1. Intercept and evaluation of the foreign press was done by Section 2 of Group I, OKH/GdNA. This section was divided into four subsections:[215]

a) monitoring of eastern wireless (Rundueberwachung Ost);
b) monitoring of western wireless (Rundueberwachung West);
c) monitoring of clear text (Helldienst); and
d) evaluation.

Owing to the personnel shortage during the years 1944-1945, Section 2 was not able to cover its commitments to any

[211] IF 144 p 2

[212] IF 126 p 10

[213] I 78 p 9

[214] I 74 p 2

[215] IF 123 pp 7-8

large extent. Eastern monitoring was confined for the most part to the Moscow wireless, although in the later months a certain amount of Balkan monitoring was instituted for Turkey and Rumania. Western monitoring was confined to the BBC London Service. News monitoring was confined to the Reuter and Tass Agencies. From these sources the evaluation center collected and collated material for its reports.

2. The interception and evaluation of special high grade machine ciphers of Russia, Britain, and the USA were assigned to Group VI of OKH/GdNA which was located at Potsdam. Section 1, dealing with Russian traffic, had three subsections:[216]

1a) Interception of Inter-Soviet State traffic,
1b) Interception of Russian Baudot traffic,
1c) Interception of Russian Army traffic.

The interception of Russian Baudot traffic (called by the Russians Z-traffic) was carried on by the same personnel who had manned the Russian Baudot station at Minsk in 1942/43. In 1943, the Russian Baudot station was moved to HLS Ost at Loetzen, where it was absorbed by Section 4 of HLS Ost. When HLS Ost was absorbed by the OKH/GdNA, the Baudot station became Section 1b of the OKH/GdNA.[217]

Section 2 of Group VI was employed with the interception (2b) and the evaluation (2a) of British and American high grade machine ciphers.[218] The interception of this traffic has been carried on by Feste 3 at Euskirchen until the establishment of the OKH/GdNA, when the responsibility for interception was transferred to the central agency.[219]

The interception of wireless photography, called by the Germans Y-traffic, was carried on by a special unit of Section I of Group VI. This unit intercepted traffic from all over the world but the non-Russian channels are said not to have yielded any valuable information. Photos intercepted from internal Russian traffic, however, often contained technical diagrams and charts.[220]

[216] IF 123 p 9

[217] IF 123 p 11

[218] IF 123 p 11

[219] IF 123 p 5

[220] IF 123 p 13

b. Intercept service in the field.-- The intercept service in the field during the last year of the war maintained its geographical distribution: eastern, southeastern, western, southwestern. Paralleling the changes in the war situation, there was an increasing emphasis on western intercept and a corresponding decreasing emphasis on southeastern intercept in the war situation.

With the pressure of the Allied invasion, western intercept assumed of necessity a position of greater importance. It will be recalled that KONA 6 was reassigned at this time from eastern to western intercept and that the western Signal Intelligence Regiments, KONAs 5 and 6, were subordinated to a Senior Commander of Signal Intelligence (Hoeh Kdr d NA) who was responsible for all signal intelligence operations in the west.[221] Upon these two KONAs fell the task of intercepting the traffic of the invading Armies.

KONA 6 monitored traffic for Army Groups H and B which were stationed in the northern part of the western front; KONA 5 monitored the traffic of Army Group G which was stationed in the southern half of the western front.[222] One member of the Long Range Signal Intelligence Company, FAK 626 (Haupts), states that his unit's original mission was the interception of traffic of the First French Army and of the Seventh USA Army. Later it intercepted traffic of the USA First, Third, and Ninth Armies.

The decreasing emphasis on southeastern interception was manifested by the disbandment of KONA 4. The component parts were apparently reassigned to various fronts. Southeastern intercept and evaluation was carried on by KONA 4's successor, the newly formed Signal Intelligence Battalion, NAA 16.[223]

The situation on the eastern and southwestern fronts remained, for the most part, much as it had been in the previous year. To the eastern front were assigned two new KONAs, KONA 8 and KONA Nord;[224] and to KONA 7 in Italy,

[221] I 76 Appendices

[222] I 76 Appendices

[223] DF 9

[224] DF 9

one new intercept unit, Feste 9, which was moved to Italy from Norway.[225]

A German Army Report on the intercept situation about January, 1945 gives the following picture of the units and their coverage:[226]

Eastern Front:

Units: KONA 8 for Army Group South
KONA 1 for Army Group Center
KONA 2 for Army Group Weichsel
KONA Nord for Army Group North
KONA 3 for Army Group Kurland
NAA 11 for 20th Mountain Army

Coverage:
Russian front traffic
Radio nets of NKVD
Rumania
Roving bands in Poland and Ukraine
Espionage units in operational areas

Southeastern front:

Unit: NAA 16 for Army Group E

Coverage:
Allied troops and communications staffs in Balkans
Soviet front traffic
TITO traffic (Jugoslavian)
ELAS traffic (Greek)
Bulgarian traffic
Mihailovic traffic (Jugoslavian)

Western front:

Units: Senior Commander of Signal Intelligence
KONA 6 for Army Groups H and B
KONA 5 for Army Groups G and Oberrhein

Coverage:
English, American French front traffic
British traffic from British Isles
USA traffic from United States
French traffic from France

Southwestern front:

Unit: KONA 7

Coverage:
English, American, French front traffic
Allied traffic from western Mediterranean and North Africa
Italian bands in upper Italy

[225] DF 9

[226] DF 9

c. Disintegration of Intercept Operations-- It may be safely assumed that the constant movement of the German Armies and their intercept units during the last months of the war prevented continuous and orderly interception of enemy traffic. A brief resume of the movements of the various Signal Intelligence Regiments will illustrate the confusion of these last months.[227] KONA 1 withdrew from the eastern front into Czechoslovakia and was found by the invading forces at Novy Jicin (Neutitschein); KONA 2 retreated from the vicinity of Grodno to Ortelburg in Prussia, Danzig, Holstein, and finally the Wismar area; KONA 3 was caught by the Russians in a pocket at Kurland and captured; KONA 8 withdrew first into Rumania, then Croatia, and finally to Lenz. KONA 5 in the west withdrew from Louveciennes in mid-August, 1944 and went first to Viggingen near Metz. At the beginning of September, it moved to krofdorf near Giessen, where it stayed until March; from there it went to the Rhoen and finally to Dischingen in the Donauwoerth area.[228] Of the component parts of KONA 6 less is known. One of its units, FAK 611, moved in the spring of 1945 from Holland to Flensbrug;[229] Feste 3 moved from Euskirchen into the Black Forest.[230]

The southwestern unit, KONA 7 and its subordinates retreated into northern Italy. Concerning southeastern intercept in the last months of the war, it is known only that NAA 16 remained as the only unit in that area.[231]

The constant shiftings of the KONAs, and in the late months of the war, the disruption of internal communications between the various parts of the KONAs and between the KONAs and the GdNA had a disastrous effect on the whole problem of enemy intercept.

[227] I 116 p 8

[228] I 113 p 2

[229] I 74 p 2

[230] I 76 p 11

[231] DF 9

During the last months of the war, the internal intercept units of the GdNA were also disrupted. The units of Groups I and V moved with the other Groups of the GdNA to Erfurt and then to Bad Reichenhall.[232] The intercept unit of Group VI which had been covering high grade machine traffic at Potsdam was moved to Stuttgart and from there to Rosenheim.[233] The equipment was buried in the cellar in the surrounding neighborhood of a house, the Pioneer-Kaserne, in Rosenheim where it was later found by TICOM interrogators.[234]

[232] IF 123 p 12

[233] IF 123 p 12

[234] IF 15

VOLUME 4

Chapter V: Operations of a Typical Signal Intelligence Regiment on the Eastern Front

Section A. Introduction

27. Sources for this chapter.--The materials describing Signal Intelligence Regiment 1 (Kommandeur der Nachrichten Aufklaerung, abbreviated KONA) provided a rather complete account of that unit, and were generally more thorough than reports available for other field signal intelligence formations; therefore, KONA 1 is discussed in this chapter as a typical Signal Intelligence Regiment. This completeness resulted from the availability of a substantial portion of this unit's personnel for interrogation. The circumstances under which the remnants of KONA 1 were found are not without interest:

> "The full facts of the surrender of this unit were explained by the Commandant, Major Ernst Hertzer. The remnant of the regiment -- approximately 700 officers, enlisted men and women, first contacted American troops on 9 May 1945 in the vicinity of Tausing, where they were directed to a PW enclosure at Stift Tepl. They had destroyed almost all of their papers except those that they considered most essential for reconstruction of their records. These documents were kept in three brief cases plus one book. In the afternoon of the 9 May, while rumors circulating in the PW enclosure to the effect that the Russians were moving into the area, the contents of the three brief cases were burned. The book, however, remained in one of the vehicles but a minute search of that car failed to produce it."[240]

Three hundred and fifty prisoners were screened at a town near Pilsen between 23 May and 28 May. All operational personnel were interviewed; and of these 41 were chosen for

[240] IF 40 p 10

further questioning. A few reports were written near Pilsen, but the bulk of documents which formed the basis for later interrogations were written between 30 May and 2 June, at Oberursel, near Frankfort-am-Main, where the unit had been moved. More specific information was given and further documents written after the group was moved to Revin, in the Ardennes.[241] The material produced consisted of 31 reports,[242] supported by supplementary "Annexes" giving information on traffic analysis, organization, etc.

Interrogations of Prisoners of War from units other than KONA 1 were relied upon in this chapter to fill out the picture. The outstanding of these was the Karrenberg Party report on "Russian Radio." Corporal (Unteroffizier) Karrenberg was an "exceedingly brilliant" man with a "phenomenal memory."[243] The report was written by him and his colleagues. All were members of the Signal Intelligence Agency of the Army High Command (Oberkommando des Heeres, General der Nachrichten Aufklaerung, abbreviated OKH/GdNA).[244]

Since the Signal Intelligence Regiments were the important field units of the German Army signal intelligence service, and since information on one of these, KONA 1, was available, in this chapter an account will be given of the functions and operations of KONA 1, which may be considered typical of those of the other Signal Intelligence Regiments operating in the East. Because organization has already been treated in Volume 4, Chapter 11, organizational matters will be noted here only as some review of them appears necessary to a full understanding of the operations.

28. Successes of KONA 1.--KONA 1 operated in the southern sector of the Russian front from June 1941 until May 1945, intercepting and evaluating Russian Army, Army Air, and NKVD[245] in that traffic area. Elements of this unit appear to have succeeded in reconstructing the detailed Order of Battle of the Russian forces, and in predicting the locality and timing of the Russian offensives before they occurred.[246] Captain Roman Roessler, Chief Evaluator of KONA 1 and Commanding Officer of the Intelligence Evaluation Center (Nachrichten Aufklaerung

241 IF 40 p 4

242 I 19b

243 IF 123 p 2

244 I 173 p 1

245 NKVD is translated as "Peoples' Commissariat for internal affairs." During the war it maintained frontier troops which performed counter espionage and had many military police functions. See I 67 p 3.

246 I 19b, 1

Auswertungsstelle, abbreviated NAAS) of the regiment, pointed out that even when identification of individual formations became impossible, the KONA was still successful in picturing the overall grouping and the number of formations. He conceded that in the case of Russian Rifle Corps and Divisions, German Intelligence units had to rely on means other than signal intelligence. However, he emphasized that the overall picture afforded, by signal intelligence units of the "movements of strategic reserves, of points of main efforts, chain of command, intentions to attack," etc., were of great value to German Intelligence units.[247]

It should be emphasized that Roessler's style was rather pompous, and his estimate of KONA 1 successes may have been overenthusiastic.[248]

29. Importance of Traffic Analysis on the Eastern Front.-- In general the successes noted above were due to traffic analysis rather than to cryptanalysis. While there seems to have been great disagreement among the persons interrogated on the relative merits of these two methods, the evidence indicated that the results achieved by the careful integration of all sources available from traffic analysis appeared to outweigh those achieved through reading of the Russian low grade codes and ciphers. This situation may be accounted for by two principal factors. In the first place: although the Germans were highly successful in reading Russian low grade systems (as described in Volume 4, Chapter VI), most of the Russian high grade codes employed by the army were one-time pad systems, and consequently defied attack by the KONA cryptanalysts.

Secondly: an enormous amount of information was available "from the Russian practice in the use of indicators, call-signs, and the generally low though improving standard of Russian wireless discipline."[249]

Because of this relative importance of cryptanalysis and traffic analysis the emphasis in this chapter will be upon the procedures through which intelligence was derived from a study of the aspects of Russian radio operations. The cryptanalysis performed by the field units will be discussed in another chapter and only its organizational relationship to the operations of the components will be noted here.

The functional relationship of the units of a KONA is pictured on Chart Number 4-4. Roughly, the KONA consisted of a Signal Intelligence Evaluation center (NAAS); of companies (FAK), subordinate to it in intelligence functions, which

[247] I 19b pp 14-15
[248] I 19g pp 3-4
[249] I 19b p 1

intercepted enemy traffic and fed the traffic back to the Evaluation center; and close range companies (NAK), which intercepted enemy low level traffic, did some analysis of the simpler systems, and passed the results and intercept into the Signal Intelligence Evaluation Center. To pick up enemy traffic of higher formations, there were so-called Long Range Signal Intelligence Companies (FAK) and so-called Fixed companies (Feste). The first intercepted primarily traffic already identified; the second concentrated on networks carrying unidentified traffic. Both types of these long range companies did analysis on the traffic they intercepted, and passed the results and their traffic up to the Signal Intelligence Evaluation Center (NAAS).

VOLUME 4

Chapter V

Section B. Functions of the KONA Units

30. Introduction.--The purpose of the KONA was to supply intelligence from signal sources to the G-2's of the Army Corps, Armies, and Army Groups. A typical KONA consisted of one Regimental Evaluation center and of 5 or 6 intercept and intelligence companies. Chart Number 4-4 shows the layout of such a Signal Intelligence Regiment.

The chart gives the picture of a typical KONA as it actually operated, with its signal intelligence platoons operating near the front lines, with its companies situated back near army headquarters, and with its main regimental evaluation center in the rear at Army Group Headquarters.

Close Range Signal Intelligence platoons intercepted very low level traffic, evaluated what they could, kept the G-2 of their assigned Army Corps informed of all intelligence derived, and passed back to an evaluation platoon at company headquarters all their results and presumably their intercepts.

Long Range Signal Intelligence Companies intercepted higher level traffic; did some evaluation, the results of which were given to the G-2 of their assigned Army headquarters; and passed back evaluation reports and intercepts to the regimental Signal Intelligence Evaluation Centar (NAAS). The Stationary Intercept Companies operated in an almost identical manner, with primary emphasis on enemy unidentified traffic.

The regimental Evaluation Center (NAAS) evaluated the reports and the intercepts from all companies of the regiment and passed their results to G-2 of Army Group.

More detailed functions of the NAAS, of the companies, and of the platoons are discussed below. (The organization of these units has already been described in Volume 4, Chapter III).

31. Functions of the Signal Intelligence Evaluation Center (NAAS).[250]--The NAAS was situated close by Army Group Headquarters.[251] The functions of the NAAS included Evaluation and Traffic Analysis, Cryptanalysis, Dissemination of Intelligence, and Direction of intercept cover.

a. Evaluation and Traffic Analysis included four types of activity:[252]

(1) Evaluation, checking, and coordination of reports passed up to the NAAS by other elements of the KONA, and the synthesis of the results.

(2) Traffic Analysis (including the study of Direction Finding results) of identified traffic passed in to the NAAS by the Long Range Companies (FAK); and of NKVD and Russian Air traffic, passed in (presumably) by either the Long Range or Close Range Companies.

(3) Attempts to identify unidentified traffic passed in by the companies, chiefly by the Feste.

(4) Keeping of full files and card indexes in which all data of any possible significance was recorded.

b. Cryptanalysis in the NAAS primarily meant the solution of unknown systems, the study of developments in known systems, and work on NKVD code. The NAAS worked on Russian systems up to and including 4-figure systems. (The cryptanalytic operations are discussed in Volume 4, Chapter VI.)

c. The NAAS was responsible for the dissemination of intelligence; it passed its results to the Intelligence Officer of the Army Group to which the KONA was attached, and reported its findings to the Signal Intelligence Agency of the Army High Command (OKH/GdNA).[253]

[250] For graphic representation of the functions of the NAAS see Chart Number 4-4. It should be emphasized that this chart portrays the main functions only, and does not represent the breakdown by table of organization sections, which is given in Chapter III.

[251] I 19b p 1

[252] I 19b p 6

[253] I 19g p 7

d. The NAAS had a key position in the direction of intercept cover. It controlled the intercept coverage of all the lower elements of the KONA, following the overall coordination exercised by the OKH/GdNA.[254]

Certain items were passed, unprocessed, through the KONA to the GdNA. The main item treated thus was 5-figure (including NKVD) traffic, and NKVD traffic which fell outside of the area of the particular KONA by whose units it was intercepted.[255]

32. Functions of the Stationary Intercept Company (Feste).- The Stationary Intercept Companies (Feste) were designed to work at the next lower level to the NAAS, that of Army. The Feste were pre-war Army intercept stations; and though they retained the traditional designation implying they were "fixed" (Feste Horchstelle), they actually were semi-motorized early in the Russian campaign. Feste 10, the "stationary" company of KONA 1 operated for, and near to, Army Headquarters.[256]

Feste 10[257] consisted of five functional sections, besides the Headquarters section. An intercept platoon (whose coverage was controlled by the NAAS)[258] covered unknown traffic in the 3500-5500 kilocycle band, fixed NKVD nets assigned by the NAAS, and nets of mobile formations[259] as directed by the NAAS.[260]

An evaluation section identified and reported unknown traffic. Apparently the interception and study of unidentified traffic were the main functions of the Feste.[261]

A cryptanalytic section contributed to the interpretation of unknown traffic by the identification of keys, also translated plain-text messages, and did some solution.[262]

The Feste had a Direction Finding platoon, which carried out the requests "of the Companies." Communications between the Direction Finding sites and the Regiment were carried out by a Communications platoon. This platoon passed the results of Evaluation by telegram or teleprinter to the NAAS.[263]

[254] DF 18 p 82
[255] I 19g p 8
[256] I 19g p 6
[257] See Volume 4, Chapter III
[258] DF 18 p 82
[259] These were also partly covered by the FAK's
[260] I 19b p 3
[261] I 19b pp 3-4; pp 19-20
[262] I 19b p 4
[263] I 19b p 4

33. Functions of the Long Range Signal Intelligence Company (FAK).--The Long Range Signal Intelligence Companies were distinguishable in function from the Feste, mainly that they were concerned to a much greater degree with identified traffic. Like Feste 10 (e.g.) they were semi-motorized and were designed to operate near Army Headquarters.[264] It was planned that one should work with each army staff covering an army sector. In actuality, however, the operations of these companies (and likewise those of Feste 10) took place further and further in the rear. The crush of work would become heaviest just at a time when safety precautions demanded a withdrawal; and it was thus found more practical to undertake the work in the rear echelon areas where it would be less frequently interrupted. Fak's 617 and 623 and Feste 10 ended up by operating in the immediate vicinity of the Evaluation Center (NAAS 1).[265]

In their interception of identified traffic, the coverage of the FAK's was directed, as was that of the Feste, by the cover control section of the Evaluation Center (NAAS).[266] The traffic intercepted by the FAK was studied by it as fully as resources would permit. Plain-text messages were translated, and traffic of known codes decoded by specialists assigned to the unit. A general section was devoted to card indexes and lists. (Raw traffic which defied analysis was sent to the cryptanalytic and traffic analysis sections of the NAAS.)

34. Functions of Close Range Signal Intelligence Company (NAK).--The Close Range Company (Nahaufkleerung Kompanie, abbreviated NAK) presumably worked at Army Corps level. Its main responsibility was to pick up and work on low-level (2-figure, 3-figure, and possibly some 4-figure) traffic.[267] It should be noted that, although the Close Range Company seemed to have been designed to work at Army Corps level, in practice such a company was apparently also stationed by the "Kommandeur" of the Regiment (KONA) with each Army as well.[268]

In contrast to the Long Range Companies, which were designed to operate in full company strength, the Close Range Companies operated by platoon.[269] The operations of each company was

264 I 19g p 6
265 I 19b p 1
266 DF 18 p 82
267 I 19b p 2
268 I 19g p 1
269 I 19g p 6

divided among four platoons: Intercept (Horchzug); Direction Finding (Peilzug); Evaluation (Auswertezug); and Communications (Sendezug).[270]

As in the case of the other units, intercept coverage was directed by the NAAS.[271] Although they were army units, in at least one case the NAK apparently covered not only enemy traffic, but also enemy air-ground, and air traffic as well. A normal program of intercept called for about twenty receivers.[272] The platoon usually had two or three intercept operators, while there were generally about twelve operators who knew Russian to pick up the radio talk.[273]

The organization of Direction Finding Platoon was rather elaborate. Normally for one company there were about eight outstations, separated from each other by 5 to 10 kilometers and parallel to the front at a distance of from one to several hundred kilometers.[274] Each section had about five men.[275]

With each platoon was a small evaluation section, consisting of two or three evaluators,[276] who worked usually in a room near the intercept station.[277] Presumably their results would be passed to the Evaluation platoon of the company. Only the simplest systems were worked on at the NAK level; most of the raw traffic was passed upwards to the NAAS, which studied it cryptanalytically as well as for tactical intelligence derivable through traffic analysis. Captain Roessler considered evaluation at NAK level a "dispersal of strength,"[278] but the NAK evaluation must not be brushed aside too lightly, for these NAK's did no evaluation and did pass the results to the Corps Intelligence Officer.[279]

270 I 62 p 4. The documents relied upon for the following account are not limited to those describing KONA 1 units. The account in I 62 is based upon one man's experience with Funkhorchkompanie 610 and 520 Nahauflklaerungkompanie on the Eastern Front.

271 DF 18 p 82

272 I 62 p 4

273 I 19b p 2

274 I 62 p 4

275 I 19b p 2

276 I 19b p 2

277 I 62 p 4

278 I 19g p 2

279 I 19b p 2

VOLUME 4

Chapter V

Section C. Features of Russian Radio Communications

35. Introduction.--The components of the KONA described in the preceding section were designed to provide the most effective overall attack upon Russian radio communications. Since unidenti fied traffic formed the great percentage of German intercept in the East, the identification and interpretation of unknown traffi was one of the most important functions of the KONA.[280] Thus it is pertinent here to survey briefly some of the characteristics facilitating German identification of Russian traffic. The operating data (such as networks and call signs) and the visible properties of the message text as transmitted formed the basic subject matter with which all units in varying degrees were concerned, and provided the clues leading to identification.

The reports available did not provide sufficient evidence to build a full picture of Russian communications. Russian nets were discussed for the most part only in terms of types of traffi they passed and their call sign practices. Details on such data as frequency systems, time of communication, and so on, were lacking. The discussion which follows is therefore limited by the sources available, and concentrates upon the distinguishing features of Russian Signal operations of value to the German signal intelligence field units.

36. Some identifying characteristics of Russian networks.--Since it was frequently possible to identify a station by its place in its network structure, the first objective of German traffic analysis was, broadly speaking, the identification of

[280] I 19b p 14; I 19g p 4

networks of which any station might form a part. This process of identification was facilitated by the following characteristics of Russian network:

a. Radio teleprinter (Baudot) traffic was characteristic of the communications of the Russian General Staff to the Front Staffs (Army Group Staffs), and of that of the Front Staffs to the "Assault Armies." Russian General Staff radio teleprinter transmissions were 2-channel, as opposed to the "modulated" (i.e. probably multichannel) transmitters used from Front Staffs to Assault Armies. Also, these latter links used lower frequencies.[281] Automatic high-speed morse transmission was possible on all such higher links, but was seldom used.[282] (Three radio teleprinter links passing Air Force traffic from Moscow to higher Air Force headquarters were also identified.)[283]

b. Great radio activity was characteristic of the morse networks of Assault Armies, because of the mobility of these Armies and their lack of land lines.[284]

c. Radio silence marked Divisional and Regimental networks just preceding attacks.

d. In general, units below division used low frequencies (2,200 to 3,900 kilocycles).[285]

37. Some identifying characteristics of Russian Call Sign Practice.--Apparently the Germans put a great deal of effort into the study of Russian call signs, which were mentioned frequently throughout the reports. One reported stated that up to "July 1944 the Russian call sign system was well known to the Germans and predictions reliable. The 1944 summer offensives, however, brought a change of system."[286] In spite of the seemingly general Russian practice of enciphering their station call signs,[287] the Germans do appear to have had considerable success in their study

[281] I 168 p 2; I 272 pp 5-7
[282] I 173 p 6
[283] I 173 p 11
[284] I 173 pp 8-10
[285] I 75 p 4
[286] I 75 p 7
[287] I 168 pp 3-4; I 173 p 21

of them as characteristics aiding in traffic identification. The prisoner quoted above stated that by the end of the hostilities the Germans had made good progress in solving the systems.[288]

Two reports indicated that most Army, Air Force, and NKVD call signs down to division level consisted, in their transmitted form, of three-figure calls, of which the first two figures were Roman letters with the third either a letter or a number.[289] Regimental networks could be distinguished from Army, Air Force, and NKVD networks, because, although they used three-figure calls, these were composed entirely of letters of the Russian alphabet.[290] Moreover, the calls of stations on the regimental networks were "usually composed of three letters of the cover name; they were either three consecutive letters or three consonants of the cover name."[291]

One Prisoner of War stated that, provided the formations took their call signs from a "Basic Book for Allotment of Call Signs (Hauptverteiler), it was possible to identify with considerable certainty Army or Air units as belonging on certain fronts.[292]

Call signs of a few higher NKVD networks, of the network of the "Artillery Reserve of the Supreme Command," and of the traffic passed on the networks of the Air Force ground stations were distinctive in that they used four-element calls.[293] One prisoner stated that the NKVD calls were mostly pronounceable,[294] and another witness went so far as to declare that the "only means of establishing the central NKVD authority" was the study of call sign usage.[295] The same reporter was of the opinion that Partisan traffic could be identified with certainty because of the consistent practice of using one call sign only.[296]

38. Some identifying characteristics of procedure.--NKVD traffic could be spotted with a high degree of probability because of the transmittal of "NK" to separate the preamble from the address(or text),[297] and because of the practice of tuning by sending a series of dots and dashes instead of by keying "v" as in other Russian traffic.[298] The absence in NKVD Administrative traffic of the group separation sign "r," common in Army

[288] I 75 p 7
[289] I 168 pp 3-4; I 173 p 21
[290] I 173 p 21
[291] I 173 p 11
[292] I 19b p 36
[293] I 173 p 11 and p 21
[294] I 19b p 48
[295] I 19b p 36
[296] I 19b p 36
[297] I 168 p 2
[298] I 19b p 47

traffic, was a clue aiding identification.[299] The appearance of SMERSCH in the preamble characterized NKVD messages sometimes picked up on Army or Air nets which might be used by the Counter Espionage organization OKR SMERSCH.[300]

The appearance of "WZD" (air raid warning signal) in the preamble characterized Russian Air Force traffic. The use of "QCO" rather than "QTC" in the preamble also was some (though by no means the exclusive) indication that the traffic was Air Force,

Partisan procedure was characterized by its use of the international abbreviations of amateur radio, such as the use of "CK" for the group count. Furthermore, most of the traffic was sent blind.[301]

Army traffic could to some degree be characterized by the absence of the features noted above.[302]

30. Some Identifying Characteristics of Russian Message Text as Transmitted.--The message texts (cipher texts) transmitted by the various formations had recognizable features. Generally, high level traffic was sent in 5-figure groups while low level traffic tended to be sent in groups of 2, 3, and 4 figures. For instance, the traffic passed on the operational networks of the General Staff, the Front Staffs, and the Armies tended to be predominantly 5-figure.[303] One witness made the generalization that 4-figure systems were used "from corps to army and from army to army group."[304] The traffic passed from Division downwards tended to be 2- or 3-figure.[305]

The significance of the characteristics of 5-figure traffic in traffic identification was emphasized in one of the reports. Two of these characteristics, the "blocknot" indicator and the "Chi-number," were of particular importance.

According to one witness, a "Blocknot" consisted of fifty sheets of 5-figure random additive, 100 additive groups to a sheet. No sheet was used more than once; thus the blocknots were in effect one-time pads. Fifty of these additive sheets, numbered 1 to 50, were issued in a sealed envelope, which bore a 5-figure number. The additive sheets in any "pad" were always

[299] I 173 p 12

[300] I 19b p 48

[301] I 19b p 36

[302] I 19b pp 36-37

[303] I 173 pp 608

[304] I 191 p 8

[305] I 173 pp 10-11

designated by the same block number. The 5-figure group designating the block number was always transmitted within the first ten groups of the message. A further 5-figure group, usually in the first seven groups but always following the clock number contained, "as the last two figures, the number of the (additive) sheet (1 to 50) used. The middle figure of this group indicated the formation level, e.g. '6' might be Corps forward to Division, '5' might be Div to Div."[306] By a daily recording of all blocknot numbers, traffic enciphered in the same blocks could be segregated and identified as being transmitted by the same unit.

Another characteristic of this 5-figure traffic, actually a "message external" feature, was the serial numbering of all messages. Every 5-figure message was assigned a 5-figure serial number. This was called the Chi-number by the Germans. These Chi-numbers began at 00001 on 1 January and ran serially throughout the year. The number was sent always as the last group of the message.[307] "Newcomers of formations would start at 000001."[308] A study of the Chi-numbers assisted materially in traffic identification. Generally, a Corps sent ten messages a day, an Army twenty to thirty, and a "front" (roughly, Army Group) from sixty to one hundred. Since each message was serially numbered with a Chi-number, the progression of these numbers could be charted on a graph, and it was possible after a short time to determine the type of formation sending out the traffic from the individual curves on this graph.[309] The importance the Germans attributed to the Chi-number was great; in fact, one non-commissioned officer who recorded the time-of-origin as a Chi-number, was threatened with court-martial.[310]

The absence of blocknot and Chi-numbers distinguished 5-figure Russian Partisan traffic from 5-figure Army traffic.[311]

NKVD messages consisted of 4 or 5 figures was said to "be easily distinguished by their characteristics from Army and Air Force messages." This was probably due to the features of NKVD traffic reported as follows:

> "The first group is a discriminant which in most cases remains constant for one line of traffic. The

306 U 75 p 12
307 I 19b p 17
308 I 75 p 12
309 I 19b p 17
310 I 19g p 3
311 I 19b p 37

> penultimate group contains the date and a number representing the number of groups in the message less a variable number according to the number of indicator groups used. .....Exceptions to these rules are very rare. Two and three-figure messages usually contained technical 'wireless chat.'"[312]

Messages of the NKVD Frontier Troops were of both 4- and 5-figure types, and in regimental networks 2-figure codes appeared as well.[313] The 2-figure NKVD messages could usually be recognized as such because of the practice, in contrast to that of the army, of enciphering the same system for months. Moreover, 3- and 4-figure codes rarely changed in NKVD traffic; and once their characteristics had been ascertained, they were also fairly easily recognizable.[314]

On the whole a good deal of carelessness prevailed in the encoding of NKVD messages, at least in those appearing on the Frontier Troop networks.[315] Such a lack of security on the part of the Russians facilitated the work of the KONA's.

Air Force traffic, which might be picked up on search by the KONA units, could be distinguished from Army traffic by several external characteristics. For instance, meteorological messages usually carried an "X" or some other padding letter between the numerals. Special Air Force expressions often appeared in 2, 3, and 4-figure messages with an admixture of plain language. In plain language messages there were mentions of take-offs, and permission to land or to take-off. Such messages appeared frequently, and once picked up enabled the immediate spotting of the network as Air Force. "In general, very many more plain language messages were passed over air force networks than over army networks."[316] Air reconnaissance reports, for example, were sent mainly in the clear.[317]

[312] I 19b p 47

[313] I 173 p 13

[314] I 167 pp 5-6

[315] I 173 p 13

[316] I 173 p 11

[317] I 19b p 37

VOLUME 4

Chapter V

Section D. Direction Finding and Radio "Finger-Printing"

40. Direction Finding.--Direction finding was of the greatest importance in Signal Intelligence activities, and its importance increased as Russian radio discipline and code and cipher security were improved.[318] "A relatively large number of direction finding personnel was employed by the KONA, e.g., five with each forward platoon, 50 (as against 84 intercept operators) with Feste 10."[319]

The NAAS evaluation section was fed by the Direction Finding sections from both the FAK and the NAK. The FAK's sent requests not only to the long range but to the close range direction finding sites. FAK 617, for example, sent its orders both to three or four long-range direction find sites and to about twelve close range ones.[320]

Long-range direction finding sets were located 200-350 kilometers behind the front line. Two to three direction finding sets at one spot constituted a direction finding group.[321] The supervisor worked in the company intercept rooms, and sent requests to the direction finding operators over a command transmitter. Through this means simultaneous fixes could be taken by two, and frequently by three sites.[322]

The Close Range sets were located with the NAK platoons. The sets received requests not only from the Long Range Companies but also from the Close Range headquarters.[323]

> "The distance from company headquarters to the nearest outstation was generally twenty to thirty

[318] I 19b p 38
[319] I 19g p 5
[320] I 19b p 38
[321] I 19b p 2
[322] I 173 p 34
[323] I 19b p 2

> kilometers. Each station was completely mobile, and moved with the sectors of heavy fighting. Wire communication was occasionally available, but for the most part W/T /wireless/ communication was employed between outstations and headquarters. There was no communication between outstations. Bearings were requested by and at the discretion of, the duty officer at the intercept station. The outstations, listening on a common frequency, were advised of active enemy frequencies by means of messages sent in simple substitution cipher. Bearings were then returned, enciphered by a daily additive. Thirty to sixty seconds were required to notify all outstations of bearings required."[324]

While generally Long Range direction finding operations could fix a station within fifteen kilometers, Close Range platoon direction-finding operations could narrow the possibility to two or three kilometers.[325]

The results were screened at company level, and the good bearings were selected, with all relevant information, and reported back to the NAAS, which passed final judgment on them.[326]

41. "Radio Finger-Printing."--To enable the identification of particular radio stations, a Corporal Arno-Graul working in the NAAS constructed an apparatus designed to "radio fingerprint" the Russian transmitters through a study of oscillograms. The method was

> "to register the incoming telegraphic traffic in the form of an image on a cathode ray tube and analyze the image. Analysis consists of a number of steps, so that all details and peculiarities of the transmitter are comprised. The apparatus is attached to a normal intercept set. The individual characteristics of the transmitter can be recorded graphically by means of tracings, or in the form of photostats, in a card index."[327]

Attempts to study the characteristics of particular radio operators, by the peculiarities of their sending habits, were evidently not undertaken by KONA 1 in any formal manner.

[324] I 62 p 4
[325] I 19b p 38
[326] I 19b p 38
[327] I 19b p 39

VOLUME 4

Chapter V

Section E. Some Aspects of Evaluation and Cryptanalysis in the KONA

42. Evaluation in the NAAS.--The main duty of the NAAS was to evaluate the enemy traffic intercepted and passed to it by the Long Range and Close Range Signal Intelligence Companies.

Captain Roessler, Chief Evaluator of KONA 1, and Commanding Officer of the NAAS, observed that "there were no prescribed rules for evaluation, and this fact...made the success or failure of the signal intelligence service a personal matter depending on the perspicacity and experience of a few specialists and persons operating in key positions."[328]

Evaluation in the NAAS was concerned with "the observation and interpretation of known (radio) nets," the study of unidentified traffic, and the results of cryptanalysis. Roessler emphasized that in the case of KONA 1, "the interpretation of unknown traffic was...from a long term intelligence point of view, the chief evaluation problem."[329]

Comprehensive research work was necessary to systematize the evidence available, and the basic instruments of this systematization were the Card Indexes. The Card Indexes were exhaustive in detail, thorough and methodical. The Germans believed that the tiniest detail, though utterly lacking in any apparent significance at the moment of interception, might form part of a significant picture when scrutinized in context with similar details. Thus the minutest phenomenon, irrespective of its momentary irrelevance was recorded.[330]

328 I 19b p 13

329 I 19b p 14

330 I 19b p 13; I 19g p 3

A special section in NAAS 1 kept up to date all card indexes.[331] These will be described below.

a. Personality Index. This index listed all officers and radio operators whose names were derived not only from radio but from all sources (interrogations, captured documents, etc.). All names were treated with caution because of the Russian propensity for using cover names. There was a special file for indexing these.

b. Unit Index. This file contained all information available from all sources on all Russian units. Each card was designed to list the following items: unit, commanding officer, chief of staff, components to which the unit was subordinate, subordinate units comprising the unit in question, location, date of first appearance, and sources of information.

c. Blocknot Index. Both Blocknots and Chi-numbers were contained in the same index. A careful recording and study of blocknots provided positive clues in the identification and the tracking of formations using 5-figure codes. This index was subdivided into two files: one, the search card index, contained all Blocknots and Chi-numbers whether or not they were known; the other, the unit card index, contained only known Block-and Chi-numbers. Inspector Berger observed that the two files formed "The most important and surest" instrument for identifying Russian radio nets known to him.[332]

d. Key (Schluessel) Index. This index contained all solved keys, irrespective of the areas in which they were used. They were arranged according to the German designation of the Russian keys. "The German system of key designation includes a self-evident description of the code plus an allotted number; e.g., R4ZC 1800: russischer 4-Zahlen Code 1800 /Russian 4-figure code 1800/."[333] The 2 and 3-figure keys especially were

331 The information on the Card Index down to but not including sub-paragraph h, follows very closely the detailed report made by Inspector Georg Berger, in charge of documents in KONA 1. This report is No. 8, I 19b pp 16-18.

332 I 19b p 16

333 I 19g p 10

"peculiar to definite formations," and thus certain inferences about the formation in question could sometimes be made on the basis of the key alone.[334]

e. Call Sign Index. All call signs picked up on the entire Eastern front, known or unknown, were listed in this index, which showed not only the call sign, but also the connection in which it previously might have appeared.[335] The index was fully cross-referenced and was relied upon not only for spot identification but for building new call sign blocks.[336]

f. Cover Name Index. The Russians used cover names abundantly, not only for units, but for "common military expressions and tactical measures as well." Some were so consistently used that all disguise was lost, and they became accepted "expressions." On the whole they presented no great difficulty and could usually be interpreted successfully.[337] All cover names obtained were scrupulously recorded by the Index Section. In many cases nearly complete cover tables were reconstructed for the various Russian fronts.[338]

g. Coordinates Index. The map coordinates derived by solution of Russian map reference systems were recorded in this index, the coordinates being arranged both by the system and by the unit making use of the system.[339] It is significant that, even though the coordinate system might not be understood, the method itself might be enough to furnish important clues facilitating the tracking of a particular formation.[340]

h. Direction Finding Bearings. This file consisted of a listing of the various bearings on each Russian radio station obtained through direction finding, and helped the NAAS to estimate the value and significance of the bearings.[341]

i. Air Traffic Index. Russian Air Traffic was frequently picked up by operators assigned to search missions. In order to spot this intercept as Air traffic, a cataloguing of its

[334] I 19b p 17
[335] I 19b p 17
[336] I 19b p 36
[337] I 173 p 25
[338] I 19b p 18
[339] I 19b p 18
[340] I 19g p 10
[341] I 19b p 38

characteristics was necessary; and to accomplish this a special index was set up in the NAAS. In this index were recorded not only the statistics derived from German Army interception of Air traffic, but also data supplied by units of the German Air Force (2nd and 3rd battalions of Air Signal Regiment 353, operating with Local Air Forces 4 and 6 respectively). The statistics gathered were passed on to the Long Range Signal Intelligence Companies (FAK), which were likely to pick up Air traffic. The companies did not have separate air data indexes, but kept the data in the Army card index.[342]

It should be pointed out that in order to insure the most comprehensive indexes possible, liaison was maintained laterally between the NAAS of KONA 1 and the other regiments on the Eastern front. Full collaboration was effected also with OKH/GdNA. A system for exchanging current information, new interpretations, corrections, etc., operated smoothly, the data being passed by telegraph or courier depending upon the urgency of the item in question.[343]

Below the level of the NAAS, card indexes were extensively used; but they were naturally less comprehensive, being only as complete as the company cover assignment permitted.[344] Of the card index in general, Roessler made a significant (and characteristic) observation, emphasizing that while "the card indexes formed the indispensable material basis for evaluation, memory, experience, and perspicacity of the individual evaluators lent the spark."[345]

43. Evaluation in a Feste.--Evaluation in the Feste was a matter of identifying and interpreting unknown traffic, the interception of which was its particular function.[346] Some characteristics of Russian communications facilitating identification have been discussed in the preceding section. The systematization of this work as carried on by the Feste Evaluation Section showed how the identifying elements were studied at this level.

The first task of the Traffic Evaluation Section[347] was to work up the information into a network diagram, which not only

[342] I 19b p 52

[343] I 19b p 16

[344] I 19g p 10

[345] I 19b p 13

[346] I 19b p 4

[347] The data on Traffic Evaluation in the Feste follows closely Report No. 9 I 19b pp 19-20.

represented the net structure but listed all pertinent information and formed the basic medium studied. The diagram contained:

a. The net number
b. The date
c. Traffic workings with call signs
d. The number and kind of messages (if any) sent
e. The "Direction finding number"
f. Block numbers and Chi-numbers on any 5-figure messages
g. Short plain text messages when available

In the case of 5-figure traffic, this diagram was turned over to a 5-figure section, where an attempt was made to identify the station from a study of the Blocknots and the Chi-numbers, which were checked against the previously indexed or charted data.

All diagrams passed through the Traffic Analysis Section, where the call sign composition was scrutinized, studied in relation to the "Basic Book for Allotment of Call Signs"(Hauptverteiler), and, if unidentified, recorded in the index. Network diagrams and messages were checked against the Card Indexes of names and cover-names[348] for interpretation in the light of the evidence accumulated there.

The network diagrams were passed to the Direction Finding Evaluation Section, which determined by the location of the "fixes" whether the intercept was likely to be, for example, Army (if in an area near the front) or Air Force; or Line of Communication traffic (if in a rear area).

The diagrams went finally to the final Evaluation[349] or Fusion Section, where the results entered on the diagram by the various sections were weighed and considered in the light of information passed to the Final Evaluation unit by the Cryptanalytic section. From here the traffic identified by the Final Evaluation unit was reported to the NAAS, together with the tactical information derived from the messages. The findings guided modification of the cover towards dropping the less important traffic and placing more sets on the "interesting" circuits.

44. Evaluation in a FAK.--The Evaluation Section in the FAK was apparently organized like that in the Feste, although the relative dearth of evidence available precluded drawing a close parallel. Presumably it differed in function from the

[348] The source did not make clear whether this function was performed in the Traffic Analysis Section.

[349] Endauswertung, I 19g p 3

Evaluation section in the FAK worked on identified traffic as well.[351]

As in the case of the Feste, the basic document of evaluation was the network diagram, prepared by the Traffic Evaluation section. This diagram included all evidence by which the station in question had been identified (in the case of 5-figure traffic, the Blocknots and Chi-numbers) and other significant data. Apparently, as in the case of the Feste, this diagram passed through various sections devoted to direction finding evaluation, traffic analysis, work on unidentified traffics, contents evaluation[352] and finally to fusion or final evaluation.[353]

45. Cryptanalysis in the KONA.--The details of cryptanalysis performed by the field units are discussed in Chapter VI of this volume. Because of the importance of cryptanalysis in the total evaluation, however, it is pertinent to note here the organization and function of the sections carrying out this work at KONA level.

Cryptanalysis in the NAAS was performed by a special section separate from the Evaluation and Traffic Analysis sections. The cryptanalytic section totalled less than 60 persons. It was divided into subsections, the most important of which was that devoted to "new developments." Other subsections were 2-figure, 3-figure, 4-figure, NKVD, bookbreaking, and plaintext examination. There was also a small subsection devoted to administration.[354]

The cryptanalytic section had the following tasks:[355]

a. To collect and work on the traffic which the companies could not deal with (whether because of lack of material or preoccupation with more important systems).

b. To test and check doubtful solutions passed up by the companies.

c. To establish whether keys broken by the companies were the first examples of their kind; to complete them and put them in a handy workable form (the so-called "basic form"), and to assign a number to each key appearing in the area of the regiment.

351 I 19b p 5

352 The section concerned with content evaluation "/worked/ on all readable messages, (identified) places, names and covernames...and sees to the immediate forwarding of all important messages to the NAAS." (I 19b p 5)

353 I 19b p 5

354 I 19b pp 10-11

355 I 19b p 9

d. To pass back down all solved key systems to companies who might be concerned.

The function and organization of cryptanalysis in the long range companies (both Feste and FAK) appears to have been much the same in each. On paper, cryptanalysis at company level was a part of the evaluation platoon, in contrast to its independent position as a separate section in the NAAS;[356] it appears to have functioned in practice independently, however, because of the special nature of its work. The evidence indicated that there may have been 15 to 20 persons engaged in cryptanalytic work in the company evaluation platoons.[357]

> "It was the task of company cryptanalysis not only to solve systems, to recover ciphers, to decode already known procedures, and/or to translate all this material, but also to contribute to the identification and interpretation of traffics on the basis of keys employed... /The cryptanalytic section/ cooperated closely with cryptanalysis of the NAAS, but was so organized and equipped that it could work on most messages itself."[358]

The cryptanalytic group was divided into separate sections for plaintext message translation, 2-, 3-, and 4-figure traffic (one section for each), and a general section which kept card indexes and lists and performed certain administrative duties. These sections, besides being responsible for the solution of new systems, the recovery of additive, and the decoding of solved systems, played an important part in traffic identification through a study of the keys employed.[359] The key indicators, which the Russians placed at the beginning and often at the end of messages, were arranged by the numerical designation arbitrarily assigned by the Germans to Russian keys in an index file.[360]

The cryptanalysts relied heavily upon the card indexes in their work, and also had at hand graphic and statistical presentations of single letter, digraphic, and trigraphic frequencies, and lists of pattern words.[361]

356 I 19b p 6
357 I 19b p 11
358 I 19b pp 11-12
359 I 19b pp 11-12
360 I 19b p 41
361 I 19b p 41

They cooperated closely with the personnel engaged in the final evaluation section, often passing notes with the translated messages calling the attention of the evaluators to the key employed on the message or to peculiarities which might have a significance when viewed in relation to the total data. Moreover, the cryptanalysts kept in touch with those responsible for intercept, to the end of obtaining the best possible copy for solution of new systems.[362]

46. Reports.--The findings of the intelligence units were passed to the operating agencies in various reports, and the intelligence in them was made available by an efficient reporting system. Captain Roessler observed that "a smoothly functioning report system was the chief problem discussed at almost all meetings to consider organization."[363] In general, careful provision was made both on low and high levels for efficient reporting. The reports were passed either laterally to other field formations or upwards through signal intelligence channels to the higher agencies. "Hot" items were sent out in "Advance Reports,"[364] while other important but less urgent conclusions were sent in the daily "Situation Reports."[365]

The companies were required to provide highly detailed reports.[366] They had to exercise their own judgment, showing initiative and intelligence in selecting the items to be passed on. A great deal of material was never reported at all but simply went into the card indexes of the companies. The companies had to distinguish urgent from routine items, and the NAAS frequently rebuked the forward units for a failure to send back in a "flash" what they had allowed to get through only in a routine report.[367]

The NAK maintained an evaluation platoon at Company Headquarters which correlated and interpreted the materials from the other platoons, and reported the findings laterally to the Army Corps G-2 and upward to the NAAS.[368]

The basic technical report at company level was a "Day

[362] I 19b p 12

[363] I 19b p 13

[364] I 19g p 7

[365] I 19b p 14

[366] I 19b p 13

[367] I 19g p 7

[368] I 19g p 5; I 19b p 22

Report" made by the intercept operators, listing all traffic heard on the frequencies monitored. There were columns for recording the time of intercept, the frequency upon which the traffic was taken, the call signs to and from, the contents of the transmission, the intercept number and remarks. All intercept operators made similar logs, which gave a picture of the total traffic carried on a particular link or network.

These logs provided the company evaluation sections with the subject matter studied in drawing up their Situation Reports.[369] A typical Situation Report described the deployment and status of identified Russian units and reported any appearance of a new unit.[370]

The reports issued by the Feste and the FAK were much the same. These included:[371]

a. Twice-daily Network Reports (Netzmeldungen)

b. Advance Reports (Vorausmeldungen or Sofortmeldungen) for important tactical items

c. Daily Situation Reports (Tagesmeldungen) for a summary of the day's Advance Reports and all less important data

These reports were sent to the NAAS for further interpretation, and significant intelligence items were then passed laterally to the Armies.[372] A long range company needed an average of 16 typist hours to get out its daily report for the NAAS.[373]

The Feste on the Eastern front issued in addition to the reports listed above a type of report known as the "5-figure offer" for circulation by OKH/GdNA to the other KONA's. The purpose of the 5-figure offer was to assure the maximum exploitation of information available, and in effect constituted invitations to all KONA's to check the data in these reports with their own files. They listed all current data derivable from the external characteristics of messages consisting of 5-figure groups.[374]

The section at the NAAS for technical and tactical analysis, collated and combined the significant findings from all these

[369] I 173 p 24
[370] I 19b pp 21-23
[371] I 19g p 8
[372] I 19g p 8
[373] I 19b p 13
[374] I 19g p 8

reports with the data at hand, passed material not immediately exploitable to the various specialists in the NAAS for a further "squeeze" and passed its combined report to the Army Group.[375] Roessler referred to the daily Situation Reports issued by the NAAS as a "Lagemeldung."

Information furnished by members of In 7/VI showed that the Signal Intelligence Reports issued by the Evaluation Centers of some regiments were called "Funklagemeldungen."[376] These consisted of four component reports:

a. Direction finding reports (Peilmeldungen)

b. Radio traffic reports (Betriebsmeldungen)

c. Radio clear text reports (Funkmeldungen)

d. Radio code-text reports (Verkehrsnachrichten)

These reports went beyond In 7/VI and were passed to the "Army Group Commander as well as to the Army High Command and other echelons and commands on a distribution list of 14 ~~listing~~ listings."[379]

375 I 19g p 8

376 IF 105 p 4

377 These were the evaluated daily reports compiled on call signs (Rufzeichen) and radio traffic (Verstaendigungs-verkehr) of enemy and neutral broadcasting stations (Funkstellen).

378 These contained the decoded and translated texts of enemy messages.

379 IF 105b p 4

VOLUME 4

Chapter VI. Russian Cryptanalysis

Section A. Organization of Cryptanalytic Effort against Russia

47. Review of Central Office Organization.-- Prior to 1939, an agency known as the Intercept Control Station (Horchleitstelle, abbreviated HLS) had a section for handling Russian traffic; but little is known in detail of its achievements.[385] In summarizing German activities before the outbreak of war with Russia, Lt. Col. Mettig (second in command of OKW/Chi) stated that the Germans were able during the first Russo-Finnish war to break a number of two-, three-, and four-figure codes.[386] In addition, a copy of the Russian five-figure code was obtained from the Finnish General Staff. (This particular code was used by the Russians in the first year of war with Germany.[387] The Intercept Control Station (HLS) was replaced in 1941 by two agencies, Inspectorate 7/VI (abbreviated In 7/VI)(serving as a cryptanalytic unit in Berlin), and the Control Station of Signal Intelligence (Leitstelle der Nachrichten Aufklaerung, abbreviated LNA) in Zossen.[388] The section for Russian cryptanalysis that had been part of HLS remained attached to In 7/VI during the first few months of its existence; Russian "evaluation" was done at LNA. Both organizations felt, however, that cryptanalysis and evaluation should be done further forward; and late in 1941, the Russian section of In 7/VI (including cryptanalysts and evaluators) was sent to Loetzen in East Prussia.[389] This section formed the nucleus for a third

[385] IF 181 p 4
[386] I 78 p 3
[387] I 78 p 8
[388] I 78 p 5
[389] I 78 p 8

central agency, the Intercept Control Station East (Horchleitstelle Ost, abbreviated HLS Ost). From this time until November, 1944, German Army Signal Intelligence activities were sharply divided into non-Russian (performed at In 7/VI)[390], and into Russian (performed at HLS Ost and LNA).

In October, 1944, HLS Ost and LNA were amalgamated, together with In 7/VI, into the Signal Intelligence Agency of the Army High Command (Oberkommando des Heeres, General der Nachrichten Aufklaerung, abbreviated OKH/GdNA), the one final central agency of the war.[391]

For the ultimate breakdown of OKH/GdNA in detail see Volume 4, Chapter II.[392] In brief, the assignment of Russian cryptanalytic functions were as follows:

Group III (under Capt. Gorzolla): evaluated traffic and cryptanalytic work from the Russian front

Group IV (under Major Hertze):- did all the cryptanalytic at OKH/GdNA

Section 3 (under Lt. Dettmann): the former cryptanalytic section of HLS Ost, and handled

a. Russian NKVD traffic
b. Russian Army traffic
c. Russian Partisan traffic
d. Research on Russian Systems

390 Discussed in Volume 4, Chapter VII

391 The amalgamation was necessitated by the retreat of HLS Ost to Zossen, where In 7/VI and LNA were located. This move was one of operational rather than cryptanalytic expediency: the Russians were advancing; HLS Ost was retreating; and when the home office and the field cryptanalytic and evaluation offices were all close together, it was certainly more expedient to combine them. The result: GdNA.

392 Derived almost wholly from IF 123 pp 6-14

Group V · Section 1 (under Specialist Block): reconstructed Russian call signs
Section 2 (under Specialist Block): exploited captured Russian documents of signals interest

Group VI (under Capt. Roeder at Potsdam):
Section 1: worked on high-grade machine systems
a. Intercept and evaluation of Inter-Soviet State Traffic
b. Intercept and evaluation of Russian Baudot traffic
c. Intercept and evaluation of Russian Army traffic

Section 3 of Group IV in the above chart was the Russian cryptanalytic section. It may be assumed that HLS Ost, although amalgamated into GdNA, continued very much as it had in its duties, and that the work performed earlier by HLS Ost was identical in nature to the work performed later in Section 3 of Group IV of GdNA.[393]

48. Review of Field Office Organization.-- While preparations were being made for the attack on Russia, it was found that there was an "acute shortage" of cryptanalysts available for field work.[394] Cryptanalysts were culled from the fixed intercept stations and trained for field work with the newly organized Signal Intelligence Regiments (Kommandeure der Nachrichten Aufklaerung, abbreviated KONA). Five of these regiments were sent into the field as complete low level intercept and evaluation units attached to Army Groups: two went to the western front; KONAs 1, 2, and 3 were assigned to the eastern front. These eastern KONAs were supplemented in 1942 by KONA 6, which was sent out to cover the German campaign in the Caucasus[395], and which was attached directly to HLS Ost. Low level cryptanalysis and evaluation was also done by KONA 8 and KONA Nord, which were made up from other Eastern front signal intelligence regiments, and activated in late 1944 and early 1945.

[393] Nothing is known from TICOM sources of the cryptanalytic activities of HLS Ost before its amalgamation into GdNA except a brief statement of Mettig in I 78 p 8

[394] I 78 pp 4, 7

[395] DF 18 p 81

The organization of field units for cryptanalysis has already been discussed in detail.[396] Since the information on Russian cryptanalysis used in this chapter, however, derives as much from interrogations of prisoners engaged in field operations as from the discussion of cryptanalysis of GdNA [397], the reader is referred for a brief review to the chart of organization of KONA 1 [398] about which we know more than any other as it was captured in toto.[399]

49. Assignment of cryptanalytic tasks to the central offices and the KONAs.-- In discussing the task of In 7/VI, Lt. Mettig said: [400]

> "Once the forward crypto-analytic units had been set up and attached to the various forward wireless units it was agreed to allot to them the investigation of forward and Line of Communication traffic which could be solved in the field. In 7/VI remained, however, responsible for all army crypto-analytic work and concentrated on the most difficult and unsolved procedures."

Of the assignments for HLS Ost and LNA as central offices, or for various KONAs in the field, there is no statement in TICOM interrogations. Of GdNA, there is only the statement of Dettmann and Samsonov [401] to the effect that "the solution of agent, guerilla, and Kundschafter traffic was the responsibility of Referat 3c [of Group IV]." The nature, extent, and assignment of cryptanalytic work to these units, both central and field, can only be inferred from the discussions of the Prisoners of War regarding solution and achievement.[402]

[396] Volume 4 Chapter III

[397] Dettmann and Samsonov, "A Report on Russian Decryption in the Former German Army", published as DF 18.

[398] Charts 4-1, 4-4

[399] See also Volume 4, Chapter V for discussion of the functions and duties of the various field units.

[400] I 78 p 8

[401] I 116 p 7

[402] DF-18 passim, for GdNA; all reports quoted in this chapter, passim, for the KONAs

It is clear, in all the interrogations, that actual cryptanalysis was done on all levels of field operations and the central offices almost interchangeably: from the lowest level (where it was considered merely a function of "evaluation") up through the highest level (where it involved pure mathematics and the assistance of IBM machinery). By inference from the interrogations, it can be said that, with one or two exceptions,[403] all types of problems were handled in all units. The flexibility of cryptanalytic assignment was determined mainly by the Russians' use of their own systems. Aside from machine traffic and five-figure codes (Army or NKVD), which it can be assumed contained the most important operational communications, the Russian tactical, strategic, and lower level operational communications were not carried in any set category of systems, determined by their relative importance. Two-, three-, four-, and even some five-figure traffic was used by the Russian Air Force, the NKVD, and the Army at all levels of operations. The German Army cryptanalytic effort, therefore, was oriented to fit the situation as determined by Russian usage. The discussion of cryptanalytic operations on the part of German Prisoners of War was invariably set forth in terms of types of encipherment and difficulty of solution, and took the form of two-figure, three-figure, four-figure, five-figure, NKVD, address, Agents' solution. As Lt. Loeffler pointed out, in discussing company cryptanalysis, "The strength of the various sections was modified to cope with developments on the Russian side--namely, the shifting of emphasis from 2-figure to 3-figure, and then later to 4-figure." Cryptanalytic sections were divided according to this scheme in the company (FAK), the battalion (NAA), and the central agency of the KONA (the NAAS). The same scheme was followed by Dettmann and Samsonov in discussing the whole problem of German Army cryptanalysis of Russian systems [404], and appears to be the underlying

[403] 5-figure codes and partisan and agents' codes are to be discussed later in this chapter.

[404] DF 18

basis for the organization of training the "Russian Cryptanalysis Course" given by Group IV of OKH/GdNA for field training.[405] In this course, more attention was given to two-figure tables and three-figure and four-figure codes because of their operational frequency and their importance for tactical and strategic intelligence.

In short, the various cryptanalytic assignments seem to have been determined for the most part by how the Russians used their own systems (operational area and importance) and by the amount of time and manpower the Germans needed to effect solution. A summary of the assignments follow:

two-figure codes were worked on mostly by the companies (where, it has been pointed out, it was considered part of "evaluation") because of the simple solution and the immediate need for the tactical intelligence involved; but it was also handled by the battalion (NAA), the central KONA agency (the NAAS), and even by the home office (GdNA): Lt. Dettmann says that solving the two-figure codes was "merely a form of crossword puzzle."[406]

three-figure codes were worked on in the companies, but were also handled by the NAA, the NAAS and HLS Ost.

[405] I 166, complete

[406] IF 5 p 6

four-figure codes offered more difficulty in solution, since a large amount of material was "absolutely necessary... the majority of unsolved four-figure codes were abandoned because of an insufficient number of messages"[407]; these were handled by the NAAS and GdNA, rather than on company level, because of the lack of men, machinery (IBM), and time necessary for solution on a forward level.

three-figure and four-figure signal codes were considered somewhat "special" and were handled in the company (FAK) by "chosen cryptanalysts, sometimes by the chief cryptanalyst"[408] and in the NAAS.[409]

five-figure codes, which were generally considered unbreakable, were handed by GdNA, though KONA 1 for a period did five-figure cryptanalysis independently[410]; Dettmann and Samsonov state that five-figure traffic was submitted for the exclusive processing of the [GdNA]."[411]

agents' codes, which had always been done in the central offices[412], were "the responsibility of Referat 3c"[413], mainly because solution "depended on captured material."[414] They were probably given to these central offices by other than Army sources.

[407] I 191 p 8

[408] I 19b p 11

[409] I 19b p 11

[410] I 19b p 43

[411] DF 18 p 83

[412] See Volume 4, Chapter VI and later in this Chapter

[413] I 116 p 7

[414] ibid.

NKVD systems formed a special group of wireless traffic from the Russian and the German points of view, and cryptanalysis of NKVD material was handled by the NAAS[415], LNA[416] and GdNA (through 4-figure) (five-figure)[417]

machine ciphers were considered on the same level of solution as five-figure code and were handled exclusively at GdNA

Whatever systems were solved, or could be easily solved and deciphered, were done as far forward and with as few men and as little time as possible. When more time, or manpower, or mechanical (IBM) or theoretical help was needed, the solution was removed as far to the rear as practicable or necessary. Because of the difficulty involved in solution of five-figure codes (Army or NKVD) and machine traffic, the GdNA was obviously the best agency for handling these; at the other extreme, the companies could almost always solve and process two-figure systems, because of their simple encipherment. All systems of intermediate difficulty, however, were assigned not only to these units but to the intermediate units, depending on state of solution, amount of material necessary, number of men required, etc. Rather than cutting across systems and thinking in terms of specific levels of operation and levels of intelligence priority, both the Russians and the Germans thought in terms of types of encipherment. In discussing the German Army cryptanalytic effort of Russian systems, therefore, the discussion will take the form of two-figure, three-figure, four-figure, five-figure, address, NKVD, etc.

[415] I 96 pp. 46-47

[416] ibid. pp. 9-10

[417] DF 18 p 63

VOLUME 4

Chapter VI. Russian Cryptanalysis

Section B. Cryptanalytic Achievements against Russia

50. 2-figure codes.-- 2-figure codes were used by the Russian Army, Air Force and NKVD. In the Army, they were used by Army Groups, Armies, Corps, Divisions, and Regiments; and by small independent special units such as Combat Engineer Brigades, Motor Regiments, and Artillery Brigades. In the NKVD, they were used on frontier regimental networks and from divisional level downwards.

Solution of 2-figure systems was done mostly on company level (FAK), but was also handled by NAA, the NAAS, and the GdNA.

a) The PT-39. The PT-39 (Peregovornaa Tablica, literally "conversation table"), a 2-figure code placed in a square 10 x 10 and then enciphered by substitution through a 2-figure, 10 x 10 Latin square[422], can be taken as the "mother" 2-figure code.[423]

[422] i.e. no figure was repeated in any row or column

[423] I 191 p 1; I 19c p 1

(Actually, according to the Dettmann and Samsonov[424], the first 2-figure operational system used over a long period by the Army and Air Force of the whole Soviet Union was PT-35, a code with 100 values, re-enciphered daily within the individual networks. In the last months of 1939, PT-35 was replaced by PT-39.) From 1940-1942, it was used far more than all other codes combined.[425] PT-39 was used by Army Groups, Armies, Corps, and Divisions. The identification of the latin square used for encipherment enabled the Germans to establish to which Russian front or army the wireless station using it belonged, or whether it was an Army or Air Force Station. Since the squares were often used for several months, the reconstruction of squares could be easily checked; this appears to have been hardly necessary, however, since the rows and columns could be solved (reconstructed) with a minimum of 15 to 20 groups. The messages were of a technical signal or tactical nature, the latter more especially after the beginning of the Russian campaign in June, 1941. This particular code (PT-39) was used from the extreme south to the extreme north of the eastern front, and in the back areas as far as the Caucasus, middle Asia, and North Persia.[426]

b) The PT-42 and PT 42N. The PT-39 was superseded in May 1942 by PT-42. There is a flat disagreement with this statement in the report of Dettmann and Samsonov, who say that "at the beginning of 1942, PT-41 came into use as the successor of PT-39."[427] Dettmann and Samsonov do not mention PT-42 at all, but their description of PT-41 corresponds to the description given of PT-42. They are very probably the same code and encipherment, misnamed by one or the other of the Prisoners of War. The PT-42 was similar to PT-39 in construction except that the distribution of

[424] DF 18 p 45

[425] I 19c p 1

[426] I 19c p 1

[427] DF 18 p 47

values in the basic square was made random, and variants for values (as many as four for common letters such as o, e, i, a) were introduced. The enciphering method was the same as for PT-39; but because of the random nature of value assignment in the basic square, the solution of a row (or column) of the enciphering square now required about 30 groups. PT-42 was restricted in use to Army Groups, Armies, or Corps. For divisions and regiments, PT-42N was used. It was smaller, with a square 7 x 10 instead of 10 x 10, but its construction was the same as PT-42. As in the case of PT-42, enciphermant was performed by rows, but these were rarely derived from a Latin square. It was used almost exclusively from division forwards and remained in force in some cases until 1944.[428] It produced much tactical information.

c) The PT-43. The PT-42 and PT-42N were superseded (no date given) by PT-43, which was the last general 2-figure code used and which remained in force up to the capitulation of the Germans. Unlike the basic square in PT-39, PT-42, and PT-42N, it contained no letters. PT-43, was used for addresses, particularly by the Air Force and the PWO (A. A. Defense).[429]

d) In addition to PT-39, PT-42, PT-42N, and PT-43, small independent special units, such as Combat Engineer Brigades, Motor Regiments and Artillery Brigades, had their own home-made 2-figure codes which were often in use for only short periods and which, besides the letters of the alphabet and numbers, contained specialized expressions appropriate to the unit concerned.[430]

[428] I 19c pp 1, 2

[429] I 19c p 2

[430] I 19c p 2

It is clear from all the interrogations that 2-figure codes were not always in use, but were being constantly read. Prisoners of War of NAA 11 said that the last known PT table was PT-43, but that they could not reconstruct it.[431] But their statement is the only contradictory one among many others according to which solution was not only easy but current. Capt. Noletzko, (of Ln. Reg. 353) though speaking mainly of air systems (ground/ground, etc.) said, for example, that 2-figure codes were used only by forward troops and were almost 100% readable;[432] he admitted that much assistance was gained through security breaches on the part of Russian operators, but insisted that 2-figure traffic was never very difficult to read.[433] For Lt. Dettmann, solving the PT codes was "merely a form of crossword puzzles."[434] Gerlich stated that one or two men were sufficient at NAAS 1 to cope with current decipherment of 2-figure messages, especially as the greater part of them were already being solved in the companies, but added that solution was made easier when plain text was interspersed.[435]

The Prisoners of War of KONA 1 stated categorically that the Russians practically ceased using 2-figure codes after 1943.[436] But other evidence would indicate that the Russians continued to use them up to the cessation of hostilities, although only for forward troops. Capt. Schmidt stated that the Army and NKVD used 2-figure codes up to the end of hostilities[437]; but Gerlich said, "In the last stages 2-figure systems only occurred where the units were engaged

[431] I 106 p 2

[432] I 75 p 10

[433] I 75 p 4

[434] IF 5 p 6

[435] I 191 pp 2, 3, 4

[436] I 19c p 1

[437] I 55 p 11

in fighting: Thus it is to be expected that they are still being used in the Red Army even if they are not appearing at the moment."[438]

51. 3-figure codes:- 3-figure codes were used by the Army, the Air Force and the NKVD. They were used first (1941-42) mainly by the Air Force; later, more widely by the Army. Every Army Group, Army, Corps, Division, Brigade, Regiment and Battalion had its own 3-figure code. The 3-figure codes were replaced by 3-figure Signal Codes in 1943 which were used by all units from Army downwards. In the NKVD, they were used by the Black Sea Fleet and from division downwards.

Solution of 3-figure codes was carried on mostly in the companies (FAK), but since the 3-figure codes offered more difficulty to solution than the 2-figure codes, they were also handled by the NAA, the NAAS, and HLS Ost.

Three-figure codes were first noticed in February, 1941. They were used increasingly from May, 1941 and the beginning of the Russian campaign. From then until the second half of 1942, the Air Force were the greatest users of this code and each Air Division had its own cipher. In 1942, the first Army unit (the 48th Army then in the Caucasus) started using a three-figure syllabic code.

"By the time of Stalingrad practically every Army engaged in the battle had its own 3-figure cipher."[439] Although they speak of specific 3-figure codes under various circumstances, Dettmann and Samsonov do not discuss any 3-figure codes as such; it can only be assumed that they considered the type of book and encipherment so similar to the 2-figure PT series that they did not warrant discussion as a special type.

Like the 2-figure system, the 3-figure system consisted of a code-book, and an enciphering table of some sort. The first 3-figure codes were simple in form, and were made up of several pages (at most 10) which contained common words arranged alphabetically. Originally the letters of the

[438] I 191 p 4; see also DF 18, p 47

[439] I 19c p 2

alphabet were placed at the end of the book (arranged alphabetically, semi-random, or random), but were soon afterwards put into the book in their alphabetic position. After some months, this total alphabeticity was replaced by a partial-alphabetic arrangement (alphabeticity maintained only within letters); and numbers were scattered at random through the book.[440] The book could have 1,000 groups, but 1st. Lt. Schubert stated that the average was 300-800, "in general small scope, but frequent change."[441] If the code were smaller than 1,000 groups, alternatives were given either to pages or first figures of the lines.[442] The methods of enciphering were extremely varied in details, but always involved encipherment of a single figure separately.[443] The substitutions could be constructed without any recognizable system or they could be made up from a Latin square; the square usually lasted about a month, although in the Air Force, it sometimes lasted longer.[444] Schubert stated that "Towards the end, there appeared quite isolated 4 to 7-figure substitution systems-- presumably private systems of the respective cypher departments. I imagine this to be so as they appeared very seldom."[445]

The only specific 3-figure code referred to in TICOM is what the Germans called R3ZC (Russian, 3-Zahlen [figure], Code) mentioned by Corporal A. Faure of NAA 11, the "Norway Party."[446] (It was a code with 10 pages of 100 positions each, 10 x 10, alphabetically arranged. Only the hundreds and tens figures of each group were enciphered.) In general, either the 3-figure code book itself or the method of encipherment were so varied that Prisoners of War were able to remember only general characteristics, no specific examples.

[440] I 19c pp 2, 3

[441] I 26 p 2

[442] I 19c p 3

[443] I 19c, p 3; I 26 p 2

[444] I 19c p 3

[445] I 26 p 3

[446] I 55 p 12

The 3-figure code, it is clear from all interrogations, was used mainly by the Army, but also by the Air Forces. According to the Karrenberg party, on regimental networks and for less important messages on the level of assault armies, mainly the 3-figure code (with a 2-figure latin square encipherment) was used.[447] But the Prisoners of War of KONA 1 stated that every Army Group, Army, Corps, Division, Brigade, Regiment, and Battalion had its own 3-figure code which it used to communicate with its subordinate units.[448]

It is curious to note that a good deal of plain text was inserted in the 3-figure enciphered code as transmitted.[449] Gerlich pointed out the advantages of plain-text insertion: "They often gave words and names not contained in the code ...."[450]; and continued, "3-figure systems were always solved when sufficient material on one encipherment was available."[451] This would appear to be the general viewpoint, since Capt. Holetzko stated that 3-figure traffic was only slightly more secure than 2-figure traffic and was 80% readable.[452] In this case, Holetzko was talking particularly of 3-figure codes as used by the Russian Air forces (ground/ground). It is known that Air Force codes were often current for much longer periods than those of the Army, sometimes lasting a year;[453] and would thus afford more opportunity to find depths and set up overlaps. Army 3-figure codes were nearly always changed after a big operation and were with few exceptions never current for more than a month or two, sometimes for only a week;[454] solution was thereby made more difficult. Nevertheless, Lt. Starke (who worked with 3-figure traffic in a NAK) stated that, given depth of traffic, all codes were readable;[455] and

[447] I 173 pp 10, 11

[448] I 19c p 4

[449] I 26 p 2

[450] I 191, p 7

[451] I 191 p 7

[452] I 75 p 10

[453] I 19c p 4; DF 18 p 5

[454] I 19c p 4; DF 18 p 5

[455] I 75 p 6

Lt. Col. Mettig said flatly that from the spring of 1943 to 1945, 2-figure and 3-figure traffic was regularly decoded.[456] It can be assumed that 3-figure traffic was being read currently enough and constantly enough, to provide a great amount of tactical intelligence.

The operational 3-figure codes were discontinued in 1943 and were superseded by 3-figure Signal Codes[457] which were different only in that they contained no letters, but only words or phrases of tactical importance, and were not alphabetic but had meanings grouped under various headings such as "attack," "defense", "enemy movements," "designation of units", "figures or numbers","signal connections", etc. Each meaning had two or three 3-figure groups allotted to it. As in the case of the former 3-figure codes, anything not contained in the book itself was sent in clear.[458] Every unit from Army downward had its own signal code for use with subordinate units. There is no evidence that solution of these 3-figure Signal Codes was more difficult than solution of the 3-figure codes; nor is there any record of success either in totality or currency of decipherment. Lt. Loeffler of Feste 10 did, however, state that they were considered "special procedures", and "were studied in the appropriate section by specially chosen cryptanalysts, for the most part also by the chief cryptanalyst."[459] The solution time varied according to

[456] I 78 p 8

[457] Dettmann and Samsonov spoke of 3-figure and 4-figure "signal codes" described by members of KONA; but there are discrepancies between the two descriptions, and again it is impossible to determine where the mistake lies. The discussion as given by KONA 1 members seems generally more reliable.

[458] I 19c p 4

[459] I 19b, report 6, p 11

security, amount of material for overlapping, etc.; and we can only assume that the Signal Codes were read as consistently and as fully as the 2-figure and 3-figure codes they superseded.

52. 4-figure codes.-- 4-figure codes were used by the Army, Air Force, and NKVD. They were used in the Army as General Army Codes (called General Commanders' Codes), and on lower operational levels by mobile formations such as Tank and Mechanized Corps, Tank Armies, and Tank Administration and Supply Units. In NKVD, they were used on Railway and Transport Nets.

Solution was handled partly by the companies (FAK) (There was a 4-figure section, as well as a 2-figure and a 3-figure section, in the organization of a typical company cryptanalytic setup[460], but in all probability mostly by the NAAS and GdNA.)

1st Lt. Schubert (of GdNA) stated that, "The Russian Army keys are 3- or 4-figure systems. The basis is the same."[461] Actually, the construction of 4-figure codes was in principle the same as in the case of 3-figure codes, except that the basic book had a possible 10,000 groups instead of 1,000.[462] Schubert stated that there were in the code perhaps only six or seven pages[463], each with a block of consecutive numbers; but the description given by the members' of KONA 1 indicates books of from 5 to 100 pages. The latter seems more likely.[464] In any case, the number of pages could vary from 5 to 100 (the Air Force Codes usually had about 10,000 groups and the Army 5,000 or less), and each page could have variant page designation.[465]

460 I 19b p 11

461 I 26 p 2

462 I 19c p 4

463 I 26 p 2

464 I 19c p 5

465 I 19c p 5

The actual construction of pages varied in 4-figure codebooks as much as it did in the 3-figure code books, in respect to alphabeticity and sequence of numbers, etc.. But the methods of enciphering the last two digits were still more varied than those used in 3-figure systems: substitution by row, digraph substitution (in comparison to single-letter substitution in the case of 3-figure codes), combinations of these two, abbreviated figures in the substitution, and others.[466] Karrenberg, in his discussion of the "Russian Cryptanalysis course", given for field training mentioned that "a 3-figure or 4-figure code can also be reciphered on an adder. For this purpose a text chosen at random is enciphered (likewise by the code) and the code text added to or subtracted from (non-carrying)."[467] But there is no other indication in interrogations that this method was met in actual practice. The general method seems to have been variant page designations for the book (2 figures), and encipherment of the last 2 digits by various means, including 2-figure Latin squares.[468]

From May, 1941, the Air Force began to use 4-figure codes in many different forms but often of the simplest construction. In the middle of 1943 many mobile formations, Tank and Mechanized Corps, Tank Armies, and Tank Administration and Supply units also started using 4-figure codes. They were also used by Railway and Transport Nets.[469]

Dettmann and Samsonov (of GdNA) described the "first general army and air force" code (4-figure with roughly 4,600 groups, enciphered with digraphic substitution), and its successors "OKK 5" to "OKK 8" (General Commanders' Codes) that rapidly replaced one another from 1939-41. OKK 5 was captured in the Russo-Finnish war; and OKK 6, 7, and 8 were captured in the Russo-German war. But Dettmann and Samsonov

[466] I 19c p 5

[467] I 166 p 7, 8

[468] I 173 pp 10, 11

[469] I 19c pp 5, 6

insisted that, "All these systems were, however, recovered by cryptanalysis before their capture and were made completely and currently readable."[470] Lt. Loeffler (of Feste 10) stated that "a general army 4-figure cipher was last observed in use in North Persia in the winter 1941-42. It had 50 pages, each designated by two alternative bigrams and 100 lines to each page."[471] There is no other indication in the interrogations that four-figure codes were no longer, or less frequently employed.[472] In 1944, however, four-figure Signal Codes (of the same form as the 3-figure Signal Codes) made their appearance in the Army, especially with the army groups,[473] and probably superseded in great part, if not wholly, the 4-figure codes just discussed.

Generally speaking, 4-figure codes were changed less frequently than other codes[474]; but even then, the change came too frequently to judge from Gerlich's statement that " a more frequent change of encipherment would have made decipherment impossible."[475] Certainly the 4-figure codes gave German cryptanalysts a certain amount of trouble; actually, a large amount of material was "absolutely necessary, and the majority of unsolved 4-figure codes were abandoned because of an insufficient number of messages."[476]

[470] DF 18, p 55

[471] I 19c p 5

[472] Lt. Loeffler said only that a four-figure code was used by the VI Guards Mech. Corps (1st Ukraine Front) from January 1945 to the end of hostilities. It was captured in January, 1945.

[473] I 19c pp5, 6

[474] I 19c p 8

[475] I 191 p 8

[476] I 191 p 8

Captain Holetzko (speaking mainly about 4-figure air force codes (ground/ground), said that they were "only 60% readable".[477] And Corporal Heudorf (of NAA 8) admitted that later 4-figure traffic on occasion provided some difficulty, but on the other hand recalled an [Engineer] Unit in March and April, 1945, whose 4-figure messages were read currently.[478]

In the interrogations of KONA 1 members, the following 4-figure codes were listed as solved:[479]

4-figure code of VI Guards Mech. Corps (1st Ukranian Front) from January, 1945 to end of hostilities

4 figure code of 152 Independent Tank Brigade (60th Army, 1st Ukranian Front)

4-figure Signal Code of VI Guards Tank Corps (1st Ukranian Front)

4-figure code of Tank Supply and Administration Authorities of 1st Ukranian Front

4-figure code of 76th Regional Air Base (Russian 76 RAB)

4-figure code of Supply Units of 13th Army (1st Ukranian Front)

4-figure code of 3rd Guards Tank Army.

1st. Lt. Schubert, of GdNA, said simply, "We broke Army three-and four-figure re-enciphered books. These were enciphered on a conversion table. Early in the war we read most of this traffic, but at the end only 40 to 50%.[480]

[477] I 75 p 10

[478] I 75 p 8

[479] I 19c pp 6-8

[480] I 15 p 1

53. 5-figure codes.-- 5-figure codes were used by the Army, Air Force, and NKVD. In the Army, they were used by the NKO (Defense Council), Army Groups, Armies, Corps, Divisions and Brigades. In the Air Force, they were used by Air Armies, Air Corps, Air Divisions, Regional Air Bases, Anti-Aircraft Defense, Anti-Aircraft Corps, and Anti-Aircraft Divisions. They contained strategic, tactical, personnel and supply matters, and political reports and directives.

With the exception of a short period in 1943, when KONA 1 did independent 5-figure cryptanalysis, solution of the 5-figure codes was handled exclusively by GdNA.

In discussing the achievements of In 7/VI (predecessor of GdNA),Lt. Col. Mettig said very glibly, "The breaking of the Russian 5-figure recyphered code... was the most outstanding cryptanalytic achievement of In 7/VI. The Russian 5-figure was broken chiefly by Dettmann."[481] And elsewhere, when rating the relative importance of cryptanalytic achievements contributing to total intelligence, he was "most impressed by the continuous breaking of the Russian 5-figure code despite the difficulties that were experienced after the Spring of 1943."[482] As the interrogator pointed out in reference to this last statement of Mettig, "Even in this case, however, there exists the danger that PW is laying more stress on organizational measures carried out to facilitate the breaking of the code than on actual cryptographic achievement."[483] It might be mentioned in passing that Dr. Otto Buggisch (of OKH/Chi and OKW/Chi) evaluated Mettig as follows: "Only a few fundamental ideas about cryptanalysis."[484]

[481] I 111, p 2

[482] I 128 p 2

[483] I 128 p 2

[484] I 176 p 6

Certainly the evidence from other Prisoner of War interrogations pointed conclusively and without a doubt to an almost complete failure on the part of German cryptanalysts to make any real progress with the solution of the 5-figure code. In the interrogations of members of KONA 1, Corporal Althans (of the NAAS) clearly stated that successful cryptanalysis of the 5-figure code was possible only if

1) there were a number of messages, at least three, which had had the same additive applied; or
2) the 5-figure code had been captured.[485]

Dettmann and Samsonov[486] talked at great length about the 5-figure codes used by the Russians. According to them, codes "011-A," "023-A," "045-A", "062-A", and "091-A", used successively from the beginning of the Russo-German war to the capitulation, did prove difficult for pure cryptanalytic solution; but they continued, "It is interesting to point out that during the course of the war all the newly appearing versions of the "cipher-code" were captured through fortunate circumstances, and always so soon that the originals were almost always in the hands of the cryptanalyst at the instant of their being put into use by the Russians."[487] Of course, this "continuous capture" was an aid in solution, under such circumstances because of the one-time pad encipherment. (See below for discussion of the encipherment itself) As they said, the "individual" tables "offer almost complete security against breaking."[488]

[485] I 19b, report 25 p 43

[486] DF 18 p 59

[487] DF 18 p 59

[488] DF 18 p 61

In the reports of personnel from NAA 11, Capt. Schmidt stated that "with regard to Russian traffic, the Abteilung /Battalion/ did everything up to and including 4-figure. 5-figure they considered insoluble and forwarded to GdNA."[489]

Corporal Karrenberg, (of GdNA) discussing 5-letter and 5-figure codes used for operational orders, said, "These were the so-called Blocknot codes, which were only used once and were therefore unbreakable."[490] Elsewhere, in his description of the "Russian Cryptanalysis course given at GdNA he stated flatly:

> "5-figure and 5-letter messages were not touched at all. In general very little work was done on decipherment of 5-group messages, although these contained the most important operational reports. They were only used to identify units and were only read if code books happened to have been captured.[491]

In 1943, KONA 1 for a period did 5-figure cryptanalysis independently of GdNA.[492] But the general practice was for all units to send 5-figure traffic directly to GdNA for possible decipherment.[493] And as Karrenberg pointed out, "even at the HQ of GdNA little attention was given to the 5-figure messages and very little enthusiasm displayed in working on it. Only the preambles were used to identify units, from Blocknots and indicator groups.[494]

[489] I 55, pp 9 and 11

[490] I 173 p 6

[491] I 166 p 78; see also I 75 p 10

[492] I 19b report 25 p 43

[493] see I 19b report 5 pp 9, 10

[494] I 166 p 79

Finally, Lt. Schubert, when questioned on possible success on five-figure codes, replied: "In the Finnish campaign the book was captured and the Russians used the one-time pads over again. Because of this we had considerable success. Recently the Russians used the pads correctly, and only very few messages were read, these through re-encodements."[495] This small measure of success was obviously due to the fulfillment of the two conditions set forth by Corporal Althans for successful cryptanalysis.[496]

Actually, the Finns had captured and turned over to the Germans a Russian 5-figure book which was used continually until the Russian-Finnish war. An additional copy had been captured by the Germans. And though the Russians introduced a new 5-figure code on 1 April, 1942, the change-over was faulty and it was possible to establish 2,000 groups of the new code within a week.[497] But it is clear that after this time, there was practically no success in 5-figure code solution, though the Germans were able to establish the nature of the book and the type of encipherment:

> The 5-figure code books contained about 25,000 out of the possible 100,000 groups, the pages being numbered 000999 with a hundred lines on each page. The Germans never broke a book and any examples they had were captures.[498]

Alphabetic at first, the 5-figure codebooks later became partially alphabetic; they contained letters, words, phrases, 2-figure numbers, types of units, specific units of the Red army, full stops and commas on every page, all designations of types of tanks, ammunition, etc.

[495] I 15 p 1

[496] see above, p 28; I 19b report 25 p 43

[497] I 78 p 8

[498] I 19c p 8

The encipherment was effected by applying additives taken from enciphering pads known as BLOCKNOTS (a variable number of sheets on which 50-100 5-figure groups appeared). Each pad had a 5-figure number, and each sheet had a 2-figure number running consecutively. There were five different types of Blocknots:

1) I - (individual): 50 pages, additive read off in one direction only
2) Z - (circular) - 30 pages, additive read off in
3) OS (?) either direction
4) Notblock (emergency)
5) Blocknot used for passing on traffic [499]

The distribution of Blocknots was carried out centrally from Moscow to Army Groups to Armies. The Army was responsible for their distribution throughout the lower levels. Occasionally the same Blocknot was distributed to two units on different parts of the front; and here the second condition for successful cryptanalytic success established by Corporal Althans was fulfilled: depth was established. "It seems that depths of up to 8 were established at the beginning of the Russian Campaign but that no 5-figure was broken after May 1943."[500]

54. Address Codes.-- Address Codes (2-figure, 3-figure, and 4-figure) were used by the Army for Army Groups, Armies, and Independent Corps. They were used more widely by the Air Force and the Anti-Aircraft Defense.

Solution of address codes was considered somewhat "special," to judge from the statements in KONA 1 interrogations describing cryptanalytic operations of the various units:

> In the FAK: 15 to 20 people were adequate for company cryptanalysis. Special procedures such as Signal Codes (3-figure and 4-figure) and word codes and address codes (3-figure), were studied by chosen cryptanalysts, sometimes by the chief cryptanalyst.[501]

[499] I 190 p 9

[500] I 19c p 10

[501] I 19b report 6 p 11

In the NAAS: Section 4 /new developments/ did the real cryptanalysis: it normally concentrated on difficult systems which the companies had neither time nor manpower to deal with adequately. It consisted mainly of mathematicians and worked on, inter alia, addresses (2-F, 3-F, 4-F)[502]

Although mention was made in the KONA 1 interrogations of 2-figure address material, nothing was recorded in the interrogations on this subject except one statement in the final interrogation of NAA 11 personnel:

"Bigrams and Trigrams in Addresses

Blome knew of the two used separately, but could not recall any case of the two in conjunction. He suggested that this might accompany something he had seen, namely 3 Z code mixed into 2Z traffic."[503]

There was no record of extent or success of solution with regard to 2-figure address codes. Likewise there was no description of 4-figure address codes nor any statement regarding the extent or success of solution.

Schubert of GdNA stated that towards the close of hostilities, the Russians were using a 3-figure code for addresses. "In this code the clear position remained unchanged for periods, but the ciphers were changed daily. These ciphers were in some way related to the call signs."[504] The only description of 3-figure address codes was given in the KONA 1 reports.[505]

[502] I 196 p 11

[503] I 106 p 2

[504] I 60 p 2

[505] I 19c--"Annexe on Russian Codes and Ciphers"

Three-figure address codes were used in connection with 5-figure messages;[506] their construction was similar to that of the PT-39 or PT-42 codes,[507] but they contained only figures, unit designations, authorities, and words such as "for" or "from." A code of this type was first used at the beginning of 1944[508] on the 1st and 2nd Ukrainian and the 1st White Russian fronts for communications between Army Groups and their respective Armies, and Independent Corps. In the summer of 1944, Armies began to use similar codes with their subordinate units; and latterly the use of such codes increased still further. According to the members of KONA 1, the solution of these codes given a fair amount of material, was generally easy.[509] But members of NAA 11 stated the following:

> "Addresses to personal names rather than titles were common in all Russian traffic, and this suggested the use of initials. The vagueness of this answer surprised interrogator who asked if the addresses, being enciphered on the PT table, were not read currently. The answer was that unless the same address was used frequently and some outside hint was given they were usually unable to read the address. They supposed it used values which had special local meanings added to the table."[510]

[506] I 173 p 8

[507] "PT 42 was superseded by PT 43.. . It contained no letters and was used for addresses, particularly by the Air Force and PWO (AA Defense.") I 19c p 2

[508] Dettmann and Samsonov gave1943 in DF 18 p 5

[509] I 19c p 4

[510] I 106 p 2

55. Miscellaneous.-- Most of the statements given here are taken from the interrogations of members of KONA 1. It is not the complete story, as the Prisoners of War themselves were aware:

> "In the above paper examples are given only of those ciphers whose basic construction was established. There were many types of cipher which were only partially broken and whose basic form could not be established, these are not mentioned... . The number of Russian ciphers of all sorts that were broken was about 3,000."[511]

a) Four-letter codes. Two forms of four-letter code first appeared in practice traffic between Army Groups and Armies and Independent Corps of the 1st Ukraine Front in November, 1944:

1) Revolving stencil: sheet of paper ruled off into 8 x 8 squares; a sheet with 16 holes superimposed and revolved at 90° turns around the central point; all 64 squares were filled; the text was enciphered horizontally in 1, 2, 3, 4 positions; the cipher text was read off horizontally.

2) Transposition: a keyword gave the key; the text was written in vertically according to the key, and upwards or downwards according to instructions; the cipher text was read off horizontally.

The contents were usually about tactical signal matters, through "recently [1944] units and positions were named."[512]

On the subject of transposition systems, Gerlich (of GdNA, Group IV, Section 3) said only this:

> "These were comparatively rarely used by the Russians... I do not know whether such transposition systems were solved at Sigint. Stn. 1, however, I know that transposition messages were being read that "stencils", etc. were used; however, I think they were solved at General of Sig. Int's."[513]

[511] I 19c p 11

[512] I 19c p 10

[513] I 191 p 10

b) Word-Code. From the middle of 1944 a word code was used in the area of the 2nd Ukranian Front. The book consisted of 2 halves each designated by a word such as SEVER ZAPAD /literally, North West/; clear groups were in 2 columns; each half of the code contained a number of columns with cover words. The words identified were only used by the Army and contained strategic and tactical reports and the names of units. They were small in size and contained only essential groups.[514] Schubert added that they were called TARNTAFELN.[515] There was no statement regarding extent of solution.

c) Periodic and Columnar Substitutions. Corporal Karrenberg stated, in discussing the "Russian Cryptanalysis Course," "/These/ rarely appear in Russian cipher systems... . Periodic and columnar substitutions concluded the sections on substitution systems in the course. Not so much time was spent on them as they are rarely encountered in practice."[516]

d) Coordinate systems. "These were very varied. Armies made up their own systems and arbitrary reference points and grids were used."[517]

e) Machine ciphers. The handling of teleprinter traffic has been mentioned earlier in this chapter in description of GdNA duties. It was processed exclusively at GdNA. Lt. Schubert stated that teleprinter traffic was worked on in the machine section /Group VI/; he thought that messages in depth had been read, but was uncertain whether the machine had been recovered. He himself never worked on machines, but knew that the Russians had a machine in use already at the beginning of the war, but not on military traffic.[518]

[514] I 19c pp 10, 11

[515] I 15 p 9

[516] I 166 pp 54, 62

[517] I 19c p 11 See also DF 18 pp 72-75 for details

[518] I 15 pp 8-9

Corporal Karrenberg(of GdNA) spoke of "Bandwurm," and defined it as Russian Baudot letter "strip," not to be confused with Russian 5-letter traffic also carried on Baudot lines. The Germans did not capture any of the apparatus used, but felt that it consisted of 2 parts: 1) a Baudot teleprinter and 2) a cipher attachment consisting of 5 small wheels driven by one large wheel.[519] Depths were frequent, but the Germans did not seem to have any attempt to reconstruct the wheel patterns. The system used by the Army and Air Force and to a lesser extent by NKVD.[520]

Dr. Otto Buggisch (of OKH/Chi) went into somewhat more historical detail and stated that:

1) In 1943 (He heard), Goering's Research Bureau Forschungsamt, abbreviated FA) had claimed some success on a Russian teletype machine and had recreated the action.[521]

2) Late in 1943 and early in 1944, OKH itself began to intercept non-morse, 5-impulse traffic (called "Hughes" by Buggisch). The Mathematics section of In 7/VI (see Vol. V, Chapter II, on organization) worked on it; at the end of 1943, there was a "Kompromiss," and a depth of 8 messages with the same setting was created. The section was able to recover 1400 letters of pure key, and to determine that the traffic was derived from a 5-figure code. The Germans postulated a machine like the German T 43, but was not able to prove any theories they had.

3) Hollerith machinery was devised to locate depths, but in actuality only three or four more depths were found and were of no long-termed value.

4) The traffic (Buggisch thought, since he left the section in June) slumped off in 1944, and LNA took steps to improve reception.[522]

[519] I 30 p 2

[520] I 30 p 2

[521] I 176 p 6; I 64 p 2

[522] I 64 p 2

"Buggisch stressed one fact which had surprised him, that they had never had information about either of these machines (he assumed that the one the FA broke was not the same because of the difference of cycles) from PW or agent sources."[523]

The number of links, according to Corporal Karrenberg, varied according to the number of armies, with a maximum of 8. One end of link was Moscow, the other mobile. After 1944, no work was done on the traffic except on the spot. No vital clues to the system were given away by the Russians, though their security precautions were not considered good.[524]

56. NKVD and Agents' Codes. NKVD Codes were simple monoalphabetic substitution, 2-figure, 3-figure, 4-figure, 5-figure, and 5-letter types. They were used without any apparent reason on two large networks: 1) the networks of the NKVD Central Authorities (the networks were subdivided into those of Security Troops, Frontier Troops, and Railway and Convoy Troops); 2) the networks of NKVD Formation (communication between units attached to Army Front Staffs). 4-figure and 5-figure codes were used on the front lines: there was a 4-figure code, for example, used by the military police, and a general 4-figure code used on Staff-Regiment-Battalion links.

Solution of NKVD codes was handled by the NAAS and GdNA. "The traffic of the NKVD formed a special group of Russian wireless traffic. The distinction applied equally to the manner of conducting traffic and to the message themselves."[525] The German Army cryptanalysts reflected this Russian "distinction" in their own attacks on NKVD systems, allocating the work--again as in regular army and air force traffics--to levels of operation determined by difficulty of solution. Lt. Ed. Woellner (of KONA 1) stated that "NKVD traffic was always covered, but only by Long Range Sigint [the FAK]. Evaluation and cryptanalysis were done by NAAS."[526] On this same subject, Lt. Loeffler (of Feste 10) stated that "all NKVD signals originating in the regiment's area were worked on in the NAAS, others were sent on to LNA."[527] But in neither case was there specified what type of NKVD traffic was worked on, and what type was passed to higher echelons. Apparently, the distinction corresponded to that observed in the case of actual army traffic. All lower-level

[523] I 64 pp 2,3

[524] I 153 p 7

[525] I 19b, report 28, p 47

[526] I 19b, report 27 p 46

[527] I 19b, report 6, pp 9, 10

operational codes (up through 4-figure, e.g) could be handled by NAAS. The five-figure codes were not dealt with by the KONA, but handled by 40 to 50 men in LNA at Zossen[528] where Lt. Loeffler "thought that a good deal of success was obtained in the case of the Far Eastern traffic." Dettmann and Samsonov substantiated this point, in their discussion of the German army cryptanalytic effort:[529]

> "All the five-place message material from the Army or the Airforce, as well as the NKVD messages, was submitted for the exclusive processing of the General of Communications Intelligence" /GdNA/

They also gave full descriptions of NKVD systems.[530] (There was no discrepancy between the facts in their report and the facts given by Lt. Loeffler.) The details of description were scattered throughout the report according to types of encipherment. They mentioned the following:

a) Mono-alphabetic substitution systems common to all NKVD organizations
b) Conversion systems /substitution and additive/
   - 1936: 4-figure code: 2500 values; used in district
   - by 1939: three 4-figure conversion systems; codebooks of up to 5,000 values; enciphered by digraphic substitution or conversion tables
   - 1939: first general NKVD 4-figure code; 10,000 book positions enciphered first by single digit substitution, later by additive

[528] I 19c p 12
[529] DF 18 p 83
[530] DF 18 pp 62-71

At time of capitulation: three 4-figure systems: (ZERNO, NEVA, VIZA, see infra) used respectively by
1) NKVD troops
2) NKVD border defense troops
3) NKVD security troops 531
(200 messages were read daily in all three)
last of larger systems: 5-figure railway code: 2500 groups; digraphic substitution encipherment few 3-figure smaller codes (read currently) letter transposition codes: never found in NKVD traffic number series:
1940: 4-figure; single letter conversion encipherment
(1941 - 1942): 4-figure; enciphered by text key (letters equalling numbers)
1942: 4-figure enciphered by military technical manual (used by Interior troops) until end of 1944: general encipherment combining single digit conversion and Gama Tables (no description of these is given)

Private Huchting (of Feste 10)532, speaking primarily from a traffic analysis point of view, gave the breakdown of NKVD nets:

1) Networks of the Central Authority, subdivided into
   a) Central Authority of the Security Troops
   b) Central Authority of the Frontier Troops
   c) Central Authority of the Security Troops (Divisions and Brigades of the Back Areas)
   d) Central Authority of the Railway Troops
2) Networks of Formation, consisting of communications between commanders of the security troops at front Staffs and their regiments and between the latter and their battalions.533

531 cf. Schubert's report, I 26

532 I 19b report 28, p 47

533 I 19b p 48

A close watch was kept on the networks of 1a, because they carried communications between the central NKVD authority in Moscow and the commanders of Security troops working with the Army groups, the directing staffs North and South, and the "less interesting independent Company Headquarters Signals regiments." The messages were not readable.[534] Messages passed on formation networks, however, were"for the most part readable."[535] In addition to the monitoring of Central Authority NKVD--Front HQ. NKVD and Front Staffs (Frontier Regiments) traffic, close watch was kept on traffic from regiments to battalions, because "most of the messages could be read. They mentioned army units by name, etc."[536] ("Traffic of rear NKVD troops and of the Signals regiments were of no interest, and were not covered by KONA 1."[537]

Lt. Schubert (of GdNA) stated, "After my studies /winter of 1941/, I was posted to a cryptanalytic course at OKH. Since I have functioned as a cryptanalyst. I worked on Russian Army till March, 1943. Then KONA 6 was given the commitment of covering Russian partisans, and I worked on that till September of that year. After that KONA 6 was dissolved... . and I went to GdNA... .and took over all Eastern Cryptanalysis /3 branches: Army, NKVD, and Partisans/."[538] Lt. Schubert was familiar with the same codes mentioned in Private Huchting's net breakdown (1a, 1b, 1d): Security Troops', Frontier Troops', and Railway and Convoy Troops' codes, but mentioned also "one or two ciphers of NKGB... .the 4th section of NKVD,"[539] concerned with measures against enemy agents and their own active espionage.

[534] I 19b, report 28 p 47

[535] I 19b p 48

[536] 19b, report 27 p 46

[537] I 19b p 46

[538] I 26 p 1

[539] I 26 p 3

Lt. Schubert spoke of two 5-figure codes: the SMERSCH /operations of Russian agents/ organization code (with an individual subtractor); and the Railways Troops Code (actually a 4-figure code, enciphered by substitution tables, the 5th digit representing the quadrant on the page in which the group appeared).[540] But he was much more familiar with 4-figure NKVD Codes, which were apparently much more exploitable than the 5-figure codes.

The Security Troops Codes were of two types. One was used forward of regiment, when a regiment was used in approximately an Army Group Sector ("it is a cipher, therefore, used forward of Army Group")[541] This particular code ran for a comparatively long period; "the last one which was still valid in the middle of February when I left OKH, had already been running 1 1/2 years." This code was alphabetical and contained 100 pages, 25 or 50 groups per page; it was enciphered by means of an enciphered indicator which provided for page and position substitution, the result of which was again enciphered by a substitution table. These substitution tables were also valid for a longer time and varied with the network.[542] The additives on the page did not change, only the substitution table.

The second type, a code used rearwards of regiment, was enciphered by a figure subtractor originally taken from tables (up to Sept. 1944). The same tables could appear on different networks, and since the subtractor was used very frequently, "it was not uncommon for 20 messages to have the same subtractor."[543] In October, 1945, 2 subtractors were used, taken from different tables; and the indicators for the 2nd subtractor were enciphered with the first one.[544] In spite of the potential difficulties involved in this method of encipherment, the system was solved by February 15, 1945, though mainly because of bad Russian usage of the system.

[540] I 26 p 4 ; see also DF 18 p 67

[541] I 26 p 3

[542] I 26 p 3

[543] I 26 p 3

[544] I 26 p 4

The Frontier Troops Code was exactly like the Security Troops Code rearwards of regiment, with a different basic book, at least in traffic out of Leningrad.[545] (Lt. Schubert made a statement on the Railways and Convoy Troops Code quoted above).

The four-figure NKVD codes exploited by KONA 1 were used by front line units (regiments and battalions) mainly employed as Military Police. "From 1933-42, R4ZC4 /Russian, 4-figure, Code 4/ was in use. It consisted of a 100 page alphabetic book each with a hundred lines. Recipher was carried out by means of 31 bigram tables. It was broken by the Germans in 1940."[546] "Only one code book (known to the Germans R4ZC 1800 and to the Russians as KODOWAA TABLICA "ZERNO") was used by the NKVD from October 1943 until the end of 1944. It was used from Battalion upwards to Front HQ's."[547]

The R4Z1800 code (which was captured in the summer of 1944)[548] was described by four different people: Corporal Thomas of NAAS 1 (as report no. 29, I 19b); Karl Exter, of NAA 11 (I 55); Lt. Loeffler of Feste 10 (as Annex I to I 19c) and the personnel of NAA 11.[549] It would seem to be the most important, if not the only 4-figure code solved and readable. "RZ 1800 was the general code of NKVD introduced in February, 1944, as successor to RZ 1100. The White Sea Code[550], broken by NAA 11, was an older /1942/ code used from 1943 to the fall of 1944. Then the White Sea Command adopted the RZ 1800

[545] I 26 p 4

[546] I 19c p 13

[547] I 19c p 12

[548] I 106 p 5

[549] I 166 p 5

[550] The White Sea Code was tackled by NAA 11 from April to July 1944, and about 60% of the traffic was solved, almost entirely on higher links. There was a different "key" for each KONA, and by them to their subordinate units, in all 6. Solution was only relative, never basic. I 166 p 6

itself... .It was used on the highest levels, Staff to Regiment and Regiment to Battalion. No addition was ever used with it. The code was still used in September 1944 and possibly in April 1945."[551] Although there were slight discrepancies in the accounts, it can be established that this particular code was alphabetic, and had 50 pages, each consisting of 50 lines-- a total of 2500 groups. The encipherment was carried out by 1) a "chiffrant" and 2) digraphic substitution tables. The "chiffrant" consisted of figures 0-9, in random order printed at the top of the page, (a different order for each page): one figure in this "chiffrant," determined by the 3rd figure of the indicator group, was added to the numbers of the lines on the page before they were enciphered by the digraphic tables.

Ten sets of 2 digraphic tables (each 10 x 10), the sets numbered 0-9, were used to encipher the 2 halves of the 4-figure group; the set number for enciphering the line was the 2nd digit of the indicator group; the set number for the page, the fourth. A series of substitution tables was current for a period of from 2 to 6 months.[552] The first digit of the indicator group was a dummy, and the indicator group itself was inserted in clear in one of the first ten groups of the message.[553]

[551] I 106 p 5

[552] I 19c p 12

[553] I 19c p 13

Though the emphasis was put by the Prisoners of War on 4-figure NKVD codes, it should be pointed out that a great variety of encipherments were worked on, though not all read. Karrenberg (of GdNA) gave the following breakdown of nets and types of codes used:

> Administration networks: usually sent 5-figure messages and, less often, 4-figure and 5-letter messages.
> Frontier networks: used 4-and 5-figure codes: on regimental networks, also 2-figure systems.
> Black Sea Fleet: used 3-figure and 5-figure codes networks from divisional level downward: used 2-figure and 3-figure, plain language and figure messages with plain language.[554]

Corporal Exter (of NAA 11) stated[555] that he worked on 2-figure NKVD ("used up to end of hostilities"); and on 4-figure codes of the NKVD type described by him as RZ4C1800 and codebooks enciphered with an additive. "In this latter type, they had had considerable success with traffic of an NKVD net on the White Sea Front, controlled from the NKVD HQ at Archangel, but that was with a captured basic book and instructions for the system... .They could not cope with 5-figure; that was sent on to Berlin."[556]

In general, certain elements seemed to be constant in all NKVD codes: contrary to regular Army usage, NKVD messages were enciphered on the same system for many months[557] ; NKVD codes were always arranged alphabetically[558]; and all NKVD messages, whether 5-letter or 4-figure or 5-figure, had the date in the penultimate group.[559]

[554] I 173 pp 13-14

[555] I 55 p 11

[556] I 55 p 11

[557] I 167 p 5; I 26 p 4

[558] I 167 p 6

[559] I 173 p 35; I 19c p 13

b) Agents' Codes. Agents' Codes included codes used by agents, guerillas, and "Kundschafter."[560] All types of systems were used, from substitutions, double transpositions, grilles, and subtractors to one-time pads (tape). Solution was always done centrally in Berlin.

"The solution of agent, guerilla, and "Kundschafter" traffic was the responsibility of Referat 3c /of Group IV, GdNA/... .Solution depended mainly on captured material to accomplish solution. Some agent traffic was one-time tape and therefore unbreakable. By and large the Gruppe did not place much value on agent traffic and neglected it."[561]

It should be pointed out that Russian agent systems were not handled exclusively by OKH/GdNA/IV/3c, who really were processing the traffic from the viewpoint of military operations (countermeasures against the partisans, for example). The agent systems were also handled by:

1) The Radio Defense Corps, (Oberkommando der Wehrmacht, Wehrmacht Nachrichtenverbindungen, abbreviated (Amtsgruppe OKW/AgWNV/FU III) who were responsible for locating, eliminating, or neutralizing all enemy agents' radio activities.[562] Preliminary reading, especially when the code was captured, or the system recognized, was done by WNV/FU/III.[563] For more difficult cryptanalysis, traffic was turned over to OKW/Chi, and worked on in the Referat VAUCK.[564] "Dr Vauck and his section used to be with OKW/Chi but were transferred to WNV/FU/III. They continued to be controlled by OKW/Chi and passed their results to them. Vauck was then posted to OKH."[565]

[560] Defined by Dettmann and Samsonov as an agent dropped for a single specific mission, e.g., blowing up a bridge; a Kundschafter was more "localized" whereas the agent was mobile. I 116 p 7

[561] I 116 p 7

[562] IF 176, foreword

[563] IF 176 p 13

[564] See also I 115 p 2

[565] I 21, p 4; cf. also I 115 p 7, par 37-40 and D 60 p 16

2) Some agents' traffic was picked up independently of OKW/WNV/FU (III) by the regular police (Ordnungspolizei, abbreviated ORPO) who sent their traffic to Kurt Sauerbier of Goering's Research Bureau (Forschungsamt, abbreviated FA), Hauptabteilung IV, Referat 9c;[566] this was an entirely independent, personal relationship between the ORPO and Sauerbier.[567] Sauerbier's superior in the FA, Specialist Wenzer, an expert in Agents' Systems, was sent from the FA by WNV/FU/III to assist Lt. Schubert of OKH/GdNA, in January, 1944[568] on Polish Resistance Movement Traffic.

There was, consequently, a certain duplication of effort and a certain amount of confusion as a result of this arrangement.[569] There were also conflicting opinions on the successes achieved. Schubert reported that "Russian agents' systems were tried by Vauck, who said they could not be solved. Later, he said that they were digit substitutions and P/L enciphered with a one-time running key derived from a book."[570] But, in another report, he stated that he could not remember enough about agents' codes to give details which were in many cases not known. In the middle of 1944, for example, the Russians had, he thought, about 3000 agents spread over all areas, and it was impossible to pick out one system and say that it was used in one area. Moreover, he pointed out that he himself had worked only on Partisan and Kundschafter traffic and knew of other systems only indirectly. Nevertheless, in his first interrogation, he stated that Agent's codes were of two types:

1. Double transpositions and grilles
2. Subtractors.

[566] See the whole report of the homework of Sauerbier, I 164

[567] IF 162

[568] I 26 p 7

[569] D 60, pp 19-20

[570] I 21 p 4

"Double transposition was only used by partisans and not by spies." The system was completely unbreakable.[571] He went into more detail about substitution systems.[572] They consist of three elements:

1. The basic cipher (code), i.e., the substitution of the plain text by a substitution system
2. The encipherment by figure subtractor
3. The encipherment of the indicators

The basic cipher: on certain links, a 3- or 4-figure code was used; in general, however, simple substitution systems were employed.[573]

The subtractor: these were of three different kinds:

a. They were printed on teleprinter rolls (the most frequently used and called "Blocknot rulon" by the Russians); the rolls had 5-figure numbers which were given in clear as indicators in Partisan traffic, not in Spy-traffic
b. They were taken from tables. There were 4 basic systems: a simple enciphering with a table of 100-300 groups, used especially in NKGB Leningrad traffic (solved); 100 enciphering pages, used especially in NKGB Leningrad traffic (solved); a double encipherment (table of 30 lines, each line, 10 groups) (solved); a special very complicated mixing procedure (not solved)
c. They were built up from an indicator: simple addition in columns, simple cross addition, addition in column with a key phrase, cross addition with a key phrase, substituted cross addition, subtractor boxes.

[571] I 26 pp 3, 5

[572] In the appendix to I 26, written as a single report on code-systems of the Russian Partisans and Spies (from which report the material given below is taken

[573] For details, see I 26 p 8

The indicator: indicators based on a roll, were always inserted in plain. Apart from a very few exceptions, there were always two indicators. The encipherment could be broken under the following conditions:

a. when both indicators were enciphered in the same systems
b. when there were messages on the same key
c. when indicators consisted of 5 different figures
d. when indicator was known by virtue of the circumstances.[574]

Lt. Schubert also mentioned[575] a third type of encipherment, by occasional simple substitution systems; but he gave no details on the types of substitutions or methods of solution. In conclusion, the interrogator said:

> The above gives the most important cipher used by Russian Partisans and spies, as far as they are known from breaks, captured documents and POW statements. Systems used in the Balkans are not included by they are of a similar type. After the middle of 1944, W/T traffic of the partisans and spies dropped heavily, as they were constantly being overtaken by the advance of the Red Army."[576]

[574] I 26 p 13 Note: on p 5 of the original interrogation, Schubert said of subtractor systems:

> "One could talk a whole day describing these methods. There was in existence a report of over 50 typed pages.... There was rarely enough depth to break these tables."

[575] I 26 appendix

[576] I 26 p 14

VOLUME 4

Chapter VI

Section C. Liaison with other Agencies on Russian Cryptanalysis

57. Liaison with the Signal Intelligence Agency of the Supreme Command of the Armed Forces.-- The liaison between the Signal Intelligence Agency of the Army High Command (OKH/GdNA) and OKW/Chi was close because of the joint derivation of both offices from the Codes and Ciphers Section of the Defense Ministry, and because of the joint and simultaneous control of OKW and OKH signal activities in the person of the Chef HNW and Chef WNV (Chef des Heeresnachrichtenverbindungswesens and Chef des Wehrmachtnachrichtenverbindungsabteilung). A certain amount of jealousy existed on the top levels of signal intelligence operations, and "liaison between specialists was discouraged."[581] Nevertheless, there were specific cases of specialist inter-service cooperation on Russian cryptanalysis.

[581] I 30 p 10

The Russian Referat of In 7/VI, under Lt. Dettmann (and, for a time, under Professor Novopaschenny) which was detached to the Chief, Army Signals Communication Agency (Chef des Heeresnachrichtenverbindungwesen, abbreviated Chef HNW/(HLS)), in Loetzen, had had considerable initial success on a Russian 5-figure code until the spring of 1942. In 1942 /probably April 1, when the Russians introduced a new 5-figure code/ OKW/Chi sent a special Russian "party" to HLS/Ost to collaborate with the OKH cryptanalysts there in the solution of a Russian 5-figure code. Professor Novopaschenny, head of that OKW/Chi party, returned to Berlin in 1943; but the cryptanalysts who had gone with him were absorbed into HLS/Ost and remained there. During 1942-43, Lt. Dettmann (of HLS/Ost) was also passing considerable Russian 5-letter traffic to OKW/Chi in Berlin for solution.[582]

In February 1943, the language department of the Radio Defense Corps (Oberkommando der Wehrmacht, Wehrmachtnachrichtenverbindung, Funkueberwachung, abbreviated OKW/WNV/FU) headed by Fenner, began collaboration on Agents' Codes with OKH/In 7/VI. By the end of March, In 7/VI had given to Fenner's section all agents' traffic intercepted since 1941. Solution was begun, and the results achieved by Fenner were passed on to In 7/VI. Somewhat later, liaison on this particular problem disintegrated, however, since In 7/VI was uncooperative about turning traffic over to Fenner.

There were no other specific examples in TICOM sources of cooperation by OKW/Chi with OKH/GdNA on Russian cryptanalysis. It is known only that OKW/Chi regularly used the IBM machinery of OKH in their cryptanalytic work.[583]

582 I 116 p 2

583 I 96 p 13; I 67 p 2

58. Liaison with the Signal Intelligence Agency of the Air Force High Command.-- Relations between the Signal Intelligence Service of the Air Force High Command (Oberkommando der Luftwaffe Generalnachrichtenfuehrer Abteilung III, abbreviated OKL/Gen Nafu/III) and OKH/GdNA were on the whole good. On a very high level, reports and information were exchanged, and periodic meetings were held to discuss techniques and experience.[584] On an operational level, the 3rd Battalion of Air Signals Regiment 353 (Luftnachrichten Regiment 353, abbreviated LN Regt 353) (on the southern sector of the Russian front) collaborated with KONAs 1 and 8 of the Army Liaison officers were exchanged and evaluation closely coordinated.[585] The German Air Force Signal Intelligence Service often helped fill in the gaps through their work on air armies when the Soviet land army observed radio silence.[586] It should be pointed out in review that the Signal Intelligence Regiments (KONAs) on the Eastern front intercepted and solved a great deal of Russian Air Force Traffic as well as Army and NKVD traffic; and Prisoners of War discussed the cryptanalytic work on Air Force systems not as a special task but as part of their general "army" assignment. Cooperation on cryptanalytic problems was good after 1943; and it can be assumed that the liaison on traffic analysis and evaluation was close and constant.

59. Liaison with the Signal Intelligence Agency of the Navy High Command.-- In its relations with other agencies, the Signal Intelligence Agency of the Navy High Command (Oberkommando der Marine, Seekriegsleitung IV, III, abbreviated OKM/SKL IV/III) maintained a traditional aloofness. There was no statement in TICOM sources of specific cooperation with

[584] I 126 p 14

[585] I 130 p 15

[586] IF 186

OKH/GdNA on Russian cryptanalysis. Lt. Schubert (of OKH/GdNA), who attempted to establish some sort of liaison with the Navy, stated simply:

> "I endeavored to achieve cooperation between the Army and the Navy. This task was actually no concern of mine. A naval officer was detached for six weeks who looked at all Army systems originating in the West and the East and I went to him to attempt some settlement. I tried to achieve collaboration, but later events upset things. There are practically no points of contact between Army and Navy--as regards the Russians."[587]

60. Liaison with Goering's Research Bureau.-- Cryptanalysts of the Signal Intelligence Agency of the Army High Command (OKH/GdNA) were not too well informed on the organization or operations of the cryptanalytic unit of Goering's Research Bureau (Forschungsamt, abbreviated FA). Liaison did exist, however, between the two organizations, and took the form of actual division of tasks, sharing of personnel, and cooperation on IBM developments.[588] Dr. Buggisch stated that (he had heard in 1943) the FA was able to break and read Russian teletype traffic,[589] though he did not know know may details. On another occasion, however, he stated (revealing that there must have been at least a modicum of liaison,[590] "The FA had analysed a Russian cipher teleprinter system in 1943 and recognized that it must have been based on a machine having certain similarities with the German SZ 40. After a short time the Russians altered the system. The FA then communicated its results to my unit and was given as a kind of recompense a report on the solution of a German cipher teleprinter. This was one of the very rare cases where FA and In 7/VI exchanged results."

[587] I 26 p 2

[588] It should be pointed out that Col. Mettig objected to liaison with the FA, however, because of the "SS" taint, and that Dr. Buggisch of GdNA considered liaison with the FA "bad anyway" I 64 p 2

[589] for details see above, Volume 4, Chapter VI, section on machine ciphers

[590] I 176 p 6

The liaison between OKH/GdNA and the FA has already been discussed in this chapter, with reference to the visit of Specialist Wenzel of the FA to OKH/GdNA to help Lt. Schubert on Polish Resistance Movement traffic.

With regard to cooperation on IBM developments, there was no statement about specific Russian cryptanalytic problems in TICOM interrogations. It is known that the Signal Intelligence Agency of the Army High Command took the lead in the development and application of IBM machinery to cryptanalysis, however, and their machinery was made available to other agencies. Tranow (of the Signal Intelligence Agency of the Navy High Command, (OKM/SKL IV/III) stated:

> "About March 1942 we paid a visit, in conjunction with the GAF and the FA, to the OKH Hollerith/IBM/ department in Berlin... ."[591]

Since there was no evidence in TICOM sources of coordinated application of IBM machines to specific Russian cryptanalytic problems, it can only be assumed that such liaison existed.

61. Liaison with the Foreign Office Cryptanalytic Section.-- There was no statement in TICOM interrogations about any liaison between OKH/GdNA and Pers Z S on Russian cryptanalysis.

62. Liaison with the Japanese.-- When asked about liaison with the Japanese on cryptanalytic problems, Dr. Buggisch said he "did not know about OKW--but had never heard of any-- and as for OKH he was sure that there had never been any Japs around in the flesh or any liaison he knew of."[592] Actually, it seems, there was a certain amount of alleged liaison with

[591] I 146 p 17

[592] I 64 p 3

Japan; for, as Dettmann and Samsonov pointed out, "the Russian Referat had been visited at Loetzen in 1942 by two Japanese officers.[593] The Japanese were given a polite reception but shown very little of anything, and no solution work: their tour lasted only three to four hours. The Japanese said they had solved the Russian OKK 6 and OKK 7, otherwise no Russian 5-figure traffic.[594] For all intents and purposes, there was liaison only on paper, certainly no collaboration on solution techniques or exchange of information.

63. Liaison with the Finns.-- Quite the contrary was true in the case of liaison with Finland. "Liaison on all cryptanalytic matters was excellent."[595] The Germans, to begin with, had a very high opinion of Finnish cryptanalysts:[596] "The Finnish crypt personnel were considered outstanding and the exchange was a great benefit to NAA 11."[597]

The main Finnish unit was RTK, "Radio Telegraf Kompanie." It was of battalion strength, with one motorized company and a fixed unit of about 200 men, located at Sortavala. RTK had about 70 cryptanalytic men, mostly officers, headed by Captain of the Reserve, Erkki Pale. It also had evaluation men.[598] The Finns worked largely on Army traffic and had no separate unit for Air Force Signal Intelligence operations.

[593] I 116 p 9

[594] I 116 p 9

[595] I 106 p 3

[596] I 116 p 10

[597] I 106 p 3

[598] I 116 p 10

Lt. Dettmann visited Finland in 1942 and exchanged technical letters from that time on. But the first German liaison officer with the Finns was Captain Marquardt (later head of Group I, GdNA, not a cryptanalyst); he was succeeded by 1st Lt. Riemerschmidt, who was stationed directly at RTK (the Air Force Liaison officer, 1st Lt. Vaatz, was stationed at Finnish HQ's in Mikkeli), and had a direct radio link to NAA 11. In return, the Finns had a liaison officer at Loetzen from 1942, 1st Lt. Mje-Koja (also not a cryptanalyst), who was succeeded by 1st Lt. Ohn; in addition, small Finnish parties visited NAA 11 from time to time.[599]

Results were exchanged between the Finns and NAA 11 every two or three days, and NAA 11 varied its cryptanalytic priorities to give full attention to any special links required by the Finns; in return, information and solution from LNA to Sortavala were sent to NAA 11: "On one occasion (the captured RZ 1800) this was faster than the direct transmission from LNA to NAA11.[600] The Finns solved 3-figure and 4-figure codes extensively, with emphasis on NKVD material. They had no success with 5-figure traffic and "never captured any copies of those codes as far as Schmidt knew."[601] This is, of course, not true: see the section on 5-figure solution (Volume IV, Chapter VI) for an account of Finnish capture and delivery and German exploitation of the Russian 5-figure code book.[602] The Germans sometimes used Finnish equipment and vice versa, but they "gave the Finns much advice..no physical help."[603] And Capt. Schmidt stated that, "NAA 11 never got straight intelligence from the Finns or vice versa. This was characteristic of the general German-Finnish understanding that Lapland was a German area for operations with South Finland allotted to the Finns."[604]

It should be pointed out, in passing, that there was no statement in TICOM interrogations about any liaison whatsoever with Hungary and Italy, German's other allies.

[599] I 116 p 10; I 106 p 3; I 21 p 2
[600] I 106 p 3
[601] I 106 p 3
[602] I 15 p 1
[603] I 106 p 3

VOLUME 4

Chapter VI. Russian Cryptanalysis

Section D. Successes and Failures

64. Successes and failures.-- In their criticism of the defects of the structure of the German Army Signal Intelligence Agency (OKH/GdNA) from the viewpoint of cryptanalysis, Lt. Dettmann and Sgt. Samsonov made five points:[608]

1) the administration, both of the central office and of the subdivisions, had no, or at most a very small specialized knowledge regarding the fields of work... Their effect was...mostly to hinder and not to forward the work.

2) Because the NAAS worked closely with Army Group commands, the NAAS and its technical direction tended to correspond more closely to the desires of the Army HQ's rather than to their own central office.

3) The division of cryptanalysts between the central office and the NAAS had as a result that in addition to an enormous amount of "paper warfare"....work of cryptanalysis and exploitation was carried on with almost complete duplication.

[608] DF 18 part III

4) The multiplication of effort derived also from the erroneous ambition of administrators in individual stations, due to "competition."

5) The most serious interference with the actual work, both in the central office and in all its branches, however, was doubtless brought about by the purely military "manipulation" of this set-up, involving treatment according to rank, not skill or competence; military exercises, field maneuvers, and the like.

They were, of course, not concerned with specific details of the cryptanalytic set-up, but rather the overall organizational and administrative difficulties involved. The contents of their report and of the reports of other Prisoners of War on the technical aspects of cryptanalysis, however, belied any long-range serious effects on the actual functioning of the specific cryptanalytic units, either in the central office or in the field. The only major failure of the German Army vis-a-vis the Russian systems was the failure to solve and read currently the 5-figure codes. Maj. Dr. Rudolf Hentze (head of Group IV of GdNA) spoke of the accomplishments of Dettmann and Samsonov in Referat 3b: "/They/ had good success, especially on the NIVA code, which did not change for a period of two years and therefore could be read almost entirely up to the end of 1944. This was a 5-figure code enciphered.. A new NIVA cane in at the end of 1944 and about 500 groups of this had been recovered by the end of the war."[609] Although he remarked in passing that Referat I of Group IV also "worked on 4- and 5-figure enciphered codes and had partial success working from depths,"[610] he was speaking there of only one specific code. And in spite of Lt. Col. Mettig's two glib statements on the "continucus breaking" of 5-figure codes;[611]

[609] I 113 p 6

[610] I 113 p 5

[611] I 128 p 2; I 111 p 2

and in spite of Dettmann and Samsonov's boast that they always captured the books and could read (although with difficulty), it seems apparent, judging from the total sum of reports from other Prisoners of War, that the 5-figure code was not read currently and that, even if the book had been captured, the encipherment by almost exclusively one-time pads rendered actual solution practically impossible.

On the operational level (i.e., outside of GdNA), it was generally agreed by all Prisoners of War that there was no trouble in reading 2-figure and 3-figure traffic of all sorts, and only a relative difficulty in the case of 4-figure traffic. The solution of the 2-figure and 3-figure codes was simple enough to be carried out on company level; and what was not finished there (either because of lack of time or lack of manpower) was completed on the level of the NAAS which did solution up to and including 4-figure material. A certain amount of difficulty was encountered in address material in agents' codes, but not enough to destroy continuity or to impede the derivation of enough intelligence of a tactical nature for current use.

In the case of NKVD codes, Dettmann and Samsonov claimed that from cryptanalysis they were able to determine the organization, deployment, and general significance of NKVD as a Russian organization; and were able to establish either direct or indirect knowledge of dispositions and changes in dispositions, enemy orders for deployment or attacks, preparations for major operations, supply, ammunition, losses, reinforcements, health and morale of troops, conditions rearwards of lines, the general traffic situation, production capacity of factories, partisan movements, and finally, information on the Polish Resistance Movement.[612]

This is certainly an impressive amount of information to have been derived solely from cryptanalysis, as is the chart made up by Dettmann and Samsonov detailing actual codes read.[613] By comparison to other interrogations, there seems to be a large amount of boasting in their report, giving a clear impression that all the informations was not strictly true as given, at least for cryptanalysis on central office level.

612 DF 18 pp 16-33

613 DF 18 p 75

If one can assume a truthful exposition in those cases where their statements agreed with the statement of other Prisoners of War, however, the amount of cryptanalytic achievement on the part of GdNA (and of HLS Ost) and of the small units on lower levels of operation and solution is still impressive. It must be remembered that other elements than pure cryptanalysis entered into the picture and played a large part in the production of total intelligence:

1) The great amount of Traffic Analysis, Direction Finding analysis carried on in the Eastern front area.[614] Statements of Prisoner's of War indicated that, although 5-figure traffic was not read, it produced, nevertheless, a great amount of intelligence from external characteristics, blocknot series numbers (for disposition of units using series numbers), etc.[615]

2) The generally "low, but improving calibre of Russian transmission," coupled with bad Russian security. As Lt. Starke stated in one place, "although 2-figure traffic was never very difficult to read, much assistance was gained from security breaches on the part of Russian operators.[616] There were scattered references throughout the interrogations to conversations of Russian operators which provided much real information on movements of all kinds. Besides, as Dettmann and Samsonov pointed out in the reference exclusively to NKVD, but by extension to ther systems," the fact alone that NKVD ciphers continued to be used often for more than two years at a time must indicate that the Russians did not believe it possible that the enemy was reading the traffic."[617]

[614] See Chapter V, Vol. V for details

[615] e.g., I 19b report 5 p 14

[616] I 75 p 4

[617] DF 18 p 71

3) Finally, the apparently large amount of capture of both codebooks and tables. The importance of this type of compromise in solution can not be over estimated.

In spite of these considerations, it is still true that the German Army read a tremendous amount of material purely cryptanalytically which, though only rarely of high level operational importance, produced a steady flow of tactical and strategic intelligence. As an example which may or may not be typical, Corporal (Uffz) Althans (of NAAS 1) drew up the following chart showing the estimated monthly average, for the year 1944, of traffic intercepted and solved:[618]

Survey of Successes in Cryptanalysis

Type of Message	Intercepted	Dealt with	%	Remarks
2-figure	140	125	90	
3-figure	6,000	2,600	43	
4-figure	5,000	1,900	38	
mixed	2,350	865	37	
Total	13,500	5,500	41	= degree of
Clear text	6,000	6,000	100	Cryptanalytic
Practice	500	500	100	Success
Grand total	20,000	12,000		
	Plus			
5-figure and				(not studied
NKVD 5-figure	8,000			at KONA 1)
NKVD	2,000			only partially studied at KONA 1
Grand total	30,000			

[618] I 19b report 25 p 44

Dettmann and Samsonov listed the following as systems worked on and solved:[619]

Army and Air Force:

1) Operation systems (carrying text concerning operations and traffic technique)
PT-35, PT-39, PT-41: there was a large volume of messages in the PT systems, which were superseded by "small Codes" in 1944
2) Signal Codes: these were used in the second half of the war and were 3 and 4-figure codes, called CYB or "front" codes. They were partially solved, but completely worked out only in the rarest cases
3) Address Codes: these were used by any unit in the "front" commands; interpretations were hard to make, because of the Russian use of covernames, and it was difficult to solve the encipherments
4) "Conversion" systems: these included codes, code tables and extended substitutions. Among those specifically mentioned were:
The Air Force General Code (1934-37), carrying information on landings, takeoffs, weather, etc.
The BAK-38, the last general Air Force system used to the end of 1939
The Army and Air Force "General Commanders' Code", OKK-5 to OKK-8 (1939-41), and OTSKK-7 ("General Central Commanders' Code"), used in rear areas
All "conversion" systems were considered CYB, or "front" systems
5) Transpositions: pure transpositions were used in the Army and Air Force only for practice traffic
6) Number codes (called by the Germans "cipher-code"): these were 5-figure codes for relaying radio reports of operational or tactical content, direction of troops (on the highest networks). Specifically mentioned were 011-A (19,000 code values in 390 pages), 023-A, 045-A, 062-A, 091-A (23,000 code values in 430 pages), which was used until the capitulation.

[619] DF 18 p 45

All these books were captured; but the encipherment by Blocknots (one-time pads) made solution practically impossible: there was almost complete security in these systems.[620]

NKVD

1) Operational systems: these were used by individual units until 1939, when a general operational system (mono-alphabetic substitution, no description was given) was introduced

2) "Conversion systems": a 4-figure code was used in the Kasakhastan area; three 4-figure codes were in use by 1939; three 4-figure codes were in use at the time of capitulation: ZERNO, NIVA, VIZA; a 5-figure railway code was also in use

3) Transposition systems: these were not used by NKVD, with the exception of one 4-figure code (used in the Arctic Ocean district and on the Finnish-Russian border) which was enciphered by a transposition: it was read currently in part

4) Number series: from 1940 on, a 4-figure code was enciphered by various methods, monographic letter substitution, sliding number sequences, and Blocknots. These were read currently up to the end of the war.

Agents' and Partisans' Systems: these were transpositions (single and double), grilles, and keyword substitutions. (Though there was no statement of cryptanalytic achievement, apparently great difficulty was encountered in solution, and not much success was achieved)

[620] DF 18 p 61

Dettmann and Samsonov concluded their discussion with a chart of German cryptanalytic achievements on Russian systems.[621] The details of which are to be found on chart #1-2 (results of European axis cryptanalytic achievements)[622]

[621] DF 18 p 75

[622] It should be pointed out once again that though Dettmann and Samsonov gave a comprehensive picture of German achievements, they were not to be trusted in every detail. Throughout this chapter it has been shown that composite picture of German achievements in Russian cryptanalysis as derived from the interrogations of other Prisoners of War in many cases did not agree with Dettmann and Samsonov, but would seem to contain more truth.

VOLUME 4

Chapter VII. Miscellaneous Cryptanalysis

Section A. Period from 1919 to 1939

65. German Army Cryptanalytic Effort 1919-1933-- Before 1938, there was no Army High Command and consequently no separate German Army Signal Intelligence Service. The codes-cipher section of the German Defense Ministry which had been maintained in skeleton force since the end of World War I handled the cryptanalytic work on foreign Army systems and any security work done on German Army systems. There is no record of the work done by this section.

66. German Army Cryptanalytic Effort 1933-1939-- In 1933 the newly established Army High Command (Oberkommando des Heeres abbreviated "OKH") set up its own central agency to handle the Army traffic of foreign countries. This central agency known as the Intercept Control Station (Horchleitstelle) was staffed by a few trained cryptanalysts who had been drawn by the Army from the Cipher Section of the German Defense Ministry.[630] Although little is known about the organization of the Intercept Control Station, Major Feichtner of the German Air Force states that it was divided into geographical sections, each section dealing

[630] I 78 p 2

with an individual country.[631] We know that before 1939 there were sections for the traffic of Belguim, Holland, Switzerland, England, and Russia.

67. French systems 1933-1939-- Mettig stated that during the years 1937-1939, continuous and significant successes were obtained by the Intercept Control Station against French Army systems.[632] In the crises of 1937 and 1938, the Germans read the systems used by the French on the wireless net which radiated from Paris to the static French formations within France. These systems, designated by the Germans as F 90 and F 110[633] were described by Dr. Otto Buggisch, one of the leading Army cryptanalysts, as French Army systems based on a four-figure code.[634] In one case, the encipherment was by means of a periodic additive; in the other it was an ordinary transposition, the transposition key being obtained from a key word which itself was taken from the code. Solution, said Buggisch, was obtained by methods generally known in cryptanalytic circles.[635]

68. Belgian systems 1933-1939-- The complete Order of Battle of the Belgian Army was known to the Germans in 1939, at least partly through the reading of Belgian systems.[636] Huettenhain, one of the leading cryptanalysts of the Signal Intelligence Agency of the Supreme Command of the Armed Forces (OKW/Chi), described the Belgian Army system as a 3-figure code used with substitution tables in such a way that the first figure of each group remained unchanged and the second and third were each enciphered individually with types of substitutions that could be varied with each message.[637]

631 IF 181 p 4

632 I 78 p 3

633 I 58 pp 2, 6

634 I 176 p 2

635 I 176 p 2

636 I 78 p 3

637 I 31 p 6

69. Dutch systems 1933-1939-- Mettig states that the Dutch Order of Battle was also available to the German Army at least partly from cryptanalytic achievements.[638] The maneuvers of the Dutch Army in 1937 were covered by the intercept stations of the Army.[639] Very simple techniques, principally double transposition ciphers; were used and these were read by the cryptanalysts of the Intercept Control Station without much difficulty. As a result, Dutch Order of Battle was established down to battalion level.

70. Swiss systems 1933-1939-- Switzerland, Mettig said, was only casually monitored.[640] Nothing is known from TICOM sources concerning the Swiss systems used in this period.

71. British systems 1933-1939-- During the period 1933-1939, the Intercept Control Station had very little success in reading British systems. Mettig attributed this to the very poor quality of the personnel employed on the task.[641] The Order of Battle of the British Army, however, was built up from direction-finding information and the evaluation of call-signs or other radio procedure.[642]

72. Summary of the 1933-1939-- The cryptanalytic effort of the Germans from 1933 to the beginning of the war, 1939, was fairly successful. The Order of Battle of the French, Belgian, and Dutch Armies up to that time was known from cryptanalytic achievements. Only in the case of Britain was cryptanalysis unsuccessful, and here traffic analysis indicated the Order of Battle. Against Germany's feebler opponents, such as Poland, little was necessary, if we may believe Mettig. Mettig stated that the speedy development and completion of the Polish campaign in 1939 made cryptanalytic effort unnecessary, particularly in view of the fact that the Poles, he believed, transmitted their radio traffic in the clear. It was with justifiable confidence in their Signal Intelligence Service that the Germans faced the early years of the war.

[638] I 78 p 3
[639] I 78 p 3
[640] I 78 p 3
[641] I 78 p 3
[642] I 78 p 3

VOLUME 4

Chapter VII. Miscellaneous Cryptanalysis

Section B. Period from 1939-1941

Paragraph

73. German Army Cryptanalytic Effort 1939-1941-- In the early years of the war, the cryptanalytic staff of the Intercept Control Station (Horchleitstelle) was unable to cope with the added burden of the wartime traffic. The British section of the Intercept Control Station was unable to solve British systems;[650] the French section was forced to call upon the Signal Intelligence Agency of the Supreme Command Armed Forces (Oberkommando der Wehrmacht Chiffrier Stelle, abbreviated OKW/Chi) to aid in the solution of French Army systems;[651] and there were not enough cryptanalysts to furnish the forward units with adequate staffs.[652]

The failure of the British section of the Intercept Control Station (Horchleitstelle) to achieve any success with British systems continued. In 1940 the six people comprising the section were moved to Bad Godesberg where no success was achieved despite an abundance of material with which to work.[653] Dr. Buggisch, who in 1942 looked over the files of the British section regarding work on the British high grade machine, Typex, characterized the work of Inspector Breede who worked in the winter of 1939/40 on the British "big machine" as complete nonsense.[654] He stated that Breede described an imaginary machine which had nothing whatever to do with Typex. No cryptanalytic success was recorded in this period. In April 1940, however,

[650] I 78 p 4

[651] D 60 p 4

[652] I 78 p 4

[653] I 78 p 4

[654] I 66 p 2

the British section received a copy of the British War Office Code captured in Norway. A second copy was obtained at Dunkirk.[655] Successes with this system were thereafter possible, since the British continued to use this system until 1943.[656]

The failure of the cryptanalysts of the Intercept Control Station to solve independently the French Army system succeeding the F 110 was another indication of their inadequacy. In early autumn 1939, the French replaced the peace-time systems, F 90 and F 110, with a new war-time system whose name is not known from TICOM sources.[657] The Army cryptanalysts found themselves unable to cope with the situation and called the cryptanalysts of the Signal Intelligence Agency of the Armed Forces, (OKW/Chi) to their aid. Huettenhain, one of the cryptanalysts of OKW/Chi, was sent to the Army Intercept Station at Frankfurt/Main to aid in the solution. Among his papers were two memoranda describing the work he did there.[658] In the memoranda, Huettenhain reported that the task was accomplished, with the aid of his own colleagues of OKW/Chi by October, (1939), so that all the September material could be read retrospectively. The system continued to be worked on successfully through October; and in November, Dr. Huettenhain returned to his own agency, the system solved. It may be noted that the head of the Army station requested Huettenhain to convey the thanks of the Army to the Signal Intelligence Agency of the Supreme Command of the Armed Forces (OKW/Chi) for the assistance given to the Army's cryptanalytic section and remarked that in his opinion such a large cryptanalytic task could not be done by the Army High Command either then or in the near future.

The system was decoded by the Intercept Control Station successfully until the German offensive of the spring of 1940. At this time the French began to use systems in the forward echelons which the cryptanalysts of the Horchleitstelle were unable to solve.[659] Mettig remarked that

[655] I 51 p 2

[656] I 51 p 6

[657] D 60 p 4

[658] D 60 pp 4-5

[659] I 78 p 4

the Army cryptanalysts both of the forward units and of the Intercept Control Station (Horchleitstelle) finally concentrated on two machine systems, the C-36 and the B-211.[660] Neither was solved, however, until after the cessation of hostilities with France. According to Mettig, the final solution of these two machines rated lower than that of the preceding system since it was not timely and was done only with the aid of captured material.[661]

In the winter of 1939, the dearth of field cryptanalysts became apparent to the German Army. When the Signal Intelligence Regiments (KONAs) were preparing to move into the field, the Army found that there were no trained cryptanalysts to send with them.[662] Col. Randewig, the commander of all intercept units in the west, was able to procure a number of cryptanalysts from intercept units around Berlin and filled out that number with mathematicians and linguists. As a result, when the German offensive started in 1940, the Signal Intelligence Regiments had a moderate supply of cryptanalytic personnel; but more were needed to cope with the field problems.

74. Summary of the 1939-1941 Period-- Although the cryptanalytic achievements of the Intercept Control Station (Horchleitstelle) during the years 1939-1941 were minor, their success in intercepting traffic and decoding solvable known systems was of great aid to the German Army. Mettig stated that all messages on the French system which succeeded the F110 were read from late 1939 until the spring of 1940 when the system changed; and that these messages, despite their administrative nature helped to fill in the tactical picture.[663] For example, the strength of units being set up on the training ground at Mourmelon was estimated by statistics of water bottles and blankets. It was possible to deduce facts about the shortage of armor-piercing ammunition with the French infantry units. Similarly, the conversion of the Second and Third French Cavalry Divisions to Armored Divisions in the area northeast of

[660] I 78 p 4

[661] I 128 p 2

[662] I 78 p 4

[663] I 78 p 3

Paris was ascertained in December 1939.[664] By the end of 1939, the complete Order of Battle of the French Army was available to the German Army from the reading of French traffic. The capture of a copy of the British War Office Code in Norway in 1940 (and of another copy at Dunkirk in June of that year) afforded the British section its first successes and furnished a constant and important source of information from that time until 1943, when the British discontinued use of the code.

In this period the Germans realized the inadequacy of their personnel and effort, and set about correcting them.

[664] I 78 p 4

VOLUME 4

Chapter VII. Miscellaneous Cryptanalysis

Section C. Period from 1941 to 1945

75. German Army Cryptanalytic Effort 1941-1944-- The experiences of 1940 showed that considerable expansion in the German Army cryptanalytic effort was desirable. As a result, in the spring of 1941, Major Mang of the German

Army, was ordered to establish a new German Army cryptanalytic and evaluation agency to replace the old Intercept Control Station.[670] The new agency was established as Group VI Inspectorate of 7 (Inspecktion 7 Gruppe VI, abbreviated In 7/VI). Its aim was to increase the cryptanalytic effort in the central office and to train cryptanalytic reserves for field work.[671] A large number of mathematicians and linguists were introduced into the organization and the number of countries covered greatly increased; detachments were sent from In 7/VI to key areas (the Russian section was dispatched to Loetzen to form there the nucleus of the (later) Intercept Control Station East (Horchleitstelle Ost); and cryptanalysts trained in British traffic were sent to Rommel's headquarters in North Africa to the evaluation center of Signal Intelligence Regiment 4 (KONA 4) in Athens, to KONA 5 in Paris, and to Feste 9 (Feste Horchstelle) in Bergen, Norway.

The cryptanalytic work of In 7/VI is described in the following pages according to geographical divisions: western and southwestern cryptanalysis; southeastern cryptanalysis; eastern cryptanalysis. Following these paragraphs the work of the Agents' Section, of the Research Section Linguistic and Mathematical, and of the IBM Section will be discussed.

76. Western and southwestern cryptanalysis, 1941-1944-- Western and southwestern cryptanalysis was handled at In 7/VI by the British section with outposts in North Africa, Athens, Paris, and Bergen, Norway; by the American section; by the French section with subsections for Swiss, Spanish, Portuguese, and Brazilian traffic; and by the Italian section. The field units which handled western and southwestern traffic were the western field units, KONAs 5 and 7. Swedish Army traffic was handled by a special unit of Feste 9 in Norway.

77. Work on British 1941-1944-- During the years 1941-1943, the main success of the British section was the reading of the British War Office Code (WOC), two copies of which had been captured in early 1940.[672] After the capture of these documents, the British section under Inspektor Liedtke was successful in reading messages from

[670] I 78 p 5
[671] I 78 p 5
[672] I 51 p 2

North Africa during the spring of 1941, encoded with WOC and superenciphered with additives.[673] British traffic in WOC was read constantly throughout 1941. In March of that year, a considerable volume of messages was read during the British Cyrenaic offensive of the British Eighth Army under Wavell. The organization of the base services and the Order of Battle of the Army were recognized. During the late summer of 1941, Rommel's counter-attack took place leading to the siege of Tobruk. The besieged fortress was solely dependent on radio for its signal communications to the Eighth Army and Cairo, and as it used the WOC with an enciphering table almost exclusively its traffic was read by the Germans. The British section of In 7/VI followed accurately the British Eighth Army's relief attempts in November 1941 which led to the cutting off of Rommel between Tobruk, Bir Omar and Sollum and, eventually, Rommel's famous break-out to the West at Sidi Rezegh.

As a result of the success with the WOC in Berlin, a special detachment of eight cryptanalysts was sent to the evaluation center of KONA 4 at Athens to solve traffic at that point and thereby reduce the time wasted in sending the traffic back to Berlin. Unfortunately for the Germans, about the time the party started (the middle of December 1941) certain difficulties were encountered in the solution of the War Office Code which prevented the solution of the WOC for the following eight or nine months.[674] During this period the British section suffered a further blow through the capture in July 1942 of the greater part of the Long Range Signal Intelligence Company, FAK 621, which had been operating in North Africa under Seebohm. Although the remnants of the unit continued to operate under a Captain Habel, information gained from the captured part of the unit gave evidence to the British that their code was being read and from that time on the British section had no success with the code.[675] Herzfeld said that after his return to Berlin in October 1942, there was a little WOC traffic but that its volume was too small for successful exploitation.[676] From December 1942 to March 1943, the British used enciphered indicators, and in March and April 1943 changed to one-time pads for enciphering tables.[677]

[673] I 51 pp 16-17

[674] I 51 p 17

[675] I 113 p 4; I 78 p 9

[676] I 51 p 20

[677] I 51 p 20

The British section had no success with these innovations although Liedtke worked for a year attempting to break into the new system.[678]

From 1942 to the end of the war, the only success attained was with British low-level traffic, particularly Slidex. Slidex was designated by the Germans as English Code (Englische Code abbreviated "EC") followed by a number to denote the variations of the basic system. Slidex was used by the British and later by the American and Canadian Army in front line units and in air support networks (tentacles). The variations of the EC system mentioned in TICOM sources are: EC 5, 12, 23, 24, 25, 30/3, and 30/20.[679]

EC 5 is described by Graupe of In 7/VI as a system in which the code values are written in alphabetical order in the columns of a rectangle 25 x 25.[680] The code groups are represented in the cipher text by the digraphic coordinates and sent in 5 letter groups. Intercepted Slidex was principally practice traffic in the United Kingdom during the period 1942-1943[681] and was solved by the British section of In 7/VI which then forwarded the material to the training section of In 7/VI for instruction purposes.[682]

In EC 12, the successor of EC 5, the code group of two letters derived from the coordinates was enciphered by a group of four figures and sent in 5 figure groups. The traffic in this code appeared in North Africa in 1942-43 and was of tactical value for operations in that area.[683] It was solved at In 7/VI and was decoded easily in most of the field units of KONA 5 and 7.

[678] IF 107 p 7

[679] IF 120 p 3

[680] IF 107 p 3

[681] IF 120 p 3

[682] IF 107 p 3

[683] IF 120 p 3

EC 23, 24, 25 were developments of the basic EC series. The systems are not described in detail in TICOM sources. The traffic originated mainly from the United Kingdom and was used from November 1943 until the time of the invasion in June 1944. Traffic in these systems was intercepted by Feste 9 in Norway and units of KONA 5 in France. The evaluation center of KONA 5 at St. Germain is said to have succeeded in reconstructing all the cards used in systems 23 and 24. Feste 9 succeeded in this only once after two days' work, and then with the help of a message of 190 digraphs. System 25 was recognized but seldom intercepted.[684]

EC 30/3 was a variation of the EC series intended to be used specifically for the Invasion and thereafter.[685] It had, however, been used by air liaison links in the United Kingdom during May 1944, and had already been reconstructed by Feste 9 by the time the invasion occurred on 6 June, 1944. The reconstruction of this code allowed the Germans at once to discover the order of battle of the invading armies at Corps level. The evaluation center of KONA 5 at St. Germain took over the work of intercepting and decoding this traffic during the summer and fall of 1944; at which time the system was currently and easily solved by units of KONA 5 and later those of KONA 6 with the aid of captured tables. Traffic in this system is said to have been solved so quickly that it could be handled like plain text.[686]

EC 30/20 was a variation of the EC system reconstructed by KONA 7 in Italy. Traffic was originated by supply units of the British Eighth Army and was currently solved until the end of September, 1944 when the traffic was replaced by a four-figure type which was not broken.[687]

After D-day, Slidex was also used by the American Army.[688] When the Germans found that the American MP units were using Slidex to report all Army units which passed their control points, the deciphering of Slidex was given high priority.[689] Graupe stated that Slidex messages were also particularly valuable for identifying bombing and

[684] IF 144 p 2
[685] IF 120 p 3
[686] I 109 p 38
[687] IF 120 p 3
[688] I 113 p 3
[689] I 80 p 3

artillery objectives.[690] The time estimated for the solution of Slidex was one to three hours if the basic cards were at hand, five to six hours if they were not. Sixty-five percent of the work is said to have been done with the cards available.[691]

Not much material concerning other British low-grade systems solved can be found in TICOM sources. Hentze of KONA 5 said that Maplay was worked on throughout 1944, but that the volume was low and the Germans found this system harder to break than Slidex. They were successful only with a great deal of traffic or with a re-encodement from Slidex which had provided the original break.[692] Codex was solved by the Germans largely with the help of a captured specimen which had been in the possession of the Germans since the days of the Leros Invasion.[693] It was read by Feste 9 in 1944-45, when that unit was in Italy. A Tiger-code (so-called from its use during the "Tiger" pre-invasion exercises in England) was solved by the Germans after a half year of work.[694] Solution was made possible by a long report in a British paper giving the names of units, officers, etc. Another British system, the '999', which was used during the pre-invasion period, was solved by the Germans; but it was never used operationally.[695] KONA 5 is said to have had considerable success with the Tiger Code and to have achieved solution on the fourth or fifth day after its regular monthly changes.[696] Matin, another British Army system, was never solved. Hentze says that the Germans arrived at the decision that Matin was a small machine, but he does not say whether research on this system was carried on at In 7/VI or in KONA 5.[697]

690 IF 107 p 8
691 I 80 p 3
692 I 113 p 4
693 IF 120 p 4
694 I 76 p 13
695 I 113 p 4
696 I 113 p 4
697 I 113 p 4

The outstanding failure of the British section of In 7/VI, and of In 7/VI in general, was the failure to solve the British 'big machine', Typex. Mettig stated that had the Germans of In 7/VI had been able to solve this system, it would have been their outstanding achievement.[698] At a previous interrogation, Mettig had stated that Typex was read in 1942 in North Africa and that success continued until the autumn of 1942 from which time In 7/VI had no more success with the system.[699] This fact, coupled with some some information from Ultra sources to the effect that FAK 621 in North Africa had been reading Typex at the time of its capture in North Africa in July and November 1942, brought about a thorough investigation of this subject by the interrogators.[700] The story in brief was that in June 1943 one of the prisoners of Bode claimed that he had worked on British machine methods from 1937 to 1940 and that messages which could not be decoded by FAK 621 in North Africa were sent to In 7/VI at Berlin. Two other prisoners from FAK 621, Haunhorst and Possel, stated that all high grade traffic was handled by a Warrant Officer Wagner, and that this man had at his disposal one or more British Typex machines captured at Tobruk. They described the machine as resembling a German Enigma machine with a special type of adjustable keyboard. They said also that certain documents were used in the solution of the settings, either captured British cipher documents or machine settings compiled by In 7/VI at Berlin from three or four years of traffic. No further information was gained concerning this incident during the war since other officers refused to give information and Warrant Officer Wagner was never identified. This 1943 evidence was contradicted by the statements made after the war by highly placed german cryptanalysts. Drs. Huettenhain and Fricke of the Signal Intelligence Service of the Armed Forces (OKW/Chi), and Mettig, emphatically denied having solved or heard of a solution of Typex. They had never seen a Typex machine

[698] I 128 p 2

[699] I 48 p 3

[700] I 161

with rotors although all admitted that a Typex machine without rotors had been captured at Dunkirk. The TICOM interrogators of Dr. Huettenhain and Fricke reported:

> "Should it turn out that some of the experts named above [i. e. Mettig] were in possession of a complete Typex machine and have achieved successes, both these POW's [Huettenhain and Fricke] would lose their last faith in their fellow beings."[701]

Mettig, moreover, stated categorically that a success of this nature would have been mentioned in the list of German cryptographic successes which was drawn up for him prior to his visit to Supreme Headquarters Allied Expeditionary Forces with the liaison commission of the Supreme Command of the Armed Forces (OKW).[702] Mettig's former statement that Typex was read in 1942 in North Africa and that success continued until the autumn of 1942 (from which time In 7/VI had no more success with the traffic) may have been a misstatement for Slidex. At least, the interrogators assumed that Huettenhain, Fricke, and Mettig in their last interrogation were speaking the truth.

Although it is almost certain that In 7/VI never solved Typex, a great deal of effort was expended on the project from 1940 to 1943. In January 1942 the files of the work on Typex done up to that time at In 7/VI were turned over to Buggisch who found work dating back to 1940,[703] when Inspector Breede of the British section had attempted to solve the system. Breede recognized the traffic as machine traffic but described a purely imaginary machine which Buggisch says had no relation to Typex, and was complete nonsense. In 1941 some mathematical studies were made on Typex; and in January 1942, Buggisch made a study of the system, from which he made the following conclusions:

a. the system was similar to that of the Enigma, according to single letter frequency counts based on 10,000 cipher letters
b. certain relationships between two message-settings frequently existed

[701] I 161 p 6

[702] I 161 p 7

[703] I 66 p 2

There is no evidence that Buggisch proceeded further than this in his investigation. He stated that a Typex machine without rotors was captured during the French campaign near Dunkirk and that some documents taken from an English security officer pointed out frequent breaches in the strict regulation that rotors of the Typex machine should be turned at random after a message was enciphered.[704] There seems to have been no knowledge of how many rotors the Typex machine had; Buggisch vaguely remembered having read that there were twenty-five.[705] He also stated that casual consideration was given to whether or not one might be able to tackle the problem of breaking (if one knew the inner wiring of the wheels). Since no one at In 7/VI knew either the wiring of the wheels or how many wheels there were, the question was of no practical interest. The whole matter was evidently permanently abandoned sometime in 1943.

Mention should also be made of the solution in KONA 4 of British traffic emanating from the Transjordan Frontier Force which gave valuable information concerning British troop movements in the Middle East. An intercepted (and decoded) message from the Transjordan Frontier Force indicated which units of the Ninth Army were being moved to Egypt to counter Rommel's threat to Alexandria. Even when this code was changed in July 1942, solution proceeded regularly after a few hours' work.[706]

In summary, one may state that the British section was able to give intelligence concerning the movements of enemy forces from the solution and constant decoding of such low-level traffic as Slidex, Codex, Maplay, 999, and the Tiger Code. During the early part of the war the solution of the enciphering tables used to encipher the British War Office Code made possible current decoding which furnished an excellent source of information; during the later years Slidex decodes were the main source. With Typex, no success was attained, and all efforts at solution were abandoned in 1943.

[704] I 61 p 3

[705] I 61 p 3

[706] IF 190B p 7

78. Work on USA traffic 1941-1944-- The USA section of In 7/VI was created with the entry of the United States into the war in early December 1941.[707] The section, made up of personnel who had been drafted from the mathematical section of In 7/VI, was placed under the leadership of Steinberg, a leading mathematician. Initial attempts at breaking USA traffic were fraught with difficulties. Because of the size of the USA wireless network and the use of alternative frequencies by USA operators, considerable trouble was experienced in identifying the various links and sorting the different systems. After a few weeks, however, order was established through the reading of call signs and the sorting by discriminants.[708]

The first major success of the USA section was in the summer of 1942 when the M-94 was solved.[709] The Germans designated the M-94 variously as URSAL, CDAF, strip, and ACr2. URSAL was a name given to the system from the fact that traffic from the USA weather stations in Greenland which used URSAL as an indicator provided the first breaks into the system.[710] CDAF was found in the traffic emanating from the Caribbean Defense Area.[711] "Strip" and "ACr2" (Amerikanischer Caesar 2) stem from the fact that this system was long thought to be a strip system.[712] The solution of the M-94 was achieved by Steinberg and Luzius, mathematicians of the USA section, who are said to have written a twenty-five page report on their work. After the solution had been achieved cryptanalytically, a USA manual (FM 11-5) with a complete description of the M-94 was found in a Berlin library.[713]

Current solution of the M-94 from 1942 to 1943 was done both at In 7/VI and at the Signal Intelligence Evaluation Center of KONA 5 at St. Germain. The work consisted of finding the daily key. A set of 25 charts (synoptic tables) corresponding to the 25 discs of the machine was constructed, apparently similar to the "synoptic tables" used by American cryptanalysts. The daily key was found by assuming a beginning, and using the charts to discover possible disc arrangements. Later IBM was used to eliminate

[707] I 78 p 10
[708] I 78 p 10
[709] I 113 p 3
[710] I 142 p 2
[711] IF 107 p 4
[712] I 142 p 2
[713] I 142 p 2

"impossible" charts. Graupe of NAAS 5 stated that it usually took two days to recover the order of the discs and that only fifty groups were required for the system to be broken.[714] This solution time seems exceptionally long, as American security studies have shown. Solution of the M-94 usually takes only a few hours. Estimates on the amount of material solved range from 70% to 90%.

The M-94 was succeeded in 1943 by the M-209, which was first solved by the Germans in the autumn of 1943.[715] and continued to be solved with some success throughout the remaining years of the war. Solution was achieved in In 7/VI by Steinberg and Luzius, who were aided by the knowledge that the US government had bought the Hagelin machine which had once been offered to the German government.[716] At first only relative settings could be recovered,[717] but later the section refined its technique of recovering absolute settings so that not only paired messages but in a large number of cases a whole day's traffic could be read. The technique of achieving true settings was passed on by In 7/VI to the Navy and the Luftwaffe.[718]

Work on an operational level was carried on jointly by the USA section of In 7/VI and NAAS 5 at St. Germain. Early in 1944, NAAS 5 had been supplied with a group of cryptanalysts skilled in work on the M-209; and this small group headed by Engelhardt competed with the section at In 7/VI in the quick solution of M-209 traffic.[719] It is estimated that 10-20% of all M-209 messages intercepted were read by establishing the true settings of the wheels, and that about half of these settings were established at In 7/VI, half at NAAS 5.[720] To insure speedy

[714] IF 107 p 4; I 113 p 3
[715] IF 107 p 5
[716] I 80 p 3
[717] I 113 p 3; I 142 p 3
[718] I 144 p 2
[719] I 142 p 2
[720] IF 153 p 1

solution all units subordinated to KONA 5 were ordered to teleprint to NAAS 5 all messages on the smae setting or with indicators differing only in the first two letters.[721] In addition, copies of all intercepts were sent to In 7/VI as well as to NAAS 5 in an effort to obtain all possible solutions.[722] Under the most favorable circumstances two days were needed to solve a depth, and two more days to reconstruct the absolute settings.[723] There were times, however, when captured lists of keys or settings made possible a quick solution of the traffic. During the campaigns of Sicily and Italy, messages of great tactical value were decoded using captured booklets containing M-209 settings.[724] At the time of the invasion of Normandy, the M-209 keys of the 82nd and 101st Airborne Divisions which covered the critical days of June 6, 7, 8, 9, 10, 11 were captured and all traffic on those days was read.[725]

The Germans of In 7/VI knew of the existence of a 'big American machine' which was designated the AM 1 (Amerikanische Maschine 1); but it is quite clear that In 7/VI never solved this machine and had no idea about its construction.[726] Hentze of KONA 5 says that his unit never succeeded in getting a model of the machine.[727] Keller's remark that the American machine cipher was tackled in Berlin with approximately 2% success and that the conclusion that it was not worth the trouble is without doubt utter nonsense.[728]

The Germans were successful with American codes. One code of no strategic value, a United States Army Administrative Code, designated by the Germans as AC 1 (Amerikanischer Code 1) had been captured before 1939, and photostatic copies of the code had been distributed to all field cryptanalytic units.[729]

[721] I 113 pp 11-12

[722] IF 107 p 6

[723] IF 107 p 6

[724] IF 107 p 5; IF 153 p 1

[725] IF 153 p 1

[726] IF 153 p 2

[727] I 113 p 4

[728] I 74 p 3

[729] IF 153 p 2; IF 105 p 5

The code was a-5 letter code with 60,000 groups, each page containing 90 groups.[730] Feste 9, while it was in Norway, intercepted and read traffic passed in this code from the summer of 1942 to the autumn of 1943.[731] Although no traffic of strategic value was passed, the intelligence was valuable enough so that when AC 1 was succeeded by a simplified version designated as TELWA (USA: SIGARM) Feste 9 took pains to reconstruct the code with the help of AC 1.[732]

Feste 9, aided to some extent in more difficult solution by the USA section of In 7/VI, also broke the simple codes used by US Army units stationed in Iceland and the Caribbean. These were designated as Division Field Code (DFC) followed by a number indicating the variation of the system. The variations described in TICOM sources were: DFC 15, 16, 17, 21, 25, 28, and 29.[733]

a. DFC 15: a 4 letter code, two-part, with variants and nulls. The system was used by the US Army in Iceland during the autumn of 1942 and was solved in January 1943 by Feste 9 in Norway by assuming clear routine messages with a basis of encoded text such as Daily Shipping Report, Weather Forecast etc.

b. DFC 16: a 4 letter code enciphered by means of daily changing letter conversion tables. The system was used by stations inside Iceland and on the Iceland-Washington link for one month only, probably November 1942. DFC 16 was solved in January 1943 by In 7/VI. The solution was given to Feste 9 which thereafter succeeded in reading 80% of the traffic intercepted.

c. DFC 17: similar to DFC 16 but with different code equivalents for certain clear letters, words, abbreviations etc. The system was used in Iceland and also from USAAF links in Central America and in the Caribbean Area in February and March of 1943. With the aid of a captured DFC 16 code, Feste 9 broke and read nearly 100% of DFC 17 traffic.

730 IF 120 p 4

731 IF 120 p 4

732 IF 120 p 5

733 IF 120 p 4; IF 144 pp 3-5

d. DFC 18: Similar to DFC 17, and this system was current in April, May, and June of 1943 with a decline in the volume of traffic in Iceland. It was broken by Feste 9 with the aid of experience gathered in the solution of DFC 17.

e. DFC 21: Similar to DFC 17 and 18, this system was current in July 1943. It was broken and read by Feste 9 with the aid of routine administrative messages.

f. DFC 25: Current only in the Caribbean Sea Area from August to November 1943, this system was intercepted by Feste 3 at Euskirchen but the traffic was handed over to Feste 9 for solution. The system was read only in part because the letters and figures which presumably meant types and makes of aircraft made book reconstruction very difficult and the intelligence was not of interest to the Army.

g. DFC 28: A training code used in the south of England, from December 1943 to March 1944, was intercepted by Feste 9. A noticeable rise in the standard of encoding occurred in comparison with the messages intercepted from Iceland. Traffic in this code was of no intelligence interest.

h. DFC 29: a copy of this book was captured in the autumn of 1943 but it was never used.

Mention should also be made of the success of the USA section of In 7/VI with the Air Transport Code used for air cargo and passenger transport circuits to Africa and South America.[734] This code, consisting of two-figure elements from 00-99, was successfully decoded by In 7/VI from May 1942 until early 1943 when it was given to the German Air Force.

[734] IF 153 p 2

The work of In 7/VI, USA section, appears to have been successful in low-grade ciphers and in some medium grade ciphers such as M-94 and M-209. Mettig rated the solution of the M-209 as the outstanding achievement of this section and one of the best of In 7/VI. It is clear also from references concerning the work on this system made by members of other agencies such as Tranow, chief cryptanalyst of the Navy, and Voegele, chief cryptanalyst of the German Air Force, that the USA section of In 7/VI evolved the best techniques of solving the M-209 and led the other German Signal Intelligence Agencies in the work on this system.

79. Work on French traffic 1941-1944-- French traffic from 1941-1944 was of two main types, Vichy French and Free French. Vichy French traffic which was under the direct control of the French Armistice Commission at Wiesbaden was monitored by the French section of In 7/VI.[735] By agreement with the Vichy government, the French were to inform the Germans of their code and cipher procedures, but wary watch was kept on their traffic. The work on Free French traffic which emanated during this period from Free French troops in Syria and in North, West, and Equatorial Africa was carried on by In 7/VI and the Signal Intelligence Evaluation Center of KONA 4 at Athens where the traffic was easily intercepted.

In a list compiled by Juehn, head of the French section of In 7/VI, of the Free French systems worked on by In 7/VI and NAAS 4, the following systems are mentioned as being used in Syria:[736]

a. a 3-letter system: code table with fortnightly key change. This system appeared from about 1942 to the middle of 1944 in Syria but was not intercepted after this. Content is described as moderate to good.
b. a variant of the above code which passed technical details of wireless traffic.
c. police systems which appeared, according to Kuehn, rarely: either 2/F substitution tables or simple transpositions.

[735] I 78 p 9

[736] I 160 p 6

d. a 4/F code with daily key change. Appeared in 1944 in the Syrian coastal network. Content described ship movements in the coastal area.

From other sources may be added the de Gaullist systems, two of which are named: Control Bedouin and Service Politique.[737] The work on French systems used in Syria was summarized by Winkler and Loeckher, two members of KONA 4: "All Syrian traffic was read and a complete picture obtained of the French armed forces."[738]

Among the Free French systems from North Africa which were solved and read by In 7/VI and KONA 4, Kuehn listed:[739]

a. 5 letter messages from a diagonal transposition system, with monthly, later semi-monthly changes, used in West Africa from 1943 to 1945. It was later discovered from a captured document that this system had been used in World War I, and was resurrected evidently for use in West Africa.
b. TTSF code. A 4 latter code reciphered by letter substitution into 4 letter cipher text. The first group of the message is always TTSF; the last group the indicator. The code was used in North Africa from 1944-1945 for routine messages.
c. 5 letter messages from a diagonal transposition used in Equatorial Africa in 1943-1944.
d. 5 figure messages from a 4 figure hatted code, designated ATM 43. Kuehn of In 7/VI notes that ATM 43 derived its name from the fact that it was possible to use the vocabulary of the pre-war French Code, the ATM, in the reconstruction of this code.
e. 3 figure messages from a 4 figure code with subtractor. This system was used in North Africa in 1944 for transport work.

A 5 figure de Gaulle code was used in North, West, and Equatorial Africa, and later in France, which had not been solved by the end of the war despite efforts made by In 7/VI since

[737] I 74 p 2
[738] I 170 p 2
[739] I 160 p 6

1941/2.[740] Buggisch stated that in 1941/2 he worked on this code with Kunze, one of the chief cryptanalysts of the Foreign Office.[741] Despite these efforts, no success was attained until compromise revealed that the code was transposed with daily changing key. No further headway appears to have been made with this system.

The French section of In 7/VI, it will be recalled, had solved the C-36 and the B-211 after the French campaign in 1940. When, therefore, the de Gaullist troops in North Africa and Corsica began to use the C-36 machine for their traffic, the French section already had a solution and it was easily solved during 1943. Even when a new indicator system based on numbers was introduced in early 1944, a high percentage of the traffic continued to be solved through the use of cribs and statistics. The indicator system itself was broken in the autumn of 1944.[742]

At the end of his paper on the French systems treated by the French section of In 7/VI and KONA 4, Kuehn made it clear that the French section was greatly aided by certain fundamental weaknesses in French cryptography which led to easy solutions of most of their systems. These weaknesses, he described as:[743]

a. "the extraordinary conservatism of the French regarding the construction of their code systems or reciphering methods. Systems which must have been used in the first World War were, for instance, used in a slightly modified form up to 1945 in West Africa. Reciphering methods are regularly of two types: either subtraction with finite subtractors or transposition with keywords taken from the code."
b. "the habitual use by the French of stereotyped message beginnings and endings which facilitates breaking into the systems."

[740] I 160 p 7

[741] I 58 p 6

[742] I 92 p 3

[743] I 160 p 22

c. "the idiosyncrasy of the French of communicating cipher matters or key changes by radio. For instance, through the diagonal system in West Africa In 7/VI was able on several occasions to break the key for C 36 machine and once a key change for the ATM 43 code was announced."

With these weaknesses, it was possible for the French section to read all or most of Free French traffic during the years 1941-1944. Their previous experience with the C-36 and B-211 provided them with solutions to this machine traffic as it was used by de Gaulle. No high grade traffic appears to have been passed by the French during this period.

80. Work on Swiss, Spanish, Portuguese, Brazilian traffic-- From 1941-1944, the French section of In 7/VI had subsections for Swiss, Spanish, Portuguese, and Brazilian traffic. As Kuehn stated, however, the volume of traffic was always extremely small and unimportant.[744]

Buggisch, one of the chief cryptanalysts of In 7/VI, worked with Kunze of the Foreign Office on the solution of the Swiss Enigma (the Commercial Enigma);[745] although they worked out a theoretical solution of the machine, the theory was never applied at In 7/VI to Swiss traffic because the volume did not warrant the effort.[746] Moreover, easy solution of the traffic was precluded by the fact that the Swiss did their own wiring of the Enigma wheels and changed these frequently.[747]

Monitoring of Spanish, Portuguese, and Brazilian traffic was coordinated by the French section of In 7/VI [748] and was carried out by various field signal intelligence units: from 1939-1942, by Feste 3; from 1942 to 1944, by FAK 624, and from

[744] I 160 p 3

[745] I 58 p 5

[746] I 176 p 3

[747] I 84 p 3

[748] I 78 p 10

1944 by FAK 624 and Feste 12. The amount of traffic read in these units was evidently small enough to be handled satisfactorily by the personnel stationed there. Graupe stated that Spanish military transpositions and also a Spanish digit system with variants were read. Of seven Brazilian systems known, five were read. Most of the systems were used between Brazil and the United States and were signed by Ciudada.[749]

81. Work on Italian traffic 1941-1944-- From the beginning of the war, the security of Italian systems was a matter of constant concern to the Germans. An Italian section under Captain Dr. Fiala was set up in In 7/VI to check the security of Italian traffic, particularly from Italy to North Africa. The Germans feared that troop movements of the German Army to North Africa were being betrayed by the insecurity of the Italian systems.[750]

As early as 1941, Dr. Fiala paid a visit to Rome to notify the Italians of the weaknesses of their systems and to request greater security.[751] The visit, however, made little impression on the Italians who remained confident of their own systems.[752] An attempt to improve Italian security as well as to demonstrate the use of IBM machinery for cryptanalysis probably lay behind the German invitation in 1942 for an Italian cryptanalyst to visit the IBM section of In 7/VI.[753] Captain Bigi, one of the cryptanalysts of the Italian Army, was sent but his report did not result in any changes in Italian cryptography. Captain Bigi's next visit to Berlin met only with coldness on the part of In 7/VI.[754] By late 1942, the general impression among the Germans was that the Italians were incapable of improving their own systems, even with Germans monitoring them,[755] and the Italian section of In 7/VI was disbanded in 1942 by order of Hitler.[756]

[749] IF 107 p 3
[750] I 78 p 11
[751] I 78 p 11
[752] IF 1524; IF 1519
[753] I 78 p 11
[754] IF 1517
[755] I 78 p 11
[756] I 100 p 2

In June 1943, however, with Italy's defection (from German viewpoint) to the Allies, work on Italian traffic was again started at In 7/VI.[757] The section in 1943 consisted only of the section head, Manaigo, and a small number of assistants. Herzfeld, who was transferred to the section in July, gave an account of the work of this section until November 1943 when it was again dissolved, this time by Major Lechner, head of In 7/VI.[758] The decision to disband the section the second time was justified by the fact that after the fall of Leros, no more Italian wireless messages could be intercepted and there was no traffic with which to continue work. The Germans assumed that the Allies had prohibited further Italian wireless transmissions.

During its brief existence from July to November 1943, the Italian section worked on two codes, the Ellade and Piave, which were being used by the Italians in that period. Great help in the solution of these codes was given by an Italian enciphering table which had been captured by some German Officers in Athens under dramatic circumstances.[759] With the aid of this and other captured cipher material from northern Italy, two codes, Ellade and Piave, were identified and their reciphering tables reconstructed. Later the Piave code with enciphering table and many messages were captured from northern Italy. Traffic was read on the Piave code. The Ellade code was partly reconstructed when the section was dissolved from lack of current traffic.

[757] I 100 p 2

[758] I 100 pp 2-4

[759] When the news of Mussolini's arrest and the Italian armistice was received at the headquarters of KONA 4 in Athens, two German officers drove to the headquarters of the Italians in Odos Amerikis, Athens, walked into the Italian code office, and began to collect the material lying on the tables and to pack it into a case in front of the bewildered Italians. In the midst of this, a number of Italian officers came in and began shouting rather excitedly. After some controversy, the Germans thought it preferable to disappear quietly since the attitude of the Italians became too threatening. They did, however, carry with them what they had collected from the tables and sent it to the Italian section in Berlin.

We know that at the end of the war, KONA 7 in Italy was ordered to cover the traffic of Italian bands in northern Italy, but how much traffic was read or of what the traffic consisted is not known.

82. Work on Swedish traffic 1941-1944-- Work on Swedish Army traffic from 1941 to 1944 was handled by a special detachment of Feste 9 called Out Station Halden (Aussenstelle Halden) from the fact that is located in Halden. For administrative purposes the station was attached to the Halden Police.[760] The best account of the systems worked on is found in a report by Bartel, a German cryptanalyst who had formerly worked on these systems.[761] According to Bartel the following Swedish Army systems were worked on:

a. SRA 1, SRA 5: a revolving grille system. Numerous cases of compromises occurred and the system was continuously read. First broken in the spring or summer of 1943.
b. HGA grille: a more difficult system not read by NAA 11 or Feste 9 in Norway. Worked on by the German Foreign Office but without success.
c. SC 2: read in May 1943. A simple field code like Slidex.
d. SC 3:read in April 1943. Simple, partly alphabetical, 3-letter field code without reciphering.
e. SC 4: read in June 1943. 3-letter alphabetical code without recipher.

The first Swedish cipher machine (Schwedische Maschine 1,abbreviated SM 1), was worked on in Norway in 1944 and was identified as a small Hagelin like the M-209.[762] Messages were read at Halden with crib, by errors in the cryptography, or by having two messages in the same key. The second machine (SM 2) was thought to be a "large Hagelin" machine. Two copies of the traffic on this machine were made, one for In 7/VI, one for the station at Halden.[763] Friedrich, a member of the station at Halden, thinks that some SM 2 traffic was read.[764] The intelligence gained from the breaking of traffic of SM 1 and the simple field codes allowed the Germans to build up a complete tactical picture of the Swedish Army

[760] I 55 p 9
[761] IF 120 p 5
[762] I 142 p 4
[763] IF 149 p 2
[764] IF 149 p 2

during the late years of the war, but neither the high grade grille, HCA, nor the large Swedish machine was solved.[765]

83. Work on Southeastern traffic 1941-1944---Southeastern cryptanalysis was handled at In 7/VI by the Balkan section under the leadership of Bailovic and in the field by KONA 4. KONA 4 had been stationed in the Balkan area during the entire period of the war, and in addition to its regular task of intercepting the traffic emanating from Syria and North Africa, it had been given the task of monitoring the traffic of the occupied countries in the Balkan area. The Balkan countries whose systems were worked on by In 7/VI and KONA 4 were: Greece, Hungary, Romania, Yugoslavia, Albania, Turkey, and Bulgaria. The work done on the traffic of each of these countries is given below.

84. Work on Greek traffic 1941-1944-- Nearly all of our information concerning Greek systems comes from a report on Greek systems by Dr. Otto Karl Winkler who was a translator and cryptanalyst with KONA 4 from the spring of 1941 to May 1945.[766]

According to Dr. Winkler, work on Greek systems started in 1941 when KONA 4 was stationed in Bucharest. The first system broken was a Greek Air Force system which consisted of a single transposition sent in 3-letter groups. Dr. Winkler stated that nearly all messages were read by the use of stereotyped beginnings. Although the messages were of insignificant value, a continuous check on officer personalities, deliveries of stores and information concerning airfields contributed to tactical knowledge of the Greek forces.

KONA 4 worked at this time also on Greek Army and Navy messages, but without success until the conquest of Greece. At that time, Winkler stated, 'Codes' were captured which were used by the Greeks during the attack on Crete.[767]

[765] I 55 p 9

[766] I 70

[767] I 170 p 2

The only other Greek system mentioned as having been attacked in 1941 was a 5-letter code with a cyclic recipherment which Buggisch says he worked on at In 7/VI. Solutions were becoming rapid when the Greek campaign ended.[768]

After KONA 4 moved its Evaluation Center to Athens in May 1941, no more work was done by KONA 4 on Greek systems until the withdrawal of NAAS 4 from Athens in the autumn of 1943. At this time Greek Partisan traffic began to be intercepted. In the spring of 1944, KONA 4 gave Winkler the task of forming a small Greek unit to handle traffic of the Greek People's Army of Liberation ("ELAS"). The unit consisted of six persons, chief among whom were one Strobl, a cryptanalyst who worked on and solved a double transposition system of ELAS while Winkler concentrated on translating the traffic already readable. The work became more important and the unit, now increased to sixteen persons, was attached to a Close Range Signal Intelligence Platoon, NAZ G, newly formed in Salonika to cover wireless and line traffic of the Greek Partisans.

Winkler stated that in the beginning the Greeks sent their traffic in two figure substitution with alternative groups.[769] As few messages were sent on the same substitution, it took several days to break and read these substitutions. ELAS soon went over exclusively to letter traffic based on double transposition, which Strobl successfully solved largely through the aid given by the carelessness of the Greek cryptographers.

Winkler estimated that 50-60% of the traffic tackled by NAZ G was solved. From these messages, the unit was able to build up an almost complete picture of the organization and composition of the Greek People's Army of Liberation (ELAS) and the National Liberty Front ("EAM"). It also compiled lists of leading Greek personalities and officers and informed the competent German political and military authorities about many planned military and political actions, acts of sabotage, ambushes, dynamitings, etc. In addition, the messages provided information about the exact location of Allied airfields in

[768] I 58 p 6

[769] I 170 p 5

the Greek mountains, about the position, strength, and activity of the Allied military missions and various British commando troops, about Greek internal and inter-allied crises and struggles, about the British tactics for the occupation of Greece, etc.[770] Work on Greek systems ceased on 15 October 1944 when NAZ G was transferred to Sarajevo.[771]

85. Work on Hungarian traffic 1941-1944-- The Hungarians used the commercial model of the Enigma, and had the rotors for the machine made by the German firm of Konski and Krueger. This firm usually turned over the records of rotor wirings to the Armed Forces Radio Communications Branch (Ag WNV/Fu) which in turn gave them to In 7/VI. However, Hungarians connected with the firm took the rotors at night and changed the wirings enough to make the firm's records incorrect.[772] No effort appears to have been made on the part of the Germans to recover the wirings or to prevent the sabotage. It is difficult to suppose that the Germans could have been so easily duped had they wished to press the matter. Evidently, they did not consider the traffic worth causing embarrassment to the Hungarians.

With the onset of war, however, the Germans grew more cautious, particularly with the movement of German troops through Hungary.[773] During the spring and summer of 1941, the radio traffic of the Hungarian Railway Administration was monitored from the Fixed Intercept Station at Tulin. The code being used at that time by the railways was a turning grille (Raster Code) with permanent squares which could be turned in four different positions, and reversed to give four additional positions. The code was solved by Doering of the mathematical section of In 7/VI.[774] After the check on the railway authorities had proved that they were dependable, interception was stopped.[775]

[770] I 170 p 6

[771] I 170 p 7

[772] I 84 p 3

[773] IF 126 p 10

[774] I 58 p 7

[775] IF 126 p 10

Watch on Hungarian traffic was dropped from 1941 to 1943 because of the high priority given to Russian traffic.[776] In 1943, however, interest again developed and a detail was sent from Feste 6 (the former Fixed Intercept Station at Tulln) to Slovakia near Pressburg, Hungary to monitor Hungarian traffic.[777] Some tenseness in the relations of Germany and Hungary may be reflected by the fact that all members of the detail wore civilian clothing. At that time also, In 7/VI began to resume its work on Hungarian traffic. Count Esterhazy of the Balkan section began work on a Hungarian code and turning grille;[778] Teuchtler and Seper are said to have worked on Hungarian messages enciphered with a two figure substitution key.[779]

Work on Hungarian traffic was done by the Balkan section of In 7/VI only when the Army thought it necessary to check up on the Hungarian allies, but the attempts which were made were apparently successful. The solution in 1941 by Doering of the Hungarian grille, while not of great strategic or tactical importance, is characterized by Buggisch as 'brilliant'.[780]

86. Work on Rumanian traffic 1941-1944-- Very little is known of the work of the Balkan section on Rumanian traffic from 1941-1944. According to Mettig, the monitoring of Rumanian traffic ceased in 1941 because of high priority given to Russian traffic.[781] In 1941, however, monitoring appears to have resumed. Kotschy and Boscheinen of In 7/VI state that Rumanian traffic was completely monitored at that time, and that the Balkan section was reading a transposition system which was decoded with comparative ease.[782] Other references to Rumanian systems are found in Herzfeld's brief statement that Schmidt, Karl, and Wagner of the Balkan section were working on a Rumanian diplomatic code consisting of 5 or 6 figure groups;[783] and in

[776] I 78 p 11

[777] IF 126 p 10

[778] I 100 p 4

[779] I 100 p 5

[780] I 58 p 7

[781] I 78 p 11

[782] IF 126 p 4

[783] I 100 p 5

Keller's statement that KONA 4's Evaluation Center while at Belgrade from September to December 1944 worked on Rumanian messages.[784]

87. Work on Yugoslav traffic 1941-1944-- With the insistence of the German government that Yugoslavia align itself with Nazi policy in the spring of 1941, and the consequent wave of Yugoslav national resistance, the Balkan section of In 7/VI and KONA 4 undertook the heavy burden of monitoring the various types of Yugoslav traffic.
These types were:

a. the traffic of the friendly Croatian Regular Army (Domobrani) and the Secret Police of that Army (Ustashi), military units of the puppet government established by the Germans in 1941;
b. the traffic of the Chetniks under General Mihailovitch who were resisting German aggression;
c. the traffic of the Yugoslav Partisans under Marshal Tito;
d. the traffic of the Croatian Resistance Movement led by Dr. Matchek.

When the German government established the puppet government of Croatia in 1941, the Croats were given the commercial model of the Enigma for use by their Army and Secret Police.[785] The traffic of these units was read by the Balkan section currently without any delay. According to Buggisch, the solution of this traffic was not an outstanding cryptanalytic achievement for the following reasons:

a. the machine used was the K model with three wheels and no stecker;
b. the wheels of the machine were wired for the Croats by the firm of Konski and Krueger which habitually gave the wirings to the Armed Forces Radio Communications, which in turn gave them to In 7/VI;
c. A single key was used throughout the entire Croat Army and area, and this consisted of a list of 100 settings per month;
d. the ringstellung of the wheels remained at AAA;
e. the wheel order 1,2,3 was always used.

[784] I 74 p 2

[785] I 92 p 2

Just to make sure, however, adds Buggisch, "the Germans paid for one of the first keys used, and with this decoded traffic were able to establish stereotypes and solve almost 100% of the traffic from the first."[786] Although Buggisch did not recall the contents in detail, he stated that there were some interesting passages about actions against Tito. He also stated that the Germans had considered equipping the Croats with the plugboard Enigma, but that they decided against this since they believed the corrupt Croats would continue to sell the keys to British agents.[787] In that case, the Germans would have to pay for the keys used by the Croats instead of solving them as they could with the commercial Enigma.

Hentze of In 7/VI states that the Balkan section was successful with a double transposition used by the Croats but nothing more is known of this system.[788]

Herzfeld states that the Domobrani and Ustashi used a five figure code based on a former Yugoslav military code.[789] Evidence is lacking about the actual results obtained but it is probable that the system was solved since the former Yugoslav code was known.

Solution of the systems of General Mihailovitch and Marshall Tito was divided between a unit of KONA 4 in Belgrade and the Balkan section of In 7/VI. The breaking of easy guerilla techniques, particularly the solution of daily recipherings, was carried on at Belgrade by a special detachment which had served in 1941 under Wollny as an evaluation center for Section III Armed Forces Radio Communications Branch (Amtsgruppe Wehrmachtnachrichten Verbindungen, Abteilung Funkwesen, Gruppe III, abbreviated "AgWNV/Fu III" or "Fu III"). With the assumption by the unit of work against the enemies Tito and Mihailovitch, the detachment came under Army control and was attached to KONA 4 which had its Evaluation Center at that time in Belgrade.[790]

[786] I 92 p 2

[787] I 92 p 3

[788] I 113 p 5

[789] I 100 p 4

[790] I 115 p 8

The solution of the more difficult systems was carried on at In 7/VI by the Balkan section under the immediate supervision of Bailovic, a former employee of the Austrian cryptanalytic bureau and specialist in Slavic traffic. Bailovic is named throughout TICOM sources as the specialist in the systems of Tito and Mihailovitch.[791] Unfortunately, he was not interrogated personally.

Herzfeld, a member of the Balkan section of In 7/VI from 1941 to the capitulation, has written in two reports, I 52 and I 69, a full discussion of the Yugoslav systems worked on by that section. The traffic of Mihailovitch was entirely double transposition with fixed key length and key word.[792] These were regularly, if somewhat slowly, solved at In 7/VI with the aid of stereotyped phrases, frequency charts, and other well known cryptanalytic methods. Herzfeld states that it took one to three days to break a single message.

The systems of Tito were far more varied, most of them of Russian origin.[793] In I 69, Herzfeld lists among the Tito systems broken at In 7/VI:

a. a simple letter or two figure substitution system used for enciphering messages sent by brigades and partisan units to Tito divisions in 1944;
b. a simple substitution key with short reciphering set used below division level in 1944;
c. simple two figure substitution key with nulls and short reciphering set used below division in northern and western Yugoslavia and Bosnia in 1944, possibly also in Serbia and Macedonia;
d. multi-columnar substitution key used for traffic between divisions and brigades in Slovenia, western Croatia, western Bosnia in 1944;
e. an Albanian multiple substitution key used by Tito partisans of Albanian nationality;
f. variable substitution key with short reciphering set, the main cipher above division until June 1944.

[791] IF 126 Appendix 2; I 51 p 5; IF 120 p 8

[792] I 52 p 2

[793] I 52 p 5

The system which succeeded the variable substitution key with short reciphering set was called Tito's "Novo Sifra." It was used after June 1944 above division level and was not broken by In 7/VI. Herzfeld claims that it could have been broken with sufficient traffic and close scrutiny.

In the autumn of 1944, work on Tito traffic was increased. Besides the unit stationed in Belgrade under Wollny, the Evaluation Center of KONA 4 was moved from Athens to Belgrade and began work on Tito ciphers.[794] The Close Range Signal Intelligence Platoon, NAZ G, which had been working on Greek Partisan traffic was also moved from Saloniki to Sarajevo to cover Yugoslav traffic.[795]

The only reference to the work of the Balkan section of In 7/VI on Croatian Resistance Movement systems is the note by Kotschy and Boscheinen that this traffic was decoded mainly by KONA 4 and was rechecked by the Balkan section of In 7/VI.[796]

In general, it may be said that the work on Yugoslav systems was successful. The systems of Tito and Mihailovitch formed the most important part of the work of the Balkan section and received the personal attention of the head of the section, Bailovic.

88. Work on Turkish traffic 1941-1944-- Both the intercept and the decoding of Turkish traffic was handled largely by signal units subordinate to KONA 4. The Close Range Signal Intelligence Platoon, NAZ "T", which was stationed at Graz, worked only on Turkish traffic.[797] At first it had intercepted Turkish Navy and Merchant Marine traffic as well as Army and Police traffic, but certain disagreements arose with the German Navy over the interception of the Navy and Marine traffic and this was abandoned.[798]

[794] I 170 p 7

[795] I 170 p 7

[796] IF 126 p 4

[797] IF 171 p 4

[798] IF 126 p 9

The police traffic of Turkey is described as:[799]

a. simple transposition used by the police departments of Ankara, Edirne, Istanbul, Izmir for police matters only;
b. two letter or figure code used for police counter-intelligence with police agents;
c. two or three letter code used for agent traffic.

The Turkish Army Codes were mainly transposition codes with a key word, sent in five letter groups preceded by a four figure number.[800] All of these systems were decoded by NAZ T, and were sent to In 7/VI simply for the purpose of checking all work.[801]

One special Turkish code is mentioned as having been read by the Germans either of In 7/VI or NAZ T -- the special code used by the President of Turkey while sailing on the State Yacht, the Savarona. This code was used in 1943 for radio messages while the President was on the yacht, and not thereafter.[802]

Sometime in 1942/43, In 7/VI received from the Research Bureau of Goering (the Forschungsamt, abbreviated "FA") the mission of solving certain Turkish diplomatic traffic. This the Balkan section did under the supervision of Bailovic, and the decoded traffic was sent to the Research Bureau. Kotschy and Boscheinen state that the traffic was used by military attaches for their reports from Russia, Bulgaria, and Italy, and that it was read continually by In 7/VI.[803] We know from other sources that this traffic proved to be a very valuable source of information concerning Russia. Mettig remembers a number of reports from the winter of 1943-44 on the Russian military situation and the preparations for an offensive.[804] Despite many warnings from British sources that the traffic was being read, Turkey failed to change the system, and the reading of Turkish diplomatic traffic remained a constant source of information.[805]

[799] IF 126 pp 12-13

[800] IF 126

[801] IF 126 p 9

[802] IF 126

[803] IF 126 p 9

[804] I 96 p 14

[805] I 96 p 14

89. Work on Bulgarian traffic 1941-1944-- There was very little work done on the traffic of Bulgaria during the war. According to Kotschy and Boscheinen, the traffic of the Bulgarian military attaches was decoded.[806] Herzfeld states that Thiele of the Balkan section worked on a Bulgarian cipher but no details are known.[807]

90. Work on Agents' traffic 1941-1944-- The Agents' section of In 7/VI was established in 1942. Before that time, the activities of this section which consisted of radio security inside Germany and monitoring of illegal transmissions had been carried on by Section III of the Armed Forces Radio Communication Branch (Amtsgruppe Wehrmacht Nachrichten Verbindungen, Funkwesen Gruppe III, abbreviated "AgWNV/Fu III" or "Fu III").[808] In 1942, however, it was seemed necessary to establish a deciphering section specializing in agents' ciphers. Fu III wanted it set up within itself, but the Supreme Command of the Armed Forces and the Army High Command opposed the establishment of another cryptanalytic agency. As a result of their opposition, it was agreed to set up a section for agents' traffic within an existing cryptanalytic organization. In 7/VI was chosen because the Armed Forces could not spare the personnel. The Agents' section was thus attached to In 7/VI although it appears to have maintained the close relation with Fu III, housing itself near Fu III and moving with it in November 1943 to Jueterbog.[809]

The most complete account of the work of the Agents' section, commonly called the Vauck section from its chief cryptanalyst, First Lt. Dr. Vauck, is found in a CSDIC report by Mettig (S. I. R. 1726) later re-published as I 115. Mettig gives great credit to the work of Dr. Vauck saying that this section achieved good results because of Vauck's leadership and his personal cryptanalytic successes. The section was not large, consisting of twenty people in the main section, ten at outposts in Paris and Brussels and other cities, and eight lent to the Polish section of the Signal Intelligence Agency of the Supreme Command, Armed Forces (OKW/Chi). Recognized traffic was decoded in the outstations; the rest was sent to Berlin. All traffic, moreover, was sent to Berlin in duplicate.[810]

[806] IF 126 p4
[807] I 100 p5
[808] I 115 p 2
[809] I 115 p3
[810] I 111 p 5

The cryptanalytic methods employed by the Vauck section differed from normal methods of solution because of the peculiar nature of Agents' systems.[811] Some of the achievements of the Vauck section are outlined in the following pages.

91. Work on Czech Agents' Traffic-- The Vauck section worked on Agents' traffic of the Czechoslovak Resistance Movement.[812] Mettig believed that the breaking in 1942/43 of two links running to England made possible the arrest of British agents in Czechoslovakia. The greatest success was achieved by intercepting the wireless communications of the Czech Resistance Movement in London. This was the only case in which Mettig is certain that it was possible for the Vauck section to break into an agent network by purely cryptanalytic means, and this was largely through breaches of security on the part of the Czech chief. After the system had been broken, the book for enciphering was found and the key recovered. In September 1942, the Czechs were about to go over to a new system but were foolish enough to name in the old system the book to be used for enciphering in the new system. Contents of messages solved on this link were nearly always concerned with reports on the political situation and activities of the Czech Resistance Movement, and were so important that for a long time the W/T traffic was allowed to continue unhindered.

92. Work on Yugoslav Agents' traffic-- Work on Yugoslav Agents' traffic was carried on by a detachment in Belgrade under Lt. Wollny. This detachment had beeh under Group III of the Armed Forces Radio Communication Branch (Fu III) but was attached in 1942 to KONA 4 because all fighting against hostile organizations such as Mihailovitch and Tito was directed by the Army.[813] The work of this group has already been described under the Balkan section's work on Yugoslav traffic, where it properly belongs since the traffic which was not solved in the detachment was sent to the Balkan section of In 7/VI for solution.

93. Work on Agents' traffic in Southern Franca and Spain-- Agents' traffic in southern France and Spain emanated largely from USA, British and Spanish Republican agents who were in

[811] I 115 pp 4-5
[812] I 115 p 8
[813] I 115 pp 8-9

radio contact with stations in Spain. To cope with this traffic, a camouflaged branch station was set up in Madrid and the intercepted traffic passed to Vauck's section. According to Mettig, the results of the traffic were very good although no details are known.[814]

94. Work on Russian Agents' traffic-- Mettig knew of three important Russian Agents' network: the "Red 3" (Rote 3), the Schulze-Boysen net operating in Berlin in 1942, and two links running from Brussels. The last named links were, as far as Mettig knew, not solved.[815]

The story of the work on the "Red 3" net is most interesting. In addition to Mettig's account, we have two memoranda written by Fenner, the chief cryptanalyst of the Signal Intelligence Agency of the Armed Forces.[816] Fenner reported that on 23 February 1943 his agency was asked by Vauck's section to collaborate in work on certain messages of Russian agents on the "Red 3" net. By the end of March, the Vauck section had furnished Fenner's cryptanalysts, Novopashni, Trappe, and Schmidt, with all the traffic in that system since September 1941 so that a start was made on solution. Fundamental findings were communicated to In 7/VI which enabled that organization to break into the system roughly at the time as did Fenner's group. After the initial break in, it was agreed that In 7/VI should continue to work on the system, and Mettig stated that from this help the Vauck section discovered that the system was based on a book text.[817] In the autumn of 1944, Vauck is said to have told Mettig that the exact sending position of this net had been determined in Switzerland. A raid was planned but had to be cancelled as Swiss authorities had forestalled the Germans. The station, according to Mettig, was evacuated and destroyed before the Germans could take action.[818]

[814] I 115 p 7

[815] I 115 p 7

[816] D 60 pp 16-20

[817] I 115 p 8

[818] I 115 p 10

The story of the second Russian net, the Schulze-Boysen net operating from Berlin in 1942, is equally dramatic.[819] This net received its name from First Lt. Dr. Schulze-Boysen whose house was the center of a Communist inspired espionage agency operating on a large scale. When the first inroad into this traffic was made by the Vauck section, Dr. Lenz, one of the members of the Vauck section, mentioned the name Schulze-Boysen to another member of the Vauck section named Haymann who frequented the Schulze-Boysen house. Haymann warned Mrs. Schulze-Boysen. Subsequently, both Haymann and Dr. Lenz were arrested, and Haymann condemned to death. Lenz was released and transferred to an out-station in Paris, since all that could be proved against him was that he mentioned the name Schulze-Boysen to Haymann. With the aid of knowledge obtained from decoded traffic, the Gestapo made arrests of from seventy-nine to eighty people of whom seventy were condemned to death. The case was kept strictly secret because some of the accused were employed in various war agencies and were betraying secrets to Russia.[820]

95. Work on Polish Resistance Movement traffic-- The most notable results in the Agents' section were achieved in the interception and solution of the systems used by the Polish Resistance Movement, particularly during the Polish uprising in Warsaw in 1944.[821] From information passed on this system, the dispositions of the Polish liberation troops as well as friction between them and the Russians could be established. It was possible, moreover, to solve all wireless traffic which the Polish government in London carried on with its organizations in Poland. In order to preserve secrecy and to insure quicker delivery of the decodes, eight members of the Vauck section were transferred in the autumn of 1943 to the Polish section of the Signal Intelligence Agency of the Supreme Command, Armed Forces (OKW/Chi)

[819] I 115 p 10

[820] See Volume 4, Chapter VI

[821] I 115 p 9

for work there. The clear text was published by the Armed Forces in their bulletins and was given extremely restricted distribution. To insure complete radio intercept coverage, the Armed Forces Agency (OKW/Chi) ordered its station at Lauf also to intercept the traffic. First Lt. Schubert, a cryptanalyst of GdNA, wrote a brief account of the systems used by the Polish National Resistance Movement in which he stated that systems 006, 117, 118, and 181 were broken and that others were worked on. Most of them were simple two figure substitutions used without an indicator, with some variations in development and the use of basic keys or key phrases.[822]

96. Work on German Traitors' Traffic-- Mettig stated that he once saw a report concerning a German who transmitted by wireless to England details of a newly constructed signals shelter in Berlin urgently requesting that it be bombed. No details of these systems are known.[823]

97. Linguistic Research 1941-1944-- Linguistic research during the years 1941-1944 was carried on at In 7/VI by a section designated as the Linguistic Research Section (Sprachforschungsreferat). Mettig listed this section as one of the twelve sections of In 7/VI in 1942 and named Koehler as its head.[824] Koehler remained head of this group throughout the war, and in November 1944 the section was transferred with Koehler from GdNA to the Signal Intelligence Agency of the Supreme Command of the Armed Forces (OKW/Chi).[825] Mettig claimed that it was contemplated that the members of the linguistic research section would advise the cryptanalysts on language problems and direct all matters of the Armed Forces concerning foreign languages. Although the plans were never realized, the nature of the work of the section can be inferred from these plans.

[822] I 26 pp 14-15
[823] I 115 p 10
[824] I 78 p 6
[825] I 96 p 15

98. Mathematical Research 1941-1944-- The Mathematical Research Section was headed by Dr. Pietsch, who, according to Mettig, collected in this section the best available mathematical brains.[826] The work of the section was two-fold:

a. the investigation of all unsolved traffic from the various sections of In 7/VI so long as it was necessary to achieve an inroad by purely analytical means;
b. the investigation of the security of current German Army systems.

To achieve these purposes, three subsections were found necessary:

a. a subsection designated "F" for the German word for research, Forschung. This subsection was headed by von Denffer and handled research on foreign systems.[827]
b. a subsection designated "7". This subsection was headed by First Lt. Lueders and dealt with the security of German Army hand systems.
c. a subsection designated "13". This subsection was headed by Dr. Doering and dealt with the security of German Army machine systems.

99. Cryptanalytic work of subsection "F" 1941-1944-- Subsection "F" of the mathematical section appears to have done some excellent work in the solution of the more simple machine systems used by foreign countries. The following examples of solution may be cited:

a. The discovery of theoretical methods of solving traffic in the Russian "K-37" (a B-211 type cipher machine) after capture of a model in 1941.[828]

[826] I 78 p 6

[827] I 78 p 6

[828] I 58 p 5; I 176 p 3

b. Development of a technique for converting the relative settings, recovered for wheels of Converter M-209 on days when such solution was possible through reading of some of the traffic, into absolute settings, thus making it possible to read all the traffic sent on those days.[829]
c. The discovery in 1943 of theoretical methods of solving messages sent in the French B-211 cipher machine.[830]
d. The reading of de Gaulle traffic enciphered by the C-36.[831]
e. The solution in 1944 of the Swedish Hagelin, the BC 38, by Marquardt and Hilburg.[832]

Doering's solution in 1941 of the Hungarian grille should be counted as one of the achievements of this section. As has been pointed out, the section had no success whatever with the large cipher machines such as the British Typex, the USA SIGABA, and large Swedish Hagelin. Hentze of GdNA states that the mathematical section worked on Russian 4 and 5 figure enciphered code with partial success.[833]

The outstanding men of this section were named by Buggisch as Hilburg, Rinow, and Wuenoche.

Subsections "7" and "13" of the mathematical section were concerned with security studies of German Army hand and machine cipher systems. They will be treated in Chapter VIII, which deals with German Army cryptographic systems.

100. Use of IBM in Cryptanalysis, 1941-1944-- The IBM section of In 7/VI was derived from the IBM section set up in 1939/40 by the German Security Agency (In 7/IV), at the suggestion

[829] I 58 p 6; I 113 p 6

[830] I 160 p 6

[831] I 160 p 6; I 58 p 5. The C-36 had been solved previously in 1940 with the aid of the Signal Intelligence Agency of the Supreme Command Armed Forces, OKW/Chi.

[832] I 176 p 3; I 160 p 6; I 58 p 5

[833] I 113 pp 5-6

of the mathematicians and former actuaries of this section.[834] It was natural that in 1942, when the study of the security of German Army systems was transferred from In 7/IV to In 7/VI, the use of IBM machinery for security studies was transferred to In 7/VI and quickly adapted for cryptanalytic work on foreign systems. The machinery used by In 7/VI was mostly of German make, although a number of captured French IBM machines were included.[835] The section, headed by Schenke, consisted in 1943 of thirty or forty women key punchers, and twenty to thirty soldier mechanics.[836] We have no exact evidence as to the number or types of machines used although Hentze states that in 1944 there were 30 key punchers and 2 tabulators.[837] The special contribution of In 7/VI to IBM work was the adaptation of the machines to various tasks by special wirings.[838] In 1943, a special workshop for the development of improved wirings was set up with the IBM firm at Lichterfeld.[839] The major success obtained was the work on the Russian 5-figure traffic.[840] In the early stages of the Russian campaign, it was comparatively simple to establish depths in these messages without the use of IBM, but by 1943 IBM machinery was indispensable for locating depths.

Buggisch declared that no tasks were undertaken by the IBM section which could have been done by 100 people. He maintained that lack of IBM machinery spurred the analysts of the Signal Intelligence Service of the Armed Forces (OKW/Chi) to the development of new and better types of analytic devices while In 7/VI remained content with inferior adaptations of IBM machinery. The Army's general attitude concerning IBM machinery is hinted at in Buggisch's statement that the Enigma could probably be solved by a large enough array of IBM machinery,[841] but it never occurred to him, evidently, that such would be contemplated by the enemy.

[834] I 67 p 2

[835] I 78 p 6

[836] I 67 p 2

[837] I 113

[838] I 67 p 2

[839] I 67 p 2

[840] I 58 p 6

[841] I 92 p 5

It should be noted that the IBM section of In 7/VI was at least toward the last hampered by the fact that their machines were outworn, outmoded and irreplaceable. The factories which had been producing parts were bombed out and, as the machines wore out, their work became inaccurate. In some instances, work by machine was abandoned. An example of this is cited by Mettig in his discussion of the attempt in 1944/5 by the Signal Intelligence Service of the Armed Forces to provide units below regimental level with signal tables. The values were to be set up by the IBM section of GdNA (formerly of In 7/VI) but it transpired that the IBM machines had been overworked in the last years and were not functioning properly.[842] As a result the trigrams were not being reciprocally enciphered and other methods of producing them were developed. In early 1945, the IBM section of GdNA was offered to Signal Intelligence Agency of Supreme Command of the Armed Forces (OKW/Chi), but Mettig states that the matter was never clinched because of the confusion at the end of the war.[843]

101. German Army cryptanalytic effort 1945-- With the establishment of the GdNA in late 1944, all operational cryptanalysis was carried on by sections 2, 3, and 4 of Group IV of the GdNA. Section 2, headed by Kneschke, dealt with the deciphering of western European traffic and probably also with Hungarian, Rumanian, and Italian ciphers. There were three subsections:[844]

2a. headed by Dr. Werner Schulz, dealt with British, USA, and Swedish systems,
2b. headed by O/Insp Otto Kuehn, handled French systems
2c. headed by Kneschke, processed Balkan systems.

[842] I 96 p 12

[843] I 96 p 13

[844] I 160 p 2

Section 3 was headed by Dettman and dealt with Russian systems, with four subsections:[845]

3a for Russian NKVD (Special Police) traffic,
3b for Russian Army traffic,
3c for Russian Partisan traffic,
3d for research on Russian systems in general.

Section 4 was devoted principally to statistical IBM work.

There is no record of any new or difficult systems being solved after late 1944. The main effort of the GdNA was apparently directed to the deciphering of systems already solved and to the simple necessity of finding a place to operate. From February 1945 until the capitulation, Group IV of the GdNA was constantly on the move seeking refuge in the south from the Allied advance.

[845] IF 123 p 10

VOLUME 4

Chapter VIII. German Army Cryptographic Systems

102. German Army cryptographic systems.--The German Army used three main types of cryptographic machines in its communications down through division: the Enigma, the teleprinter cipher attachment ("Schluesselzusatze," abbreviated "SZ"), and the cipher teleprinter ("Schluesselfernschreibmaschine," abbreviated "SFM").

The commercial type Enigma was introduced probably in 1925.[850] It was replaced in 1939 by the plugboard Enigma.[851]

The first teleprinter cipher attachment, the SZ-40 "original model," was introduced into the Army probably in 1940[852] although Dr. Huettenhain of the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) said that the Army had been experimenting with this type of cryptographic apparatus as early as 1937.[853] It was replaced by the SZ-40 "regular model," and this was succeeded by the SZ-42a and the SZ-42b, developed by Dr. Liebknecht of the Army Ordnance Development and Testing Group Signal Branch (Wa Pruef 7) and by Inspector Menzer and Dr. Huettenhain of the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi).[854] The SZ-42c was also developed and 30 or 40 test sets built, but the apparatus was evidently not used.[855]

The first cipher teleprinter, the SFM T-52a, was introduced in 1939; improved models were called the SFM T-52b, c, d, and e. By the end of the war only models T-52 c, d, and e were in use. A one-time tape cipher teleprinter designated the SFM T-43 was introduced in 1943.

850 I 31 p 17
851 I 78 p 7
852 I 31 p 14
853 I 31 p 7
854 I 57 pp 5-6; I 45 p 19
855 I 31 p 13

The German Army used hand ciphers below division. After World War I, and before 1942, some of the hand systems of the Army, as listed by Dr. Huettenhain of the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) were:[856]

a. A monoalphabetic type substitution using a keyword mixed alphabet in a 5 x 5 square.

b. A "comb-transposition" ("Kammwurfel").

c. A "book key" ("Heftschluessel").

d. A double transposition (DOPPEL WUERFEL, abbreviated "4-S-40"). This system was used until 1926 or 1927.

e. The "Single Playfair" (KASTE-SCHLUESSEL, abbreviated "TS-42").

f. The "Double Playfair" (DOPPEL-KASTE-SCHLUESSEL, abbreviated "NS-42").

In 1942, subsection 7 of the Mathematical Section of In 7/VI declared that all hand systems currently used by the German Army were insecure.[857] Since the Field Army had no reserve hand systems, In 7/VI was ordered to cooperate with In 7/IV in producing new systems.[858] The following hand systems were evolved and used by the German Army from 1942-1945:

a. Three letter field codes ("Signaltafeln") with or without enciphering tables ("Schluesseltafeln").[859]

b. Single transposition using grille ("Rasterschluessel 44," usually called "Raster").[860]

c. Double transposition ("Rasterersatzverfahren").

Under field conditions many makeshift systems were employed, such as monoalphabetic substitution, transposition consisting only of reversing the order of the letters of the plain text, and whatever the particular radio operators might adopt by agreement among themselves.

856 I 31 p 17
857 I 20 p 3
858 I 78 p 13
859 I 20 p 3
860 I 20 p 3

For weather reporting, the Army used two types of systems until 1945:

a. The "Barbara Code" ("Barbaraschluessel") consisting of figure cards for encoding artillery meteorological reports for Army and anti-aircraft units.

b. Weather substitution tables, for enciphering meteorological reports in the Reich Weather Service (Reich Wetterdienst).

Lt. Col. Mettig stated that the Barbara Code was replaced in 1945 by the "Raster."[861]

103. Preparation and distribution of cryptographic keys.-- The history of the preparation, printing, and distribution of cryptographic keys by the German Army was outlined by Fricke, a member of In 7/IV and latterly of the Signal Intelligence Agency of the Armed Forces (OKW/Chi).[862] According to Fricke, the keys for the Army were produced at the beginning of the war on In 7/IV's own press. The number of personnel required was small (about twenty people in all), since only enigma, weather and book keys (Heftschluessel) were printed.

With the introduction of the SZ 40/42 and other cryptographic systems which required keys, the amount of work entailed in the preparation, printing, and distribution of keys became too great for In 7/IV alone. In 1942, therefore, the production of key table manuscripts was transferred to the IBM section of In 7/VI, and the printing to the Reich press in Berlin; In 7/IV was confined to reading proof and distributing the finished product.

At the time of the bombing attacks on Berlin in November 1943, the printing press and all key material of In 7/IV were destroyed. The key producing section of In 7/IV was then moved from Berlin into emergency quarters prepared some weeks before in the Army Signal School (Heeres Nachrichten Schule) at Halle/Saale. During this period, private printing firms were increasingly drawn on for the production of keys; first, because the Reich printing press could not meet the requirements; and secondly, because decentralization was increasingly necessary to avoid bombing. About twenty firms in the central German area were given contracts for the printing of keys. The high number was largely attributable to the introduction in 1944 of the Stencil System 44 (Rasterschluessel 44).

861 I 96 p 12

862 I 36

In May 1944, the key producing section of In 7/IV was transferred to the Hindenburg barracks at Dresden, where Major Dr. Metzger assumed direction. This remained the situation until 1 November 1944 when all tasks of producing, printing, and distributing of keys for the Army were transferred from In 7/IV to Section IIIa of the Signal Intelligence Agency of the Armed Forces (OKW/Chi/IIIa). This section was established at Dresden in the headquarters which the key preparation section of In 7/IV had occupied. In March 1945, Section IIIa was transferred from Dresden to the Army Signal School at Halle/Saale because of the approach of the Russians. Work was never begun, however; and on 12 April, keys and material for producing them were loaded on trucks to be sent to southern Germany. Keys left at Halle were destroyed by the Germans at the approach of the United States Army.[863]

104. German Army Security Studies.--Before 1939, the Army High Command had no security organization of its own. Questions of security concerning Army systems were referred to the Codes and Ciphers Section of the German Defense Ministry. Huettenhain stated that he and Menzer, as members of the Codes and Ciphers Section, did a security study on the SZ 40 ("original model") and found that it could be solved in two days.[864] This led to its improved form.

In 1939, the Army High Command established its own Signal Security Agency (In 7/IV), which functioned as such until 1942. During the period of its activity, the Signal Security Agency (In 7/IV) examined the plugboard Enigma[865] from the point of view of security, and made security studies on two other cryptographs proposed for Army usage, the M 40 and SG 41.[866] The security study of the plugboard Enigma was occasioned by a suspicion roused during the Polish campaign in 1939 that the Poles were reading Enigma traffic.[867] Pietsch, Steinberg, and Bohm (mathematicians of In 7/IV) made security studies on the machine,

863 I 36 p 3

864 I 31 p 17

865 I 92 p 2

866 I 58 p 5. Buggish actually said "C-41" but doubless meant "SG-41." Both the M-40 and SG-41 are described from a cryptographic viewpoint in Volume 2 of this paper.

867 I 78 p 7

the results of which apparently set to rest any doubts about its security. The Army continued to use the system without change until Fricke (another mathematician of In 7/IV)[868] indicated that the Army's manner of using indicators led to an easy solution. At his recommendation, the indicator system was changed.[869]

The two machines proposed for Army use, the M-40 and SG-41, had been invented by Menzer, a member of the Signal Intelligence Agency of the Armed Forces (OKW/Chi). Security studies on the M-40 were made by Dr. Doering and Dr. Buggisch, mathematicians of In 7/IV[870] Dr. Buggisch stated that the studies proved the device to be moderately secure, but that it was never used because it was as bulky as the plugboard Enigma but could not print letters.[871] With regard to the SG-41, the studies made by In 7/IV showed it to be superior to the M-40, but Buggisch stated: "The Army hemmed and hawed and never did adopt it."[872]

In 1942, the responsibility for making security studies of German Army systems, and most of the personnel of In 7/IV who had worked on Army communications security testing, were transferred from In 7/IV to the Mathematical Section of In 7/VI. Pietsch, Steinberg, von Denffer, Hilburg, and Luzius were named among those transferred.[873]

The Mathematical Section of In 7/VI assigned security studies to two subsections: "7" and "13." Subsection "7" undertook the work on German hand systems; subsection "13," on German machine systems.[874] The first studies of subsection "7" on German hand systems proved that all hand systems currently used by the German Army were solvable. As a result, In 7/VI was ordered to collaborate with In 7/IV in the development of new systems for the Army.[875] Although In 7/VI would have preferred to establish this section within itself, where the preparation of systems would be done in close cooperation with cryptanalytic specialists, this point of view was not recognized by the Army and In 7/VI was ordered to send mathematicians back to In 7/IV. The mathematicians sent were Fricke, Jesse, and Kehren.[876] From that time on, subsection "7" confined itself to the study of hand systems handed to it by the Field Army. Mettig noted that the amateur systems with which the section dealt were very bad and betokened great ignorance on the part of the Field Army in regard to code and cipher security.[877]

Subsection "13," which was responsible for the security of

868 I 92 p 5
869 I 92 p 5; I 20 p 2
870 I 58 p 5
871 I 92 p 2
872 I 58 p 5
873 I 92 p 6
874 I 92 p 6
875 I 78 p 13
876 I 78 p 3

German Army cryptographic machine systems, concentrated on security studies of the SFM T-52 teleprinters. SFM T-52a, b, and c were tested by Dr. Doering in the summer of 1942 and were shown to be easily solvable.[878] By the autumn of 1942, it was clear to the mathematicians of this subsection that SFM T-52c could not be made secure. Despite the warnings from the security unit, the Field Army continued to use SFM T-52c. They were particularly sure of it because they thought the land lines on which SFM T-52c messages passed could not be tapped by the enemy. Not until a cellar equipped to tap land lines was found in Paris in late 1942 did the Army consent to the improvement of the machine.[879] This improvement, the T-52d, was ready in early 1943 and was shown by Dr. Doering to be probably insecure. From his experiments with the T-52d evolved the T-52e, which was considered secure.[880]

Some investigation of the plugboard Enigma was carried on by subsection "13" although no definite conclusion was reached concerning its security. In 1943-44, definite proof was obtained from two Polish officers in a prison camp at Hamburg that the Poles had read the plugboard Enigma both before and for some time after the Polish campaign.[881] This proof corroborated the suspicions aroused at the time of the campaign in 1940. Two Army cryptanalysts, Pietsch and Doering, were sent to interrogate the Poles. Although the interrogations were said to have drawn a blank, it became evident that Polish cryptanalysts at Wicher had solved Enigma traffic, had gone to France after the Polish campaign and had continued their work there. Solution was said to have stopped sometime later. The mathematicians of subsection "13" believed that solution had ceased when the Field Army followed Fricke's indicator recommendations. The general result was that subsection "13" did not press the matter of Enigma security.

Subsection "13" had also been assisting in the design of Cipher Device 39 (Schluesselgeraet 39), an improved Enigma which was intended to employ a plugboard, changeable turnover rotors, pluggable reflecting wheels, and additional Hagelin-type drive wheels.[882] Buggisch stated these machines were his specialty. They were under construction at the Technische und Normalzeit firm at Frankfurt am Main at the time of the surrender.[883]

878 I 58 p 2
879 I 78 p 11
880 I 78 p 12
881 I 92 p 5
882 I 58 p 6
883 I 20 p 4

The responsibility for the security of German Army cryptographic systems remained with subsections "7" and "13" until November 1944, when it was turned over to the Signal Intelligence Agency of the Armed Forces (OKW/Chi). The Army then retained only the responsibility for seeing that the systems approved by OKW/Chi were properly used in the field.[884]

105. Attitude of the Field Army toward Security Studies.-- The Field Army maintained an uncooperative attitude toward security studies made by the Mathematical Section of In 7/VI. Whenever the Field Army was asked to change a system, there was a storm of protest. All changes in methods were supposed to be enforced by the staff of the Army Communications Branch (Heeres Nachrichten Verbindungsabteilung, abbreviated HNV), and the nature of the results depended upon whether the officer at staff headquarters happened to know anything about cryptanalysis. Fricke said he usually did not.[885] Only with the greatest difficulty was the Field Army persuaded to change its methods.

One of the specific ways in which the Field Army consciously hampered progress in security studies was to refuse to furnish In 7/VI actual traffic. Fricke said that In 7/VI never knew how the Field Army actually used the systems which it approved. When In 7/VI asked for traffic for its studies, it was given specially prepared messages such as: "We are standing in Berlin and see the Polish infantry coming down the Frankfurt Allee."[886] However, the Field Army made a brief attempt in 1941 to provide the analysts with actual traffic. For this purpose a Signal Intelligence Regiment of the Replacement Army (Nachrichten Aufklaerung Abteilung/Chef der Heeresruestung und Befehlshaber des Ersatz Heeres, abbreviated NAA/Chef H Ruest u BdE) was formed. While two companies of this unit were to act as administrative units for personnel of In 7/VI, the third company was an intercept unit which worked in the field collecting material for the analysts. (Due to personnel shortage, however, this unit was dissolved in February 1942, and no subsequent attempt was made by the German Field Army to procure actual traffic for In 7/VI).[887]

As described in Paragraph 104, it was difficult to persuade the Field Army to accept as valid the security studies made by

884 D 68 pp 3-4
885 I 20 p 3
886 I 20 p 3
887 I 20 p 3

the cryptanalysts of In 7/VI. For instance, not until an entire cellar with excellent equipment for tapping land lines used by the T-52c was raided in Paris in early 1943, was the Army High Command persuaded that the security study made by In 7/VI had been valid.[888]

The attitude of the Field Army could be traced largely to the ignorance on all levels of matters pertaining to codes and cipher security. Fricke's remark that the staff officer of the HNV who controlled code and cipher methods usually knew nothing about cryptanalysis has already been mentioned. Mettig stated that the suggested systems handed to In 7/VI for scrutiny betrayed the lamentable ignorance of the Field Army.[889] Signal tables set up by the troops revealed serious cryptographic errors, such as the failure to change keywords for long periods.[890] In an attempt to correct this ignorance, In 7/VI gave lectures at the Army Signal School at Halle and issued instructions on code and cipher security. The situation, however, was never satisfactory. Buggisch aptly called it tragic-comic: When In 7/VI detected an insecurity, it was not able to achieve effective remedies; if In 7/VI wanted to install new devices, it had even more difficulties. The Army "hemmed and hawed" and never got around to acting.[891]

888 I 78 p 11
889 I 78
890 I 96
891 I 58 p 5

VOLUME 4

Chapter IX. Training of German Army Signal Troops

114. Training of Signal Recruits.--The Signal Intelligence Replacement and Training Battalion (Nachrichten Aufklaerungs Ersatz und Ausbildung Abteilung, abbreviated NAEUAA), which was located at Frankfurt/Main, was responsible for the training of German Army Signal recruits. It had control over Signal Intelligence Replacement and Training Companies in each Service Command (Wehrkreis) where basic training and some training in signal matters were given to the recruits.[895] In time of peace, basic training lasted for one year, signal training being taken up after the first three months. During the war, the time of basic training was shortened in order to place more troops more quickly in the field. Recruits were trained in direction finding, teletype operation, and simple field codes, and were then sent out into field units.[896] No special courses were conducted in the Replacement and Training Companies.

115. Training of Signal Technicians.--Most of the signal technicians were trained in specialist schools of various sorts. Schools for carrier frequency, switchboard operators, repair men, etc., were established by the Army and Division and Corps Signal Battalions and at Army Signal Depots.[897] Instructors were mainly non-commissioned officers who had had experience in the field.

116. Training of Specialists.--The Signal Interpreter Replacement and Training Battalion (Nachrichten Dolmetscher Ersatz

[895] IF 250 p 2
[896] IF 250 p 3
[897] IF 250 p 3

und Ausbildungs Abteilung, abbreviated NDEUAA) was located at Halle/Saale.[898] This battalion was responsible for the training of signal interpreters who were to be employed in signal intercept units for radio and wireless monitoring. The battalion was divided into three companies: company one for Romance, company two for Slavic, and company three for Germanic languages. For matters of administration the battalion was divided into the following five platoons:[899]

1) cadre platoon (Stammzug) comprising cadre personnel, and instructors in military and intelligence technical matters.

2) instructor platoon (Lehrzug) comprising teachers and members of the instructor group.

3) training platoon (Ausbildungszug) comprising the students who were under instructions in some language.

4) alert platoon (Marschzug) comprising men who have passed their final examination and who are expecting to be sent into action.

5) pool (Auffangkorporalschart) comprising newcomers waiting for their entrance examination.

A rough estimate of the personnel shows that in 1944 there were about 350 to 400 men attending the various language classes. After the courses which lasted six weeks, the men were given a final examination. According to the results of this examination, they were assigned to one of the three following categories:[890]

S -- Speakers (Sprachmittler). These were people who spoke well and were able to make themselves understood, but who did not master the language in speaking and writing correctly.

U -- Translators (Uebersetzer). These were people who mastered the foreign language in writing, but were only fair in speaking.

D -- Interpreters (Dolmetscher). These were people who spoke and wrote the foreign language correctly and fluently and whose general education was up to a corresponding standard.

898 IF 105 p 5
899 IF 105 p 3
900 IF 105 p 5

Employment was assigned according to the category to which each person was assigned.

For persons of category "S," a special course in monitoring Allied radio communications was organized at Leipzig for English speaking personnel only. The course consisted of three weeks' daily instruction in the following subjects:[901]

1) USA and British organization of signal units
2) USA and British radio sets used at all levels
3) USA and British radio call signs
4) USA and British authorized abbreviations
5) USA and British message forms
6) USA and British fixed station and net operational methods
7) USA and British Army terminology

Each of the subjects was taught for one hour a day and had a brief examination. In most cases, the lectures were conducted in English to facilitate practice in this language.

117. Training of Signal Officers.--The Army Signal School at Halle (Heeres Nachrichten Schule, abbreviated HNS), conducted the course for officer candidates of the Signal Corps.[902] Emphasis here was in the first months evenly divided between technical and military subjects. The officer candidates were selected by their commanders in the field after having proved themselves in combat or in outstanding work in their specialty. All enlisted men were eligible, although the racial origin evidently played some part in the selection. One prisoner, for instance, states that he was not allowed to become an officer candidate because of a Jewish grandmother.[903]

After their selection, the men were given a four weeks course in tactics, Army regulations, customs, technical subjects, etc. Those who passed this preliminary course were sent to the Armed Forces Signal Troop School (Fuehrungs Nachrichtentruppen Schule, abbreviated FNS), where they were trained for three months in Signal Corps work.[904] From there they were sent into the field for a probation period as leaders of platoons. During this period of training, Colonel Grube states, many of the candidates lost their lives. A final three months at the Signal School at Halle brought with graduation the rank of Lieutenant. Failure

901 IF 131 p 4
902 IF 205 p 5
903 IF 127 p 1
904 IF 250 p 6

118. Training of German Army Cryptanalysts.--Nothing is known of the training of German Army cryptanalysts before 1939. Mettig states that when the Signal Intelligence Regiments (KONA) moved into the field in 1939, no cryptanalysts were available.[906] Colonel Radewig, the commander at that time of all intercept stations in the west, however, was able to procure a number of cryptanalysts from the Fixed Intercept Stations (Feste) around Berlin, and to this force he added a few mathematicians and linguists.[907] As a result, when the German offensive began in April 1940, the KONA's had a moderate supply of cryptanalytic personnel. The early years of the war, however, showed that many more cryptanalysts were needed. Provision to train these cryptanalysts was made by establishing a Training Section in In 7/VI under the leadership of Kuehn but Mettig stated that the work of the section was not fully exploited until 1942.[908] The section was located at Matthaikirchplatz 4 in Berlin until November 1943, when it was moved with the rest of the Agency to Jueterbog because of Allied bombings. In November 1944 the Training Section 7 of IN 7/VI became Section 5 of Group IV of the GdNA.[909] According to Graupe, the school consisted of about twenty officers with one hundred and twenty men, and about twelve women as stenographers.[910]

The course which lasted 10-12 weeks[911] is outlined in some detail in IF 122 pp 3-8. During the morning and for two or three afternoons a week, cryptography was studied from a syllabus. This syllabus included a brief history of cryptography, a general picture of the methods of encipherment, details of various means of encipherment and decipherment. During the remaining afternoons, the students evidently specialized in whatever field to which they were to be assigned. One prisoner of war, Gerd Coeler, states that during the afternoons he studied English military terms and abbreviations, studied the history and organization of the British Empire and the geography of England.[912] Karrenberg[913] outlines the course given for those who were specializing

905 IF 250 p 6
906 IF 78 p 4
907 I 78 p 4
908 I 78 p 7
909 IF 123 p 9
910 IF 127 p 2
911 IF 123 p 9
912 IF 122 p 2
913 I 166

in Russian cryptanalysis. Participants were selected from the personnel of the Signal Interpreter Replacement and Training Battalion who knew Russian. After the most capable interpreters had been selected they were given a course in Russian cryptography which included all types of Russian systems. For practice in this course actual Russian military texts were used by which the men were gradually accustomed to field problems.[914]

119. Evaluation of Signal Training.--The training of cryptanalysts by the Army appears to have been eminently successful. Through the classes of the Training Section at In 7/VI passed most of the men who later became outstanding in the field of cryptanalysis either in the KONAs or in the central agencies. Major Hentze, head of cryptanalysis at Paris (KONA 5) and later of Gruppe IV of GdNA; 1st Lt. Vauck, head of the Agents' section of In 7/VI; 1st Lt. Lueders, head of one of the subsections of the mathematical section of In 7/VI; and 1st Lt. Schubert, head of cryptanalysis at HLS Ost, were all graduated from this course.[915]

The training of signal troops in the field, however, appears to have been less successful. Attention is continuously drawn throughout the TICOM publications to the acute shortage in the Field Army of personnel who were well trained in signal intelligence operations. This was particularly true in the late years of the war when courses became more sketchy. The central agencies recognized this weakness and attempted to remedy it by publishing field manuals on security and having lectures given at the Signal School at Halle by members of In 7/VI. Despite these efforts, however, the Field Army remained, according to Fricke, pitifully ignorant of the principles of security. Ignorance undoubtedly lay at the bottom of the non-cooperative attitude of the Field Army in regard to the adoption of systems considered more secure than those in use by the Army. Conditions were aggravated at the end of the war by the necessity for sending all able-bodied men into the front line and by the general confusion of the Army. Very little training could be carried on by the Field Army during the late months since their schools were taken over by operating agencies. The Army Signal School at Halle, for example, had been used by In 7/IV since November 1943 for the preparation of Army keys; and after March 1945 it housed a considerable section of the Signal Intelligence Agency of the Armed Forces, including service personnel and male and female civilians. It may be safely stated that after 1944 little if any signal training was carried on by the Army.

[914] See Volume 4, Chapter VI for details of this course

[915] I 78 p 8

VOLUME 4

Chapter X. Liaison of the Signal Intelligence Service of the Army High Command with Other Signal Intelligence Services at Home and Abroad

106. Liaison with OKW/Chi.--The relations of the Signal Intelligence Agency of the Army High Command (OKH/GdNA and its predecessors) with the Signal Intelligence Agency of the Supreme Command of the Armed Forces (Oberkommando der Wehrmacht Chiffrier Stelle, abbreviated OKW/Chi) were conditioned by a number of important facts.

a. The office of the Chief Signal Officer, Armed Forces (Chef der Wehrmacht Nachrichtenverbindungen, abbreviated Chef WNV) and Chief Signal Officer Army (Chef des Heeres Nachrichtenverbindungswesens, abbreviated Chef HNW) were held jointly from August 1939 to the capitulation. The close relationship which evolved from this combined office is outlined by a German officer who was aide de camp to General Praun, Chef WNV and HNW from September 1944 until the capitulation.[920] As Chef WNV, General Praun (and his predecessors) was directly subordinated to General Jodl of the Armed Forces Operations Staff (Wehrmacht Fuehrungsstab, abbreviated WFST) and was responsible for all signal operations and policy from an inter-service point of view. As Chef HNW, General Praun was responsible for signal operations and policy within the Field Army, and in this capacity was subordinate to General Guderian, Chief of General Staff.[921]

[920] IF 108

[921] IF 108 p 2

b. The Signal Intelligence Service of the Army (GdNA and its predecessors) and the Signal Intelligence Service of the Armed Forces (OKW/Chi) stemmed from a common origin, the Codes and Ciphers Section of the German Defense Ministry. The Army High Command had set up its first Signal Intelligence Agency, the Intercept Control Station (Horchleitstelle), in 1933, by drawing a few trained cryptanalysts from the Codes and Ciphers Section of the German Defense Ministry. The Signal Intelligence Agency of the Supreme Command of the Armed Forces was the direct descendant of the Codes and Ciphers Section of the Defense Ministry and acquired its new name in 1939.[922]

The close inter-relationships of these three organizations is reflected in the relationships among the officers who controlled them. Colonel Boetzel, who ended the war as chief of the GdNA, had been from 1934 to 1939 head of the Codes and Ciphers Section of the Defense Ministry.[923] General Fellgiebel, who had been head of the Codes and Ciphers Section of the Defense Ministry from 1931-1932 held the office of Chief Signal Officer Army (Chef HNW) and Chief Signal Officer Armed Forces (Chef WNF) from 1939 until 20 July 1944.[924] Colonel Kettler who ended the war as head of the Signal Intelligence Agency of the Supreme Command of the Armed Forces (OKW/Chi) had been head of HLS Ost.[925] Lt. Col. Mettig, second in command of the OKW/Chi, had been head of OKH/In 7/VI from November 1941 to June 1943.[926]

Close collaboration of OKW/Chi and the Signal Intelligence Agency of the Army High Command (OKH/GdNA and its predecessors) can be traced in a number of recorded instances from 1939 to the capitulation. In 1939, Huettenhain, chief cryptanalyst of OKW/Chi, was sent by that organization to the Intercept Station of the Army at Frankfurt/Main to collaborate with the Army on the solution of a new French Army system.[927] The most cordial relationship between the organizations is manifest in his memoranda on his visit to Frankfurt/Main:[928]

> "When I was saying goodbye to the military head of the evaluation section of Army Group C at the termination of my attachment in FRANKFURT-ON-Main, the head of the evaluation section expressed his regret to me that he could not yet present me with some sign of outward

922 See Supra Chapter I

923 I 123 p 4

924 I 123 p 4

925 IF 123 p 3

926 I 78 p 2

927 See Supra, Chapter

928 D 60 pp 4-5

recognition for work successfully carried out in FRANKFURT-On-MAIN. To that I replied that success attained was not due to the effort of an individual but was the result of development and common effort and that if outward recognition should reward this work, Herrn TRAPPE (Chi OKW), SCHMIDT (Chi OKW) and Professor Dr. Foppl (Chi OKW) should likewise remembered. The head of the project thereupon told me that these gentlemen would be similarly distinguished.

"In the course of the conversation, I said that for us the finest recognition was the knowledge that important intelligence, which could serve as a basis for the further conduct of the war, had been sent to G.H.Q. The head of the project replied that he quite understood this attitude but he would like to make military departments appreciate our work at the full value for up to now, they have shown little understanding of the difficulties of such work.

"At the same time, the head of the project requested me to convey his thanks to the Chiffrier Section OKW for the assistance given to the military deciphering section and remarked that in his opinion such a large decyphering task could not be done by OKH either now or in the near future."

In 1942, the Signal Intelligence Agency of the Supreme Command of the Armed Forces (OKW/Chi) sent a special Russian "party" to HLS Ost to collaborate with cryptanalysts there in the solution of a Russian 5-figure code. Prof. Dr. Novopaschenny, head of that party returned to Berlin in the autumn of 1943, but his cryptanalysts were absorbed into the unit at HLS Ost.[929]

OKW/Chi also collaborated with the Agents' section of OKH/In 7/VI in the solution of Russian agent traffic. The memoranda of Fenner, chief linguist of OKW/Chi, give a detailed picture of the nature of this collaboration.[930]

On 23 February 1943, Fenner's department was asked by Section III of the Armed Forces Radio Defense Corps (Fu III) to collaborate with the Agents' section of OKH/In 7/VI in work on certain Russian agents' traffic. By the end of March, OKH/In 7/VI had furnished Fenner's section with all traffic in that system intercepted since September 1941 so that a start was made on solution. Fundamental findings were communicated to In 7/VI which enabled its Agents' section to break into the system roughly at the same

[929] IF 123 p 3

[930] D 60 pp 16ff

time as did Fenner's group. After the initial break-in, however, it was agreed that In 7/VI should continue the work on this system while the Signal Intelligence Agency of the Armed Forces started work on another system. From then on, relations became somewhat strained because of the non-cooperative attitude of the Agents' section of In 7/VI in furnishing traffic to Fenner's section. The basic cooperation of the two departments, however, is noteworthy.

One of the most striking instances of cooperation between the Signal Intelligence Agency of the Supreme Command of the Armed Forces (OKW/Chi) and the Signal Intelligence Agency of the Army High Command (OKH/GdNA and its predecessors) is manifest in the work of the two agencies on Polish Resistance Movement Systems.[931] During the years 1943/44, the Agents' section of AgN/NA was able to intercept and solve the systems used by the Poles in their traffic with the Polish government in London. From this traffic the disposition of the Polish liberation troops as well as the friction between them and the Russians could be established. The traffic was considered so important that eight members of the Agents' section were transferred in the autumn of 1943 to the Polish section of the Signal Intelligence Agency of the Armed Forces (OKW/Chi) to work on the systems there. The clear text was published by the Signal Intelligence Agency of the Armed Forces in bulletins with extremely restricted distribution. The Signal Intelligence Agency of the Armed Forces also cooperated by intercepting this traffic at their own station at Lauf in order to be certain that it was completely covered. Speed in solving the traffic was obtained by having the messages sent to the IBM section of AgN/NA for sorting. The work on Polish traffic thus appears to have been as much a joint project as is possible for two separate agencies to attempt.

Long before the time of official "Chi-conferences" held by Lt. General Gimmler, Chief of the Armed Forces Communications Branch (Chef Amtsgruppe Wehrmachtnachrichten Verbindungen, abbreviated Chef AgWNV), the Army and the Armed Forces, Signal Intelligence Services worked together on security studies of German cryptographic machines and issued joint resolutions concerning their investigations. Among the papers of Dr. Huettenhain of OKW/Chi are memoranda describing this cooperation.[932] As early as December 1942, In 7/VI, OKW/CHI and Wa Pruef 7 proposed issuing a statement concerning improvements for the secret teletypewriter machine SFM T-52c to be submitted to the "big executive committee."[933] Although it is not known specifically what is meant by the "big executive committee," it is possible that it may have been composed

931 I 115 p 9
932 D 59
933 D 59 p 6

of officials of these same organizations. Throughout 1943, General Thiele, who held the position of Chief of the Army Communications Branch (Chef Amtsgruppe Heeres Nachrichtenverbindungswesens, abbreviated Chef AgHNW) called conferences of representatives of the various services concerning matters of security. Buggisch, one of the mathematicians of In 7/VI, mentions conferences at which Drs. Stein and Hassenjaeger of OKW/Chi were present.[934] The minutes of one of these conferences (dated 13 December 1943) have been published.[935] It should be noted that the conference is said to have been called at the suggestion of In 7/IV, and was held in the office of that unit at Matthaikirchplatz 4, Berlin. Those who took part were Major Kempe, head of In 7/IV, Specialist Luehrs, Dr. Fricke, and Dr. Kehren, mathematicians of In 7/IV; Dr. Pietsch and Dr. Doering of AgN NA; representatives of Wa Pruef 7; and Dr. Huettenhain, Dr. Stein, and 1st Lt. Hasenjaeger, mathematicians of OKW/Chi. From this evidence, it is clear that the "Chi-conferences" called by Lt. General Gimmler in 1944 were only a formal exteriorization of an already existing relationship. This is the reason that Buggisch of AgN NA and Huettenhain of OKW/Chi were able to minimize the efforts of Lt. General Gimmler.[936] Both observe that the conferences did not foster a closer relationship among the services -- the cooperation of Army and Armed Forces had been of the closest nature for many years, but the collaboration with other services was not improved.

At the formal "Chi-conferences" and at the official Army-Air-Naval conferences of 1944, the Armed forces could always depend upon the full cooperation of the Army. The completeness of this cooperation is illustrated by the fact that when OKW/Chi was ordered to take over the supervision of all security studies within the Armed Forces, the Army compiled by transferring to OKW/Chi all personnel of In 7/IV and of the security sections of the Mathematical Section of AgN NA.

In the field of machinery used for cryptanalytic and security studies, the Armed Forces and the Army appear to have informed each other fully concerning their respective developments although no exchange of machinery was made. As early as 1939/40, the mathematicians and former actuaries who had been drawn into In/7IV suggested the use of IBM machinery for statistical studies. This led to an extensive use of the machinery for security studies. When security studies were transferred from In 7/IV to In 7/VI in 1942, IBM machinery was developed by In 7/VI for both security

934 I 58 p 3

935 D 59 p 16

936 I 92 p 4; I 84 p 2

studies and cryptanalytic work. It is not known whether the Signal Intelligence Agency of the Armed Forces had its own IBM machines separate from those of the Army or not.[937] Mettig and Buggisch both state that it had no IBM machinery, but depended upon the IBM machines of the Signal Intelligence Agency of the Army. The preparation of three-letter codes for the use of the Army was done, for instance, by the IBM machines of the GdNA at the request of the Signal Intelligence Agency of the Armed Forces.[938] In early 1945, the IBM section of GdNA was offered to the Signal Intelligence Agency of the Armed Forces (OKW/Chi); the transfer was never carried out, however, because of the turn of events.[939]

The relation of the Signal Intelligence Agency of the Supreme Command of the Armed Forces (OKW/Chi) and of the GdNA and its predecessors may be summarized as one of complete cooperation. Although the cryptanalytic problems of the two organizations were quite distinct, those of OKW/Chi dealing with diplomatic systems, of GdNA with Army systems, whenever joint problems were dealt with by the two agencies there was complete accord.

107. Liaison with the Navy.--The Signal Intelligence Agency of the Navy (Oberkommando des Marine, Seekriegsleitung, abbreviated OKM/4 SKL III) appeared to have little liaison with the Signal Intelligence Agency of the Army (GdNA and its predecessors). Tranow, the chief cryptanalyst of the Signal Intelligence Agency of the Navy, stated that the Navy cooperated with the Army until early 1944, but that thereafter the attempt at cooperation was given up since no results of value were obtained.[940]

The collaboration, where it existed, of the Signal Intelligence Agency of the Navy High Command with GdNA and its predecessors dealt principally with: the USA machine M-209, and IBM procedures.[941] In both instances, it so happened that the Navy received more from the Army than it gave.

a. Collaboration between OKM/4 SKL III and In 7/VI began in 1943 when In 7/VI passed over to the Signal Intelligence Agencies of the Navy and the Air Force the technique of recovering true settings from relative settings in M-209 solution. Thereafter, according to Lt. Muentz of OKM/4 SKL III there was considerable liaison between the three services in regard to M-209 and they exchanged all techniques.[942] Schulze, another

937 I 96 p 13; I 67 p 2
938 I 96 p 11
939 I 96 p 13
940 I 93 p 3
941 D 21 p 2
942 I 144 p 2

cryptanalyst in OKM/4 SKL III, stated that in his investigations of the M-209 he met Dr. Steinberg of In 7/VI and that they had a detailed conversation of the methods used by the German Army, Navy, and Air Force for solution of this system.[943] From these conversations he concluded that the Navy was superior in the matter of breaking into a message; the Army, in reconstructing the internal setting. This was mainly because the Army had more material to work on, and could depend upon having a few messages in depth every day, whereas the Navy never got traffic with identical settings. Schulze persuaded the Army to give the Navy some M-209 material in depth with which he could carry out experiments in OKM/4 SKL III to expedite the solution of the message.[944]

b. In regard to collaboration on IBM procedures, Tranow readily admitted that the Army first conceived the idea of using IBM machinery for cryptanalysis.[945] In March 1942, the Navy, Air Force, and Goering's Research Bureau (FA) visited the IBM section of In 7/VI in Berlin. "On this occasion," said Tranow, "I came to the conclusion that there were enormous possibilities in the IBM system for our work also." Tranow immediately set about to get some machinery for the Signal Intelligence Agency of the Navy, but found it difficult to obtain IBM machines at that time. From March to May or June 1942, the Signal Intelligence Service of the Navy sent work to the Naval Armaments Economic Section which was already using IBM machinery for statistical purposes. This Economic Section agreed to do the work on condition that Tranow furnish his own staff. Here again, Tranow had trouble, since the Signal Intelligence Agency of the Navy had very few IBM specialists in the ranks. He was forced to approach the Army and Air Force to obtain personnel in exchange for naval personnel of "equal value," as he is careful to point out. By May 1942, Tranow says, the Navy was able to carry out its own task.[946] According to Mettig, however, in June 1942, In 7/VI undertook a considerable volume of IBM work for the Signal Intelligence Agency of the Navy.[947] It seems reasonable to suppose that this is true, and that Tranow conveniently "forgot" this favor on the part of the Army. In September 1944, according to a Navy document, the Signal Intelligence Agency of the Navy was still "collaborating" with the Army on IBM procedure.

943 I 147 p 22
944 I 147 pp 22-23
945 I 146 p 17
946 I 146 p 17
947 I 78 p 12

As a matter of general policy, the Signal Intelligence Agency of the Navy High Command disapproved of indiscriminate exchange among the services. Lt. Muentz, stated that the head of his section Franke, disapproved of any contact with other services, and maintained contact only with the Army on M-209 solution. Lt. Schubert of GdNA complained that he personally could not bring about closer relations between the two agencies.[948]

> "I endeavoured to achieve cooperation between the Army and Navy. This task was actually no concern of mine. A naval officer was detached for six weeks who looked at all Army systems originating in the west and east and I went to him to attempt some settlement. I tried to achieve collaboration but later events upset things. There are practically no points of contact between the Army and Navy."

108. Liaison with the Air Force.--Before the German Air Force established its own Signal Intelligence Agency (OKL/LN Abt 350, formerly Chi-stelle OBdL) in 1937 the Army fixed intercept stations (Feste) intercepted foreign Air Force traffic and worked on it at the Intercept Control Station (Horchleitstelle). According to Major Fiechtner of the German Air Force, however, the Army did not give air traffic so much attention as it did ground force traffic and the Air Force became increasingly dissatisfied with the Army's work. In 1935, the Air Force began the formation of its own signal intelligence service, although for three years close relations with the Army were maintained. Air Force employees underwent familiarization training at Army Fixed Intercept Stations and the Air Force's first intercept stations were set up according to Army prototypes. By 1939, the dependence of the Signal Intelligence Agency of the Air Force High Command (OKL/LN Abt 350, formerly Chi-stelle OBdL) on the Signal Intelligence Agency of the Army High Command (GdNA and its predecessors) was ended.[949]

During the succeeding period (1939-1945) relations of the Air Force and Army were particularly good in field operations. This was fostered by such means as unification of Army and Air Force signal regulations, a regular exchange of liaison officers, working personnel, equipment, reports, raw traffic, and cryptanalytic methods. A few outstanding examples of Army-Air Force collaboration have been selected from multitudinous instances on every battle front.

[948] I 26 p 2

[949] IF 181 pp 14-15

We know from the minutes of a Chi-conference held in October 1944 that the Army and Air Force attempted to coordinate their signal regulations. According to the notes of the minutes preserved among the papers of Huettenhain, Lt. General Gimmler, Chef AgWNV, stated that one special difficulty in signal communications was the fact that the diverse parts of the Armed Forces used different wireless and cipher phraseology. In response to this, Lt. Col. Schulze of the German Air Force stated that by means of far-reaching assimilation of Army and Air Force regulations, the difficulties arising in those services from different wireless and cipher phraseology would soon be overcome.[950] This attitude of cooperation between Army and Air Force is typical and extended to all echelons.

A regular exchange of liaison officers between Army and Air Force field units was maintained both on the eastern and western fronts. In the west, from 1942 an Air Force liaison officer had been stationed with NAAS 5 at St. Germain.[951] Major Hentze, CO of KONA 5, stated that the two units worked closely together and Hentze showed familiarity with the unit there, its complement, and its work.[952]

One of the chief duties of the Army liaison officer at an Air Force signal intelligence post was to keep the ground situation map up to date from Air Force reports.[953] Among other duties, the Air Force liaison officer at an Army signal intelligence post passed requests to the Air Force for support.[954]

Friendly liaison between commanders and men of units of the Air Force and Army which were closely associated in the field must not be overlooked as a source of contact. Col. Muegge and Col. Rosenkrantz form an excellent example of this type of relationship. When Col. Muegge was commander of the Signal Intelligence Regiment 4 (KONA 4) in Athens, Col. Rosenkrantz, an old friend of his, was commander of the Air Force Signal Intelligence Unit stationed there. When Col. Muegge was moved in 1943 to Italy as commander of Signal Intelligence Regiment 7 (KONA 7), Col. Rosenkrantz happened to be commander of the Air Force signal intelligence in Italy and the friendly relationships of their units continued.[955]

Much of the interchange of men and equipment between field units of the Air Force and Army was caused by the fact that the Army had very few long distance direction-finding sets, and

950 D 57 p 14
951 IF 180 p 24
952 I 113 p 8
953 I 130 p 10
954 I 107 p 3
955 I 18 pp 4-6

depended upon equipment and reports from the Air Force to compensate for this deficiency. Major Oeljeschlaeger of the Air Force stated that the Army Signal Intelligence Regiments willingly detached direction-finding parties to reinforce the Air Force effort and that the Air Force was always open to receive Army direction-finding requests.[956] Muegge told interrogators that as commander of KONA 7 in Italy he borrowed two Air Force Direction Finding sets with long and short wave receptive powers from Rosenkrantz's unit and 'forgot' to give them back.[957] NAA-11 in Finland relied on the excellent Direction Finding reports of the Air Force and stated that these reports were furnished directly to NAA-11 whenever they were requested.[958]

Intelligence reports of all sorts were exchanged at every level of field intelligence. Army Group Headquarters received from the local Air Force which served its area copies of the Air Force's daily situation report and fortnightly summary.[959] These fortnightly summaries were sent by the Army Group Headquarters to Jodl who stated that they were well illustrated with sketches and plans.[960] Among the lower echelons, reports, summaries, and experiences of value were constantly interchanged between units of the KONA and the correlative air signal intelligence units. Reports from the Air Force were of particular importance in the identification of enemy concentrations. Major Oeljeschlaeger of the German Air Force stated that the Air Force was always quicker off the mark than the Army mobile ground forces. The enemy could sneak up against German positions by imposing radio silence, but long before this the Air Force would have advised the Army commands of significant moves of Air Force ground units.[961]

An interchange of traffic and methods of solution was also constantly maintained between the two services. Newly established Air Force traffic was handed over to Air Force units when it was intercepted by the Army,[962] and from 1943 on an interchange of cryptanalytic methods on both western and eastern fronts was normal. On the western front, traffic and methods of solution for USA traffic M-94, M-209, TELWA[963] were exchanged between NAAS 5 and western Air Force signal intelligence units. After

956 I 41 p 3
957 I 18 p 4
958 I 106 p 4
959 I 130 p 11
960 I 143 p 6
961 I 41 p 3
962 I 130 p 15
963 I 112 pp 4-6

Section B of the Signal Intelligence Agency of the Air Force High Command (OKL/LN Abt 350) moved to Paris following the invasion, messages encoded in Slidex were decoded at Paris by Section B, of the Signal Intelligence Agency of the Commander in Chief of the Air Force, and by NAAS 5 at St. Germain and were exchanged daily in the form of written reports.[964] On the southeastern front there was also an exchange of cryptanalytic procedure. Muegge of KONA 4 contacted the deciphering unit of the Air Force unit in Athens for aid in the solution of RAF four-figure traffic. Although neither unit had any success collaboration was maintained.[965] On the eastern front common problems of the Air Force units and Army Signal Intelligence Regiments were continuously worked on together.[966] Collaboration of LN 353 and KONA 1 and 8 is specifically mentioned.[967]

The most striking instance of field collaboration is shown at the time of the Dieppe raid. The Air Force intercept company which was responsible for monitoring landing traffic had good line connections with German fighter defense and Army forces responsible for defense against landing operations. The Air Force unit maintained continuous contact with the Army units involved and exploited their findings for immediate action by Air and Army. The Army signal intelligence headquarters passed on this intelligence to the higher headquarters, thus maintaining an effective division of labor with outstanding results. The work at Dieppr was publicised in the German newspapers and Goering praised it in a speech.[968]

In summary, the Army and Air Force maintained in their field relations the close working relationship with an exchange of personnel equipment, reports, traffic and cryptanalytic methods. Relations between the central agencies are less well known, but appear to have been adequate for all that was necessary. Operative systems on both fronts, such as USA M-94, M-209, Slidex, and Russian systems, were worked on jointly by Army and Air Force units in the areas where the systems were used and methods of solution exchanged.

109. Liaison with Foreign Office.--Relations of the Signal Intelligence Agency of the Army High Command (GdNA and its predecessors) and the cryptanalytic section of the Foreign Office (Pers ZS) were not close. This is to be expected both from the nature of their separate commitments (the GdNA dealing exclusively

964 I 112 p 9
965 IF 190 p 7
966 I 26 p 2
967 I 130 p 15
968 I 109 p 5

with Army systems, the Foreign Office with diplomatic) and from the well-known unwillingness of the Foreign Office to share any information.

Buggisch, a mathematician of In 7/VI said that he worked at one time on the Swiss model of the Enigma with Kunze, one of the cryptanalysts of the Foreign Office, and on a 5-figure de Gaulle code in 1941 and 1942.[969] Further than this there is, to our knowledge, no record of any cooperation between the two agencies. Jodl, Chief of Operations of the Armed Forces, stated that he did not receive the products of the Foreign Office bureau which went directly to the Foreign Minister, Von Ribbentrop. He knew from military lectures that the Foreign Office had broken some political traffic, but his knowledge was not direct.[970]

110. Liaison with Goering's Research Bureau. Liaison between the Signal Intelligence Agency of the Army High Command (the GdNA and its predecessors) and Goering's Research Bureau (FA) was characterized in general by narrowness of approach and mutual animosity of feeling. This was true, apparently, at every level. Jodl, Chief of Operations of the Armed Forces, told interrogators that he knew little about the Research Bureau:

> "It was a large office and efficiently organized, but Goering's special affair."[971]

Items of special interest from the Research Bureau were passed to Jodl from Keitel, in a special folder and Jodl returned them after perusal. He himself received nothing directly from the Research Bureau. Likewise, Goering stated that he never received copies of Army decodes as such, and had no opinion of the ability of the "Army bureau."[972]

Between the GdNA and the Research Bureau, liaison was apparently poor. Buggisch of In 7/VI stated that this was because Mettig, head of In 7/VI from 1941 to 1943, was opposed to the Storm Trooper taint of the Research Bureau.[973] Sauerbier, a lesser light in the Research Bureau, claimed that the narrowness of the department heads of the Research Bureau affected relations of that organization with other bureaus including the GdNA.[974]

Whatever liaison was carried on by the Goering's Research

969 I 58 pp 5-6
970 I 143 p 5
971 I 143 p 5
972 I 143 p 16
973 I 64
974 I 162 p 4

209

Bureau was done by a single representative and never involved any exchange of visits of operational personnel. Klautsche, who was liaison officer for the Research Bureau after 1943, maintained an office at the Signal Intelligence Agency of the Armed Forces (OKW/Chi) and passed on material to the Navy, Air Force, and Army.[975] Besides actual contact with GdNA, Klautsche is said to have passed on intelligence material to the Army General Staff, Western Armies Branch, and Eastern Armies Branch.[976]

The lack of contact between personnel of the Research Bureau and the GdNA is very apparent from interrogations. Fricke, a prominent mathematician of In 7/VI who was later transferred to OKW/Chi, stated that he had never seen any personnel from the Research Bureau until the war was over and they turned up in prison camps.[977] Sauerbier of the Research Bureau said he did not know a single person in another cryptanalytic bureau.[978]

There are a few instances of cooperation between the Research Bureau and the In 7/VI, but Buggisch, an Army cryptanalyst, insists that these were very rare.[979] One of the outstanding instances of effective collaboration occurred when the Research Bureau was having difficulty with a Turkish diplomatic code. The problem of solution and reading was turned over to In 7/VI. Traffic was intercepted by KONA 4 in Athens and relayed to the Balkan section of In 7/VI where it was broken and read until the capitulation. Decoded messages were forwarded to the Research Bureau.[980]

Buggisch stated that there was an exchange of results between the Research Bureau and In 7/VI in connection with some work of the Research Bureau on a Russian secret teleprinter in 1943. The Research Bureau had analyzed the machine and recognized that it must resemble the German SZ 40. When the Russians altered their system, the Research Bureau communicated the results of its investigations to the Mathematical Section of In 7/VI and was given in regurn a report on the solution of a German secret teleprinter. No more details of the incident are known, but Buggisch emphasizes the fact that this exchange of results was a very rare occurrence.[981]

[976] I 54 p 4
[977] I 20 p 8
[978] I 162 p 4
[979] I 176 p 6
[980] IF 126 p 8
[981] I 176 p 6

Collaboration between the Research Bureau and the Agents' section of In 7/VI is hinted in the statement that Wenzel, a civil employee of the Research Bureau, was sent from the Research Bureau by the Radio Defense Corps (FU III) to the GdNA to work on Polish Resistance Movement Systems.[982] Nothing more is known concerning the incident from TICOM sources.

Evidence indicates that under pressure, Goering's Research Bureau resorted to the GdNA and its predecessors for help in intercept solution, and editing of difficult traffic, but that in general the Research Bureau held itself aloof and disaffected.

111. Liaison with Finland-- Liaison with Finland was always close, both at HLS Ost, and in the eastern field units. Formal liaison at HLS Ost was maintained by a Finnish liaison officer stationed there. This officer in 1942 was a Lt. Mikkoja,[983] and he was succeeded by 1st Lt. Ohn. Army traffic of Russia, Poland, Rumania, and Sweden was exchanged. The Finnish General Staff is said to have handed over to the Germans a copy of the Russian 5-figure codes which was used by the Russians in the first year of the war with Germany.[984] The Germans had a high opinion of Finnish cryptanalysis. Dettman of HLS Ost stated that he had visited Finland in 1942 and had exchanged technical letters ever since that time with the Finns.[985]

Liaison in the field is known in some detail from the reports of NAA-11 when it was in Finland.[986] NAA-11 kept a signal intelligence liaison officer stationed with the main Finnish signal intelligence unit at Sortavala. This liaison officer, whose name was Riemerschmidt, had a direct radio link to NAA-11. Although the Germans of NAA-11 never went to Sortavala themselves, small Finnish parties did visit NAA-11 from time to time.[987]

The liaison between NAA-11 and the Finns can be divided into several types: traffic liaison, cryptographic liaison and technical liaison.[988]

In the field of traffic liaison, NAA-11 is said to have varied its cryptographic priorities to give full attention to any special links requested by the Finns through Riemerschmidt. NAA-11 also aided the Finns in traffic analysis, in which the

[982] I 26 p 7

[983] I 21 p 2

[984] I 78

[985] I 116 p 10

[986] I 55 I 106

[987] I 106 p 4

[988] I 106 pp 3-4

Finns were admittedly weak. NAA-11's systematic work and its ability to grasp intelligence from the analysis of small amounts of traffic was of great benefit to the Finns. D/F operations were coordinated very closely between the Finns and NAA-11. Here, on the other hand, NAA-11 relied heavily on the Finns who had D/F sets with long range. According to Riemerschmidt, a liaison observer was stationed by the Germans with the Finnish stations at Mikkeli, Ylene, Kemi, and Rovanieme for the specific purposes of observing long range D/F.

In the cryptanalytic field, NAA-11 neither gave nor received straight intelligence from the Finns but cryptanalytic procedures were exchanged. The Finns gave the Germans some very valuable information on Russian 3- and 4-figure ciphers which they had succeeded in reading. It is amusing to note in connection that Riemerschmidt passed to NAA-11 some information and solution of traffic in the Russian RZ 1800 code which hae had received at Sortavala from HLS Ost and this reached NAA-11 faster than did the direction transmission from HLS Ost to NAA-11.

Technical liaison was also handled by Riemerschmidt and this proved far more helpful to the Finnish radio telegraph company than to NAA-11. Finnish equipment was mostly of German make, with some British and a few American receivers. The Germans gave the Finns a great deal of advice concerning the operation of the machines and on one occasion they put their own apparatus and men at the disposal of the Finns for an operation in a key sector during a Russian offensive.[989]

112. Liaison with Italy-- Liaison between Germany and Italy was negligible because of the German lack of confidence in the Italians. There could be no exchange of information, or intelligence when the Germans were so apprehensive of the Italin cipher department that they thought it not competent enough to institute changes in cipher procedures even if the Italians desired to do so.

This lack of confidence on the part of the Germans was based on long experience with Italian codes and ciphers. As early as 1941, Captain Dr. Fiala, head of the Italian section of In 7/VI, was sent to Rome to inform the Italians of their code and cipher weaknesses.[990] The Germans were particularly apprehensive at this time because they feared that movements of German troops around North Africa were being betrayed to the British by messages of the Italian wireless. Dr. Fiala's visit, however, does not seem to have impressed the Italians who were confident of their

[989] I 106 p 3

[990] I 78 p 11

own systems, and the Germans tried another scheme.[991] In 1942, the Italians were invited to visit the IBM section of In 7/VI to observe the use of these machines for cryptanalytic and security work. Captain Bigi, a cryptanalyst of the Italian army, was sent by the Italians for this purpose.[992] Upon his return to Italy, the Italians did set up an IBM section of their own, but it did not function efficiently and the Germans despaired of improving Italian cipher or cryptanalytic methods.[993] In late 1942, the Italian section of In 7/VI which had monitored Italian traffic was dissolved by order of Hitler.[994]

After Italy's defection to the Allies, the Italian section of In 7/VI was revived from June 1943 until November 1943 when it was again disbanded.[995] During this brief period, however, no relations with Italy were maintained.

113. Liaison with Japan.--According to all evidence, there was very little liaison between the Army and Japan. In 1943, two Japanese officers visited the HLS Ost at Loetzen for about half a day. According to Dettman 7 HLS Ost they were given a polite reception but shown very little of anything and were given no hints as to what solutions the Germans had reached on Russian traffic. The Japanese stated that they had solved the Russian OKK 6 and OKK 7 but just what help, if any, they gave the Germans on these systems is not mentioned.[996] Buggisch emphatically stated that he had never seen any Japanese around "in the flesh" and that he knew of no liaison with Japan.[997]

At the end of the war, the Germans had decided to send a cryptologic mission to Japan by submarine. Included among the officers were Major Opitz, a German intercept officer, Schubert, of HLS Ost, and Morgenroth, a Navy cryptanalyst. How little the mission knew of Japanese Signal Intelligence agencies is shown by the fact that they did not know whom they were to contact when they got there but were to ask the German Counter Intelligence in Japan for further instructions.[998] The last minute plan could not be carried out because of the precipitate end of the war.[999]

991 IF 1524; IF 1519
992 I 78 p 11
993 I 78 p 11
994 I 100 p 2
995 I 100 p 2
996 I 116 p 9
997 I 64 p 3
998 IF 108 p 12
999 I 48 p 3

Only one instance is remarked on in TICOM interrogations of exchange between the Japanese and Germans. This occurred, according to Barthel, in connection with an Army field cipher machine captured by the Japanese. Nothing more is known of the incident.[1000]

[1000] IF 120 p 7

VOLUME 4

TAB A

AgN/NA (Amtsgruppe Nachrichten/Nachrichten Aufklaerung).--Department of Signals, Signal Intelligence. Name of cryptanalytic agency for non-Russian traffic 1943-1944 (successor to In 7/VI).
AHA (Allgemeines Heeres Amt.--General Army Office.
Air Signals Regiment.--Luftnachrichten Regiment (LN Regt).
Allgemeines Heeres Amt (AHA).--General Army Office.
Althans,_____, Corporal. Attached to NAAS 1.
AMEM. See Amtmann.
Amtmann (AMTM).--Specialist.
Amtsgruppe Nachrichten/Nachrichten Aufklaerung (AgN/NA).--Department of Signals, Signal Intelligence.
Andrae,_____, Lt. Col. Chief of Staff of Boetzel, Chief of Signal Intelligence Agency of Army High Command (OKH/GdNA).
Armed Forces Signal Troop School.--Fuehrungs Nachrichtentruppe Schule (FNS).
Army Communication Branch.--Heeres Nachrichten Verbindungsabteilung (HNV).
Army High Command.--Oberkommando des Heeres (OKH).
Army Ordnance, Development and Testing Group, Signals Branch.--Waffenpruefung (Wa Pruef).
Army Signal School.--Heeres Nachrichten Schule (HNS).
Army Signal Security Agency (1940-1942).--Inspectorate 7/IV (Inspektion 7/IV, abbreviated In 7/IV).
Arntz,_____, 1st Lieutenant. Aide-de-Camp to Praun. Chef WNV and Chef HNW.
Bailovic, Rudolf. Superior Governmental Councillor; former employee of Austrian Cryptanalytic Bureau; head of Balkan Section of In 7/VI; Specialist of Yugoslav systems of Tito and Mihailovic.
BANDWURM. Term used by the Germans to designate Russian Baudot letter "strip".
Barthel, Thomas. Member of KONA 7.
BAUDOT. A 32-character alphabet used in transmitting plain or enciphered teleprinter messages (corresponds to 26-letter Morse alphabet for hand-keying).
Befehlshaber Suedost.--Commanding Officer South-east.

Benold,_____, 1st Lieutenant. Commanding Officer of Close Range Signal Company (NAK Benold).

Berger, Georg, Inspector. In charge of documents in KONA 1.

Block,_____, Specialist. Head of Section 2, Group V, GdNA.

BLOCKNOT. Russian term, used by Germans to designate a one-time pad.

Boetzel,_____, Colonel. Chief of Signal Intelligence Agency of Army High Command (OKH/GdNA) 1944-1945. Had been Chief of Code and Cipher Section of German War Ministry 1934-1939.

Boscheinen, Heinz, Non-Commissioned Officer. Turkish Interpreter; Member of Bailovic's section at In 7/VI and also worked in Evaluation.

Breede,_____, Inspector (?). Member of British section of In 7/VI during 1941 and worked on Typex.

Buggisch, Otto, Dr. Cryptanalyst of In 7/VI.

Buschenhagen,_____, Lieutenant. Chief of Code and Cipher Section of German Defense Ministry 1919-1927.

Chef der Heeresruestung und Befehlshaber des Ersatzheeres.--Chief of Army Equipment and Commander of the Replacement Army (Chef H Ruest u BdE).

Chef der Wehrmacht Nachrichten Verbindungen (Chef/WNV).--Chief Signal Officer, Armed Forces.

Chef des Heeres Nachrichtenverbindungswesens (Chef/HNW).--Chief Signal Officer, Army.

Chef/GdNA (Chef/General der Nachrichten Aufklaerung).--Chief, Signal Intelligence Service.

Chef/General der Nachrichten Aufklaerung (Chef/GdNA).--Chief, Signal Intelligence Service.

Chef/HNW (Chef der Heeres Nachrichtenverbindungswensens.--Chief Signal Officer, Army.

Chef H Ruest u. BdE (Chef der Heeresruestung und Befehlshaber des Ersatzheeres.--Chief of Army Equipment and Commander of the Replacement Army.

Chef/WNV (Chef der Wehrmacht Nachrichten Verbindungen.--Chief Signal Officer, Armed Forces.

Chief of Army Equipment and Commander of the Replacement Army.--(Chef der Heeresruestung und Befehlshaber des Ersatzheeres (Chef H Ruest u. BdE).

Chief, Signal Intelligence Service.--Chef/General der Nachrichten Aufklaerung (Chef/GdNA).

Chief Signal Officer, Armed Forces.--Chef der Wehrmacht Nachrichten Verbindungen (Chef/WNV).

Chief Signal Officer, Army.--Chef der Heeres Nachrichten-verbindungswesens (Chef/HNW).

Chiffrierabteilung/Reichswehrministerium.--Code and Cipher Section/German Defense Ministry.

Chiffrier Stelle des Oberbefehlshabers der Luftwaffe (Chi-Stelle OBdL).--Signal Intelligence Agency of the Commander in Chief of the Air Force.

Chi-Stelle OBdL (Chiffrier Stelle des Oberbefehlshabers der Luftwaffe)--Signal Intelligence Agency of the Commander in Chief of the Air Force.

Close Range Signal Intelligence Company.--Nachrichten Nahaufklaerung Kompanie (NAK).

Close Range Signal Intelligence Platoon.--Nachrichten Nahaufklaerungszug (NAZ).

Code and Cipher Section/German Defense Ministry.--Chiffrierabteilung/Reichswehrministerium.

Combined Staffs Detailed Interrogation Center.--CSDIC.

Commander in Chief South.--Oberbefehlshaber Sued.

Commander in Chief West.--Oberbefehlshaber West.

Commanding Officer South-east.--Befehlshaber Suedost.

Control Station of Signal Intelligence--Leitstelle der Nachrichten Aufklaerung (LNA). Central evaluating agency of Army High Command 1942-1944.

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

CSDIC.--Combined Staffs Detailed Interrogation Center.

D-60. Miscellaneous papers from a file of RR Dr. Huettenhain of OKW/Chi. A TICOM publication.

Denffer, von. Mathematician in In 7/IV and In 7/VI.

Dettmann, Alex, 1st Lieutenant. Head of cryptanalysis at HLS Ost; later head of section 3, Group IV of GdNA. Specialty: Russian systems.

D-18. "Russian Decryption in the Former German Army" by Dettmann and Samsonow. See T-805.

Doering, _____, Dr. Mathematician with In 7/VI, later GdNA. Specialty: Machine cipher, mathematical research.

Esterhazy, Paul, Count Wachtmeister. Member of Balkan section of In 7/VI.

Exter, Karl. Attached to NAA-11.

FA (Forschungsamt).--Goering's Research Bureau.

FAK (Nachrichten Fernaufklaerung Kompanie).--Long Range Signal Intelligence Company.

FAZ (Nachrichten Fernaufklaerungszug).--Long Range Signal Intelligence Platoon.

Feichtner, Ferdinand, Major. Commanding Officer of LN Regt 352 (German Air Force).

Fellgiebel, _____, General. Chief of Code and Cipher Section of German Defense Ministry 1931-1932; Chief Signal Officer of Army High Command and of Supreme Command of Armed Forces 1942-1944; Killed in July 1944 after attempt on Hitler's life.

Feste. 1923-1939: Abbreviation for Feste Horchstelle (Fixed Intercept Station); 1939-1945: Abbreviation for Feste Nachrichten Aufklaerungsstelle (Stationary Intercept company).

Feste Horchstelle (Feste).--Fixed Intercept Station.

Feste Nachrichten Aufklaerungsstelle (Feste).--Stationary Intercept Company.

FF (Funkfernschreib).--USA non-morse radio teletype.

Fiala,_____, Captain. Head of Italian Section of In 7/VI during 1941-1942.

Fixed Intercept Station.--Feste Horchstelle (Feste).

FNS (Fuehrungs Nachrichtentruppen Schule).--Armed Forces Signal Troop School.

Forschungsamt (FA).--Goering's Research Bureau.

Fricke, Walter, Dr. Mathematician and cryptanalyst: In 7/VI 1941-1942; posted to In 7/IV in 1942; transferred in 1944 to OKW/Chi IIb. Specialty: Production of codes and ciphers, security studies of Army systems.

Fuehrungs Nachrichtentruppe Schule (FNS).--Armed Forces Signal Troop School.

Funkfernschreib (FF).--USA non-morse radio teletype.

Geheime Kommandosache (GKdoS).--Secret.

General Army Office.--Allgemeines Heeres Amt (AHA).

General der Nachrichten Aufklaerung. (GdNA).--Signal Intelligence Agency.

Gerlich, Wilhelm, Dr. Attached to NAAS 1 (of KONA 1). Specialty: Russian systems.

German Defense Ministry.--Reichswehrministerium.

German War Ministry.--Reichskriegsministerium.

Gimmler,_____, Major General. Chief Armed Forces Communications.

GKdoS. See Geheime Kommandosache.

Goering's Research Bureau.--Forschungsamt (FA).

Gorzolla,_____, Captain. Head of Group III, Signal Intelligence Agency of the Army High Command (OKH/GdNA).

Graul, Arno. Member of NAAS of KONA 1. Invented radio "fingerprinter."

Graupe,_____, Corporal. Member of In 7/VI 1942-1943, and later member of FAK 624, NAAS 5 of KONA 5. Deserted in August 1944.

Habel,_____, Captain. Successor to Seebohm as commanding officer of FAK 621 in North Africa. Captured February 1943.

HASSO (Horchauswertestelle Suedost).--Intercept Evaluation Station Southeast.

Hauptreferat.--Main Section.

Heeres Nachrichten Verbindungsabteilung (HNV).--Army Communication Branch.

Heeres Nachrichten Schule (HNS).--Army Signal School.

Heimann, Wilhelm, Corporal. Specialty: Russian procedure, call signs, and frequencies.
Hentze, Rudolf, Major Dr. Head of Group IV, Signal Intelligence Agency of the Army High Command (OKH/GdNA).
Herbrueggen,_____, Captain. Head of Personnel Section of In 7/VI in 1941.
Hertzer, Ernst, Major. Commanding Officer of KONA 1.
Hertzfeld, Heintz Wolfgang, Corporal. Member of Gruppe IV, GdNA; formerly member of British, Italian, Balkan sections In 7/VI.
Heudorf,_____, Corporal. Member of NAA 8.
Hilburg,_____, Corporal. Member of Mathematical Section of In 7/VI.
HLS (Horchleitstelle).--Intercept Control Station. Central cryptanalytic and evaluating agency 1933-1941.
HLS Ost (Horchleitstelle Ost).--Intercept Control Station East.
HNS (Heeres Nachrichten Schule).--Army Signal School.
HNV (Heeres Nachrichten Verbindungsabteilung).--Army Communications Branch.
Hoeh Kdr d NA (Hoeherer Kommandeur der Nachrichten Aufklaerung).--Senior Commander of Signal Intelligence.
Hoeherer Kommandeur der Nachrichten Aufklaerung (Hoeh Kdr d NA).--Senior Commander of Signal Intelligence.
Hoeppner,_____, Lt. Col. Commanding officer of KONA 8 in 1944.
Holetzko,_____, Captain. Member of LN Regt 353.
Horchauswertestelle Suedost (HASSO).--Intercept Evaluation Station Southeast.
Horchleitstelle (HLS).--Intercept Control Station. Central cryptanalytic and evaluating agency 1933-1941.
Horchleitstelle Ost (HLS Ost).--Intercept Control Station East.
Horchzug.--Intercept platoon.
Huettenhain, Erich, Dr. Cryptanalyst of Signal Intelligence Agency of Supreme Command of Armed Forces (OKW/Chi).
Huchting, Leonhard, Pfc. Attached to Feste 10.
I-2. "Interrogation of Dr. Huettenhain and Dr. Fricke at Flensburg, 21 May 1945." A TICOM publication.
I-3. "Uebersicht der Russischen Chi Verfahren (Nov. 1940-May 1945)." A TICOM publication.
I-7. "Statement of Major McIntosh on Uffz. Graul." A TICOM publication.
I-15. "Interrogation of Oblt. Schubert." 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-18. "Interrogations of Oberst Muegge, O.C. of NA 4 and NA 7 of German Army Sigint Service." A TICOM publication.

I-19 A-G. "Report on Interrogation of KONA 1 at Revin, France June 1945." 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, RR Dr. Huettenhain, Sdf. Dr. Fricke and Oblt. Schubert (OKW/Chi), 15 June 1945." A TICOM publication.

I-23. "Interrogation of Major Ernst Hertzer, German Army Signals Intelligence Service (KONA 1)." A TICOM publication.

I-26. "Interrogation of Oblt. Schubert (OKH/Chef HNW/Gen.d.NA) on Russian Military and Agents' Systems." A TICOM publication.

I-30. "Report on Interrogation of Uffz. Karrenberg at Steeple Claydon on 7th July 1945 at 1100 a.m." A TICOM publication.

I-33. "Report on Traffic Analysis of BAUDOT Traffic by Capt. Jack Magilavy, A.U.S. and D.R. Uzielli, SIXTA." A TICOM publication.

I-36. "Translation of Paper Written by Reg. Rat. Dr. Huettenhain and Sonderfuehrer Dr. Fricke of OKW/Chi, Sections A.III and B.V." 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-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-51. "Interrogation Report on Uffz. Herzfeld, Heintz Wolfgang, and Translation of a Paper he Wrote on the British War Office Code." A TICOM publication.

I-52. "Papers Written by Uffz. Herzfeld on Mihailovic and Tito Ciphers." A TICOM publication.

I-55. "Interrogation of Seven Members of NAA 11." A TICOM publication.

I-58. "Interrogation of Dr. Otto Buggisch of OKW/Chi." A TICOM publication.

I-59. "Interrogation of Uffz. Arno Graul at Revin." A TICOM publication.

I-60. "Further Interrogation of Oblt. Schubert of OKH/Chef HNW/Gen.d.NA." A TICOM publication.

I-62. "Field Interrogation of Paul Ratz of the German Army Signals Intelligence (1933-1945)." A TICOM publication.

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 C.S.D.I.C. on approx. 1 Aug. and 10 Aug. 1945." A TICOM publication.

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-74. "Interrogation Report on Obgefr. Keller, formerly Auswertestelle 4 and Nachrichten Aufklaerungskompanie 611." A TICOM publication.

I-75. "Interrogation Reports on German Field Sigint Personnel carried out at Buffer - Ltn. August Schroeder, Ltn. Starke, Obegefr. Heudorf, and Hptm. Holetzko." A TICOM publication.

I-76. "Interrogation Reports on Lehwald, Haupts, Klett and Lauerbach." Also I-76 Supplement (Diagrams). A TICOM publication.

I-78. "Interrogation of Oberstlt. Mettig on the History and Achievements of OKH/AHA/In 7/VI." A TICOM publication.

I-80. "P.O.W. Interrogation Report - Obgefr. Clement Schuck Insp. VII/6 (OKH)." A TICOM publication.

I-84. "Further Interrogation of R.R. Dr. Huettenhain and Sdf. Dr. Fricke 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-92. "Final Interrogation of the Wachtmeister Otto Buggisch (OKH/In 7/VI and OKW/Chi)." A TICOM publication.

I-96. "Interrogation of Oberstlt. Mettig on the Organisation and Activities of OKW/Chi." A TICOM publication.

I-98. "Interrogation of Oberst Randewig on German Deception Plans." A TICOM publication.

I-99. "Interrogation Report of Hptm. Herbert Roeder (Head of Gruppe VI, Gen.d.NA, OKH, 1944-45)." A TICOM publication.

I-100. "Report by Uffz. Herzfeld of NAAST 5 (Gen. d. NA) on the Work of the Italian Referat of In 7/VI." A TICOM publication.

I-106. "Final Interrogation Report on the Norway Party (NAA 11). A TICOM publication.

I-111. "Further Interrogation of Oberstlt. Mettig of OKW/Chi on 14th September 1945." 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 (Funküberwachung)." 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 C.S.D.I.C. on or about 28th August 1945." A TICOM publication.

I-122. "Interrogation Report on Obergefreiter Hansa (OKH/Gen d. NA)." A TICOM publication.

I-125. "Interrogation Report on Anton Stock of OKH/Gen. d. NA." 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-136. "Homework by Regierungsrat Dr. Huettenhain and Sdf. (Z) Dr. Fricke on Hagelin B.211." A TICOM publication.

I-137. "Final Report written by Wachtmeister Otto Buggisch of OKH/Chi and OKW/Chi." A TICOM publication.

I-142. "P/W Barthel's Account of German Work on British, American, Swedish, and French Machine Ciphers." A TICOM publication.

I-143. "Report on the Interrogation of Five Leading Germans at Nuremberg on 27th September 1945." A TICOM publication.

I-149. "Report by Uffz. Karrenberg and Colleagues on Allied Cypher Machines." A TICOM publication.

I-153. "Second Interrogation of Uffz. Karrenberg of OKH on the Baudot-Scrambler Machine ('Bandwurm')." A TICOM publication.

I-154. "Interrogation of Uffz. Rudolph Schneider of In 7/VI." A TICOM publication.

I-156. "Report of preliminary interrogation of Wilhelm Gerlich, AIC 1900, carried out by 3rd U.S. Army, 28th September 1945." A TICOM publication.

I-157. "Chart of Communications Within a Russian Army Drawn up by Uffz. Karrenberg." A TICOM publication.

I-160. "Homework by Sonderfuehrer Kuehn of Gen. d. NA on General Organisation and Work of French Referat." A TICOM publication.

I-161. "Further Statements on Typex by Huettenhain, Fricke, and Mettig." A TICOM publication.

I-164. "Homework by Kurt Sauerbier of RLM/Forschungsamt on Russian Agents' Traffic." A TICOM publication.
I-166. "Report by Uffz. Karrenberg on Russian Cryptographic Course." A TICOM publication.
I-167. "Report by the Karrenberg Party on the NKVD." A TICOM publication.
I-168. "Report by the Karrenberg Party on Miscellaneous Russian W/T." A TICOM publication.
I-169. "Report by Uffz. Karrenberg on the Bandwurm." A TICOM publication.
I-170. "Report on French and Greek Systems by Oberwachtmeister Dr. Otto Karl Winkler of OKH/FNAST 4." A TICOM publication.
I-171. "Report on Work on Russian Systems by Wachtmeister Berger of FNAST 6." A TICOM publication.
I-173. "Report by the Karrenberg Party on Russian W/T." A TICOM publication.
I-175. "Report by Alfred Pokorn of OKH/Chi on M.209." A TICOM publication.
I-176. "Homework by Wachtmeister Dr. Otto Buggisch of OKH/Chi and OKW/Chi." A TICOM publication.
I-178. "Homework by Hptm. Boedigheimer of IV/Nachr. Regiment 506." A TICOM publication.
I-179. "Homework by Obwm. Riel, of Stoerbefehlsstelle Balkan." A TICOM publication.
I-180. "Homework by Uffz. Keller of In 7/VI and WNV/Chi." A TICOM publication.
I-191. "Homework of Dr. Wilhelm Gerlich on Russian Systems." A TICOM publication.
IF-5. "Notes on Field Interrogation of Various German Army and Air Force Signal Intelligence Personnel on 18/20 May 1945." From TICOM.
IF-15. "Final Report of TICOM Team 1 on the Exploitation of Kaufbeuren and the Berchtesgaden area." From TICOM.
IF-40. "Final Report of TICOM Team 2." From TICOM.
IF-105. Two reports. First: Interrogation report on POW Heinz Boscheinen and Walter Kotschy. Second: Summary interrogation report. From Headquarters, 3rd US Army, SIS.
IF-107. "Interrogation of POW Werner K.H. Graupe regarding German Cryptographic Organization and Solution of Allied Codes."
IF-108. "Interrogation of Oblt Arntz." CSDIC (U.K.) SIR 1606.
IF-109. "Report on Information Obtained from Oblt Arntz. CSDIC (U.K.) SIR 1646.
IF-115. "Interrogation Report on Willy Grube." 6824 DIC (MIS) M.1185.
IF-117. "Interrogation Report on Willy Grube." 6824 DIC (MIS) M. 1190.
IF-120

IF-120 "First detailed Interrogation Report on Thomas Barthel." CSDIC/CMF/Y 40.

IF-122 "Third Detailed Interrogation Report on Gerd. Coeler." CSDIC/CMF/Y 38, 31 May 1945.

IF-123 "Consolidated Report on Information obtained from the following: Erdmann, Grubler, Hempel, Karrenberg, Schmitz, Suschowk." CSDIC (U.I.) SIR 1717.

IF-126 "Interrogation Report on Schwartze and Graupe." CSDIC (U.K.) SIR 1335.

IF-127 "Interrogation Report on Schwartze and Graupe." CSDIC (U.K.) SIR 1374.

IF-130 "Copy of MIS Dossier on Fellgiebel." From Captured German Army Official Dossier now in MIS Files, Pentagon.

IF-131 "Detailed Interrogation Report--Notes on Signal Intelligence (Monitoring)." 6824 DIC (MIS) M. 1080 18 March 1945.

IF-162 "Report on Preliminary Evaluation of German Equipment for interception of Russian Multichannel teletype circuits."

IF-171 "Report on Further Information obtained from Uffz. Kotschy and Uffz. Boscheinen both from Festungs art Abt. 1518, deserted Diffenbach." CSDIC (UK) SIR 1346.

IF-172 "Report on Further Information obtained from Uffz. Kotschy and Uffz. Boscheinen both Festungs art Abt 1518, deserted at Diffenbach 22 Nov. 1944." CSDIC (UK) SIR 1341 20 Dec. 1944.

IF-176 Seabourne Report, Vol. III. "Operation and Techniques of the Radio Defense Corps, German Wehrmacht."

IF-181 Seabourne Report, Vol. VI. "Origins of the Luftwaffe SIS and History of Its Operations in the West."

IF-190 "The Organization and History of the Cryptographic Service Within the German Army." CSDIC (UK) SIR 1704 8 July 1945.

IF-202 "Report on Information Obtained from PW Uffz Boscheinen, both of Fest Art Abt 1518, deserted at Diffenbach, 22 Nov. 44." CSDIC (UK) SIR 1326.

In 7/IV (Inspektion 7/IV, Inspectorate &/IV). Army Signal Security Agency 1940-1942; Army Agency for production of Army systems 1942-1944.

Inspektion 7/IV, Inspectorate 7/IV (In 7/IV). Army Signal Security Agency 1940-1942; Army Agency for Production of Ciphers 1942-1944.

Inspectorate 7/IV, Inspektion 7/IV (In 7/IV). Army Signal Security Agency 1940-1942; Army Agency for Production of Codes for Army 1942-44.

In 7/VI (Inspektion 7/VI, Inspectorate 7/VI). Central cryptanalytic agency of the German Army High Command 1941-1942. Central cryptanalytic agency of the German Army High Command for non-Russian traffic 1942-1943.

Inspektion 7/VI, Inspectorate 7/VI (In 7/VI). Central cryptanalytic agency of the Army High Command 1941-1942. Central cryptanalytic agency of the Army High Command for non-Russian traffic 1942-1943.

Inspectorate 7/VI, Inspektion 7/VI (In 7/VI). Central cryptanalytic agency of the Army High Command 1941-1942. Central cryptanalytic agency of the Army High Command for non-Russian traffic 1942-1943.

Intercept Control Station.--Horchleitstelle (HLS). Central cryptanalytic and evaluating agency of the Army High Command 1933-1941.

Intercept Control Station East.--Horchleitstelle Ost (HLS Ost).

Intercept Evaluation Station Southeast.--Horchauswertestelle Suedost (HASSO).

Jering, Karl, Tech. Sgt. Attached to Chi-Stelle / OBdL.

Jodl, Alfred, General. Chief of Armed Forces Operations Staff, OKW.

Karrenberg,_____, Corporal. Attached OKH/GdNA. Cryptographer on enciphered Baudot Traffic.

Kettler,_____, Col. Head of HLS Ost 1942; Chief of Signal Intelligence Agency of Supreme Command of the Armed Forces (OKW/Chi) 1942-1945.

Kneschke,_____. Head, section 2, Group IV, Signal Intelligence Agency of Army High Command (OKH/GdNA)

Koebe,_____, Lt. Chief of Understaff, Signal Intelligence Agency of the Army High Command (OKH/GdNA).

Koehler,_____, Technician. Head of linguistic section 1941-1945.

Kommandeur der Nachrichten Aufklaerung (KONA).--Signal Intelligence Regiment.

KONA (Kommandeur der Nachrichten Aufklaerung).--Signal Intelligence Regiment.

Kopp,_____, Col. Senior Commander of Signal Intelligence late 1944. Attached to C in C West.

Kotschy, Walter, Non Commissioned Officer. Hungarian Interpreter. Worked in Italian section of Afrika Korps. Trained in "encoding and decoding" at In 7/VI.

Kuehn,_____, Senior Inspector. Head of training section of In 7/VI 1941-1945 (later head of section 5, Group IV GdNA).

Kuehne, Hans Wolfgang, Technician. Head of French section In 7/VI from 1941 to Feb. 1945.

Lechner,_____, Major. Chief In 7/VI 1943; Commander KONA 6 1945.

Lenz. Waldemar, Doctor O/Funker. Member of French section In 7/VI; later in Paris. Involved in Schulze-Boysen Case.

Leitstelle der Nachrichten Aufklaerung (LNA).--Control Station of Signal Intelligence. Central evaluating agency of Army High Command 1942-1944.

Liebknecht,_____, Cryptanalyst in OKW/Chi.

Liedtke,_____, O/Insp. Head of English section of In 7/VI until 1943. Specialty: British codes.

LNA (Leitstelle der Nachrichten Aufklaerung).--Control Station of Signal Intelligence. Central evaluating agency of Army High Command 1942-1944.

LN Regt. (Luftnachrichten Regiment).--Air Signals Regiment.

Loeffler, Lt. Harry. Attached to Stationary Intercept Company 10 (Feste 10)

Long Range Signal Intelligence Company.--(Nachrichten Fernaufklaerung Kompanie (FAK).

Long Range Signal Intelligence Platoon.--(Nachrichten Fernaufklaerungszug (FAZ).

Lueders,_____, 1st Lt. Head of Mathematical section, sub-section 7 of In 7/VI.

Luftnachrichten Regiment (LN Regiment).--Air Signals Regiment.

Luzius,_____, Doctor Corporal. Mathematician in USA section of In 7/VI Specialty: M-209.

Main Section.--Hauptreferat.

Manaigo,_____, Corporal. Head of Italian section 1943, In 7/VI.

Mang,_____, Major. Organized In 7/VI in 1942; Chief In 7/VI 1941-1942.

Marquardt,_____, Captain. Commanding Officer NAAS 4. Head of Group 14, Sub Section 1a, of Signal Intelligence Agency of Army High Command.

Martini,_____,General. Chief Signal Officer of the Air Force.

Menzer,_____. Member of OKW/Chi.

Mettig,_____, Lt. Colonel. Signal Officer since 1933; Head, In 7/VI from November 1941 to June 1943; Second in command of OKW/Chi from December 1943 to April 1945.

Mje-Koja,_____, 1st Lt. Finnish liaison officer at Loetzen (HLS OST)

Moravec,_____, Lt. Adjutant to Boetzel, Chief of Signal Intelligence Agency of Army High Command (GdNA).

NAA (Nachrichten Aufklaerung Abteilung).--Signal Intelligence Battalion.
NAA/Chef H Ruest B d E (Nachrichten Aufklaerung Abteilung Chef der Heeresruestung u, Befehlshaber des Ersatzheeres).--Signal Intelligence Regiment of the Replacement Army.
NAAS (Nachrichten Aufklaerung Auswertestelle).-- Signal Intelligence Evaluation Center.
Nachrichten Aufklaerung Abteilung (NAA).-- Signal Intelligence Battalion.
Nachrichten Aufklaerung Abteilung/Chef der Heeresruestung u, Befehlshaber des Ersatzheeres (NAA/Chef H Ruest B d E).--Signal Intelligence Regiment of the Replacement Army.
Nachrichten Aufklaerung Auswertestelle (NAAS).--Signal Intelligence Evaluation Center.
Nachrichten Aufklaerungs Ersatz und Ausbildungs Abteilung (NAEuAA).-- Signal Intelligence Replacement and Training Battalion.
Nachrichten Dolmetscher Ersatz und Ausbildungs Abteilung (NDEuAA).--Signal Interpreter Replacement and Training Battalion.
Nachrichten Fernaufklaerung Kompanie (FAF).-- Long Range Signal Intelligence Company.
Nachrichten Fernaufklaerungszug (FAZ).--Long Range Signal Intelligence Platoon.
Nachrichten Nahaufklaerung Kompanie (NAK).--Close Range Signal Intelligence Company.
Nachrichten Nahaufklaerungszug (NAZ).--Close Range Signal Intelligence Platoon.
NAEuAA (Nachrichten Aufklaerungs Ersatz und Ausbildungs Abteilung).--Signal Intelligence Replacement and Training Battalion.
NAK (Nachrichten Nahaufklaerung Kompanie).--Close Range Signal Intelligence Company.
NAZ (Nachrichten Nafhrichten Nahaufklaerungszug).--Close Range Signal Intelligence Platoon.
NDEuAA (Nachrichten Dolmetscher Ersatz und Ausbildungs Abteilung).--Signal Interpreter Replacement and Training Battalion.
NKVD (Narodni Kommissariat Vnutrinikh Del).--Peoples' Commissariat for Internal Affairs.

Novopaschenny,_____,Prof. Member of Signal Intelligence Agency of Supreme Command of Armed Forces (OKW/Chi) and of In 7/VI.

Oberbefehlshaber Sued.--Commander in Chief South.
Oberbefehlshaber West.--Commander in Chief West.
Oberkommando der Luftwaffe/General Nachrichten Fuehrer/Abteilung III (OKL/Gen Na Fue/III).--Signal Intelligence Service of the Air Force High Command.
Oberkommando des Heeres/Allgemeines Heeres Amt/Amtsgruppe Nachrichten/Nachrichten Aufklaerung (OKH/AHA/AgN/NA).--Signal Intelligence Department of Signals, General Army Office, Army High Command.
Oberkommando des Heeres (OKH).--Army High Command.
Oberkommando des Heeres/General der Nachrichten Aufklaerung (OKH/GdNA).--Signal Intelligence Agency of the Army High Command.
Oberkommando der Marine/Seekriegsleitung/III (OKM/SKL IV/III).--Signal Intelligence Agency of the Navy High Command.
Oberkommando der Wehrmacht/Chiffrierabteilung (OKW/Chi).--Signal Intelligence Agency of the Supreme Command of the Armed Forces.
Oberkommando der Wehrmacht, Wehrmacht Nachrichten Verbindungs Funkueberwachung (OKW/WNV/FU).-- Radio Defense Corps_____.
Oeljeschlaeger, Franz, Major. Chief of Group II, Division III of the Chief Signal Office.
OHN,_____, 1st Lt. Finnish liaison officer at Loetzen (HLS Ost).
OKH (Oberkommando des Heeres).--Army High Command.
OKH/AHA/AgN/NA (Oberkommando des Heeres/Allgemeines Heeres Amt/Amtsgruppe Nachrichten/Nachrichten Aufklaerung).--Signal Intelligence Department of Signals, General Army Office, Army High Command.
OKH/GdNA (Oberkommando des Heeres. General der Nachrichten Aufklaerung).--Signal Intelligence Agency of the Army High Command.
OKL/Gen Na Fue/III (Oberkommando der Luftwaffe/General Nachrichten Fuehrer/Abteilung III).-- Signal Intelligence Service of the Air Force High Command.
OKM/SKL IV/III (Oberkommando der Marine/Seekriegsleitung/IV/III).--Signal Intelligence Agency of the Navy High Command.
OKW/Chi (Oberkommando der Wehrmacht/Chiffrier Abteilung).--Signal Intelligence Agency of the Supreme Command of the Armed Forces.

OKW/WNV/FU (Oberkommando der Wehrmacht, Wehrmacht Nachrichten Verbindungen Funküberwachung)--Radio Defense Corps of the Armed Forces High Command.
ORPO (Ordnungspolizei).--Regular Police
Ordnungspolizei (ORPO).--Regular Police
Oschmann,_____, Major. Chief of Code and Cipher Section of German Defense Ministry 1932-1934.
Osten-Sacken, von der, Baron Col. Head of HLS Ost 1942-1944. Implicated in plot on Hitler's life 20 July 1944 and committed suicide.
Pale, Erkki, Captain in Reserve. Chief of Finnish Crypt. Outfit at Sortanala.
Peilzug,_____. Direction Finding Platoon.
Peoples' Commissariat for Internal Affairs.--NKVD
Pers ZS (Sorderdienst des Referats Z in der Personal Abteilung des Auswaertigen Amtes).--Cryptanalytic Section of the Foreign Office.
Pietsch,_____. Baurat Dr. Sonderfuehrer, Head of Mathematical Section of In 7/VI (later Section 1 of Group IV, GdNA).
Praun,_____, General. Chief Signal Officer, Armed Forces, Chief Signal Officer Army 1944-1945 (Chef WNV Chef HNW).
Preuss,_____, 1st Lieutenant. Commanding Officer of Close Range Signal Company (NAK Preuss).
Radio Control Station.--Rundfunkueberwachungsstelle.
Radio Defense Corps of the Armed Forces High Command, (OKW/WNV/FU).--Oberkommando der Wehrmacht, Wehrmacht Nachrichten Verbindungs Funküberwachung.
Radio Intercept Station.--Wetterfunkempfangsstelle, (W-Stelle).
Randewig,_____, Col. Commander of Western Intercept Stations 1939 C.O. of Hoeh. Wehrmachts Nafue z.b. V 700.
Referat,_____. Section
Reichs Kriegsministerium.--War Ministry [term used during 1935-1938, later changed into Oberkommando der Wehrmacht].
Reichswehrministerium.--German Defense Ministry.
Rhinow,_____, Corporal. Member of Mathematical Section of In 7/VI.
Riemerschmidt,_____, 1st Lt. German Army liaison officer at RTK (Finnish Crypt. Outfit).
Roeder, Herbert, Captain. Head of Gruppe VI, Gen.d.NA, OKH, 1944-45.
Roessler, Capt. Chief Evaluator with KONA 1, Commanding Officer of NAAS 1.
Rohdan,_____, Pfc. Head of Swedish section of AgN/NA 1943.

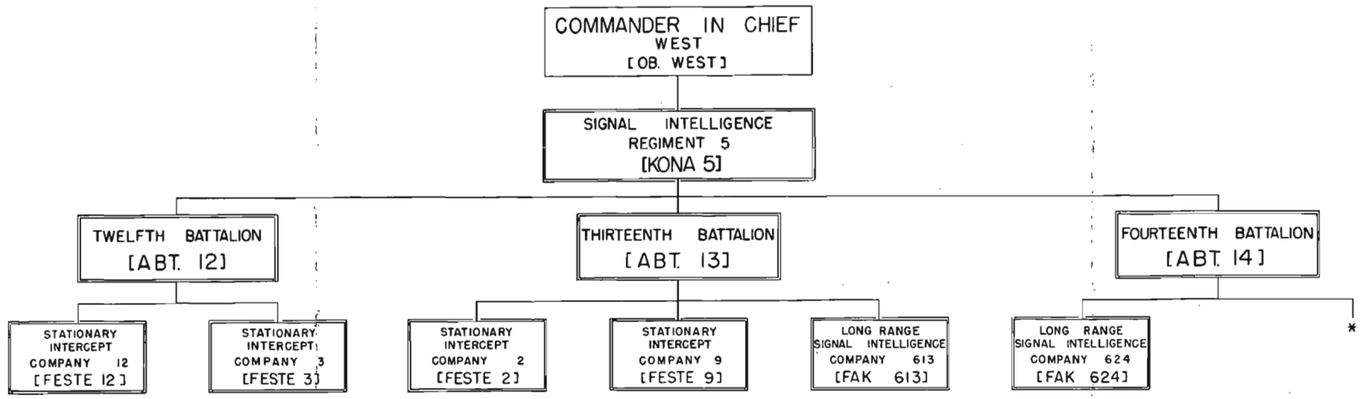
Rundfunkueberwachungstelle.--Radio Control Station.
Samsonow, Sergius, Master Sergeant. Head of Section 3a of Group IV. Specialty: Russian Secret Police Systems (NKWD).
Sauerbier, Kurt. Member of FA. Worked on Russian Agents' Code.
Schenke, Specialist. Head of IBM section of In 7/VI 1942-1945.
Schmidt,_____, Captain. Commanding Officer of NAA 11, head of 'Norway Party'.
Schmidt,_____, Major. Head of Code and Cipher Section of German Defense Ministry 1927-1931.
Schubert,_____, 1st Lt. Expert on Russian and Polish Army and Agents' Codes and Ciphers.
Section.--Referat.
Seebohm,_____. Commander of FAK 621 in North Africa until capture July 1942.
Seemueller,_____, Lt. Col. C.O. of KONA 4 Feb. 1943-April 44.
Sendezug,_____. Communication Platoon.
Senior Commander of Signal Intelligence.--Hoeherer Kommandeur der Nachrichten Aufklaerung (Hoeh Kdr d NA).
Signal Intelligence, Department of Signals, General Army Office, Army High Command.--Oberkommando des Heeres/ Allgemeines Heeres Amt/Amtsgruppe Nachrichten/ Nachrichten Aufklaerung (OKH/AHA/AgN/NA).
Signal Intelligence Agency of the Army High Command.--Oberkommando des Heeres/General der Nachrichten Aufklaerung OKH/GdNA).
Signal Intelligence Agency of the Commander in Chief of the Air Force.--Chiffrierstelle des Oberbefehlshabers der Luftwaffe, abbreviated (Chi-Stelle, OBdL).
Signal Intelligence Agency of the Navy High Command.--Oberkommando der Marine/Seekriegsleitung IV/III (OKM/SKL/ IV/III).
Signal Intelligence Agency of the Supreme Command of the Armed Forces.--Oberkommando der Wehrmacht/Chiffrier Abteilung (OKW/Chi).
Signal Intelligence Battalion.--Nachrichten Aufklaerung Abteilung (NAA).
Signal Intelligence Evaluation Center.--Nachrichten Aufklaerung Auswertestelle (NAAS).
Signal Intelligence Regiment.--Kommandeur der Nachrichten Aufklaerung (KONA).

Signal Intelligence Regiment of the Replacement Army.--Nachrichten Aufklaerung Abteilung/ Chef der Heeresruestung u. Befehlshaber des Ersatzheeres, (NAA/Chef H Ruest B d E).
Signal Intelligence Replacement and Training Battalion.--Nachrichten Aufklaerungs Ersatz und Ausbildungs Abteilung (NAE u AA).
Signal Intelligence Service of the Air Force High Command.--Oberkommando der Luftwaffe/ General Nachrichten Fuehrer/ Abteilung III (OKL/Gen Na Fue/III).
Signal Interpreter Replacement and Training Battalion.--Nachrichten Dolmetscher Ersatz und Ausbildungs Abteilung (NDE u AA).
Sorderdienst des Referats Z in der Personalabteilung des Auswaertigen Amtes (Pers ZS).--Cryptanalytic Section of the Foreign Office.
Specialist, See Amtmann (AMTM).
Starke,_____, Lt. Attached to NAK on the Eastern front.
State Police.--Ordnungspolizei(ORPO).
Stationary Intercept Company.--Feste Nachrichten Aufklaerungsstelle (Feste).
Steinberg, Dr. Technician. Mathematic section of In 7/VI; later section 1 of Group IV, GdNA; Worked on USA systems--M 94 and M 209.
T-805 "Russian Decryption in the Former German Army" by Dettmann and Samsonow. See: DF-18.
Thomas,_____, Pfc. Attached to NAAS 1.
USA non-morse radio teletype.--Funkfernschreib (FF).
Vaatz,_____, 1st Lt. German Air Force Liaison officer with Finnish Hq's at Mikkeli.
Vauck,_____,1st Lt. Head of Agents Section In 7/Vi 1942-1945.
Waffen pruefung (Wa Pruef).--Army Ordnance, Signal Equipment Testing Laboratory.
Wa Pruef (Waffen Pruefung). Army Ordnance, Development and Testing Group, Signal Branch.
Wehrmacht Nachrichten Verbindungen/Funkueberwachung (WNV/FU).--Radio Defense Corps.
Wenzel,_____, Specialist. Attached to Forschungsamt (FA).
Wetterfunkempfangsstelle (W-Stelle).--Radio Intercept Station, [Weather].
W-Stelle (Wetterfunkempfangsstelle).-- Radio Intercept Station.
Winkler, Oscar, Corporal. Member of KONA 4.

GERMAN ARMY SIGNAL INTELLIGENCE SERVICE IN THE WEST

CHAIN OF COMMAND

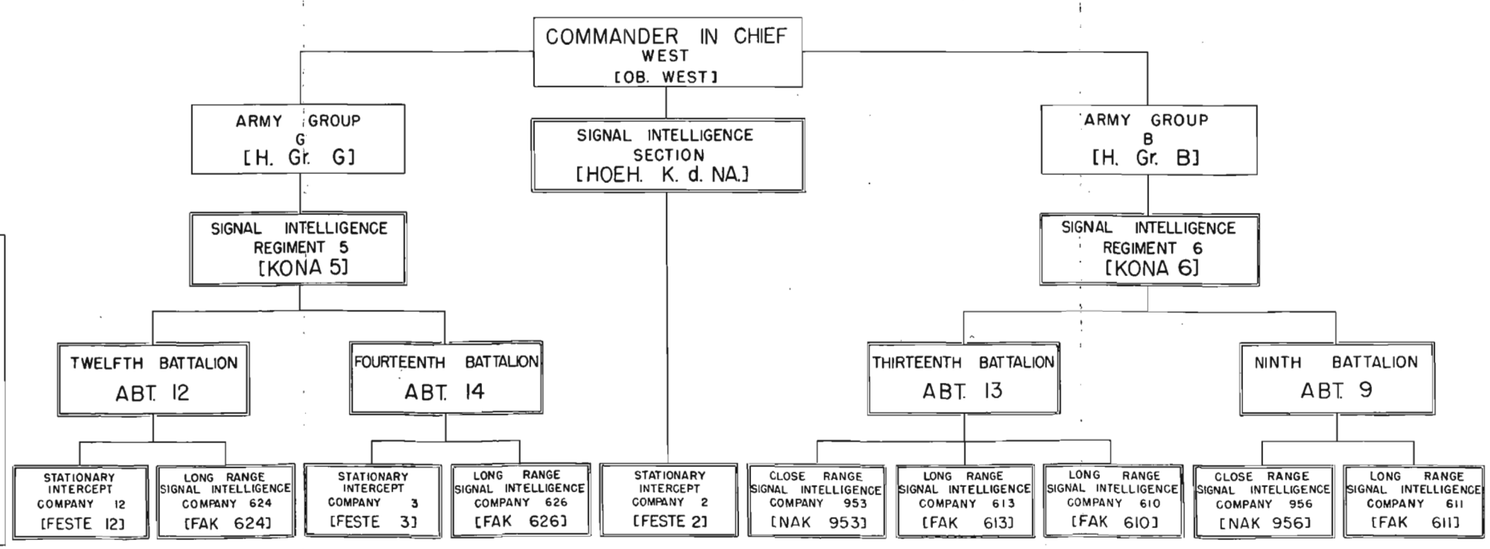
SPRING 1944



GERMAN ARMY SIGNAL INTELLIGENCE SERVICE IN THE WEST

CHAIN OF COMMAND

JANUARY 1945



LEGEND

ABT.	–	ABTEILUNG
FAK	–	FERNAUFKLAERUNGSKOMPANIE
FESTE	–	FESTE HORCHSTELLE
H. Gr.	–	HEERESGRUPPE
HOEH. K.d. NA.	–	HOEHERER KOMMANDEUR DER NACHRICHTEN-AUFKLAERUNG
KONA	–	KOMMANDEUR DER NACHRICHTENAUFKLAERUNG
NAK	–	NAHAUFKLAERUNGSKOMPANIE
OB.	–	OBERBEFEHLSHABER
*		OTHER COMPANIES, IF ANY, NOT KNOWN

GERMAN ARMY SIGNAL INTELLIGENCE REGIMENT OPERATIONS CHART

(BASED ON "KONA 1")

LOW LEVEL TRAFFIC

IDENTIFIED HIGH LEVEL TRAFFIC

UNIDENTIFIED HIGH LEVEL TRAFFIC

CLOSE RANGE SIGNAL INTELLIGENCE PLATOON (2 OR 3 PER COMPANY)	
R/T INTERCEPT 12 OPERATORS	W/T INTERCEPT 3 OPERATORS
DIRECTION FINDING 5 OPERATORS	EVALUATION 3 PERSONS

G2 OF ARMY CORPS

CLOSE RANGE (MOBILE) SIGNAL INTELLIGENCE COMPANY
(2 PER REGIMENT)

INTELLIGENCE COORDINATION
10 PERSONS (ESTIMATED)

LONG RANGE (MOBILE) SIGNAL INTELLIGENCE COMPANY
(2 PER REGIMENT)

DIRECTION FINDING 50 OPERATORS	INTERCEPT 80 OPERATORS
CRYPTANALYSIS 16 PERSONS	EVALUATION 30 PERSONS

STATIONARY INTERCEPT COMPANY
(1 PER REGIMENT)

INTERCEPT 80 OPERATORS	DIRECTION FINDING 50 OPERATORS
EVALUATION 30 PERSONS	CRYPTANALYSIS 16 PERSONS

G2 OF ARMY

SIGNAL INTELLIGENCE EVALUATION CENTER

(1 PER REGIMENT)

CRYPTANALYSIS 60 PERSONS	TRAFFIC ANALYSIS 80 PERSONS (ESTIMATED)
EVALUATION 70 PERSONS (ESTIMATED)	

G2 OF ARMY GROUP

Other Signal Intelligence Regiments
OKH/GDNA
GAF Signal Intelligence

TOTAL PERSONNEL (Including 580 Overhead) — 1330

LEGEND

- WIRELESS INTERCEPTION
- FLOW OF RAW TRAFFIC
- FLOW OF INTELLIGENCE
- ENEMY TRANSMITTER

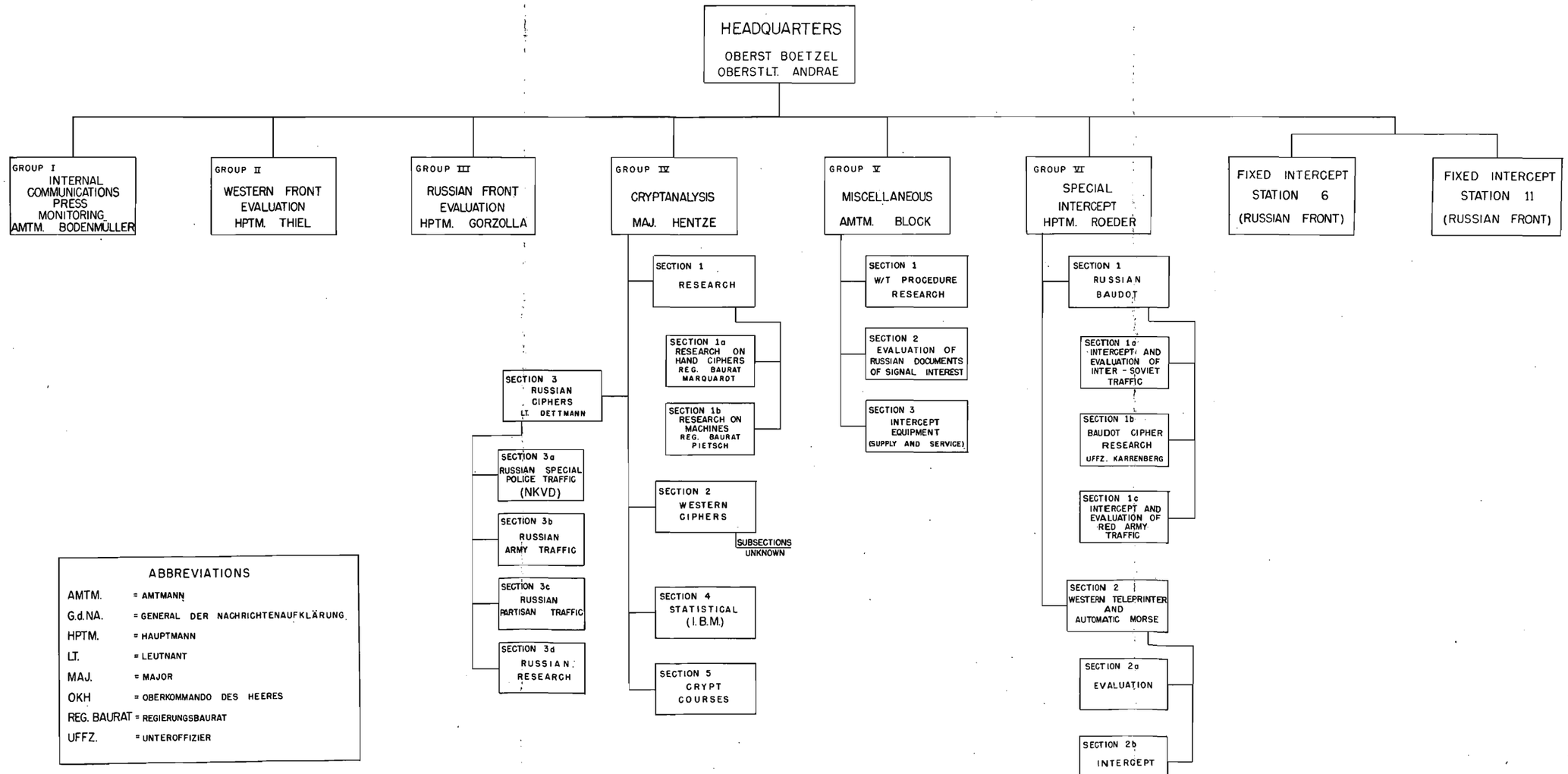
CHART NO.

TOP SECRET

SIGNAL INTELLIGENCE AGENCY OF ARMY HIGH COMMAND

(OKH/G.d. NA.)

FROM OCTOBER 1944 – MAY 1945



ABBREVIATIONS

AMTM.	= AMTMANN
G.d.NA.	= GENERAL DER NACHRICHTENAUFKLÄRUNG
HPTM.	= HAUPTMANN
LT.	= LEUTNANT
MAJ.	= MAJOR
OKH	= OBERKOMMANDO DES HEERES
REG. BAURAT	= REGIERUNGSBAURAT
UFFZ.	= UNTEROFFIZIER

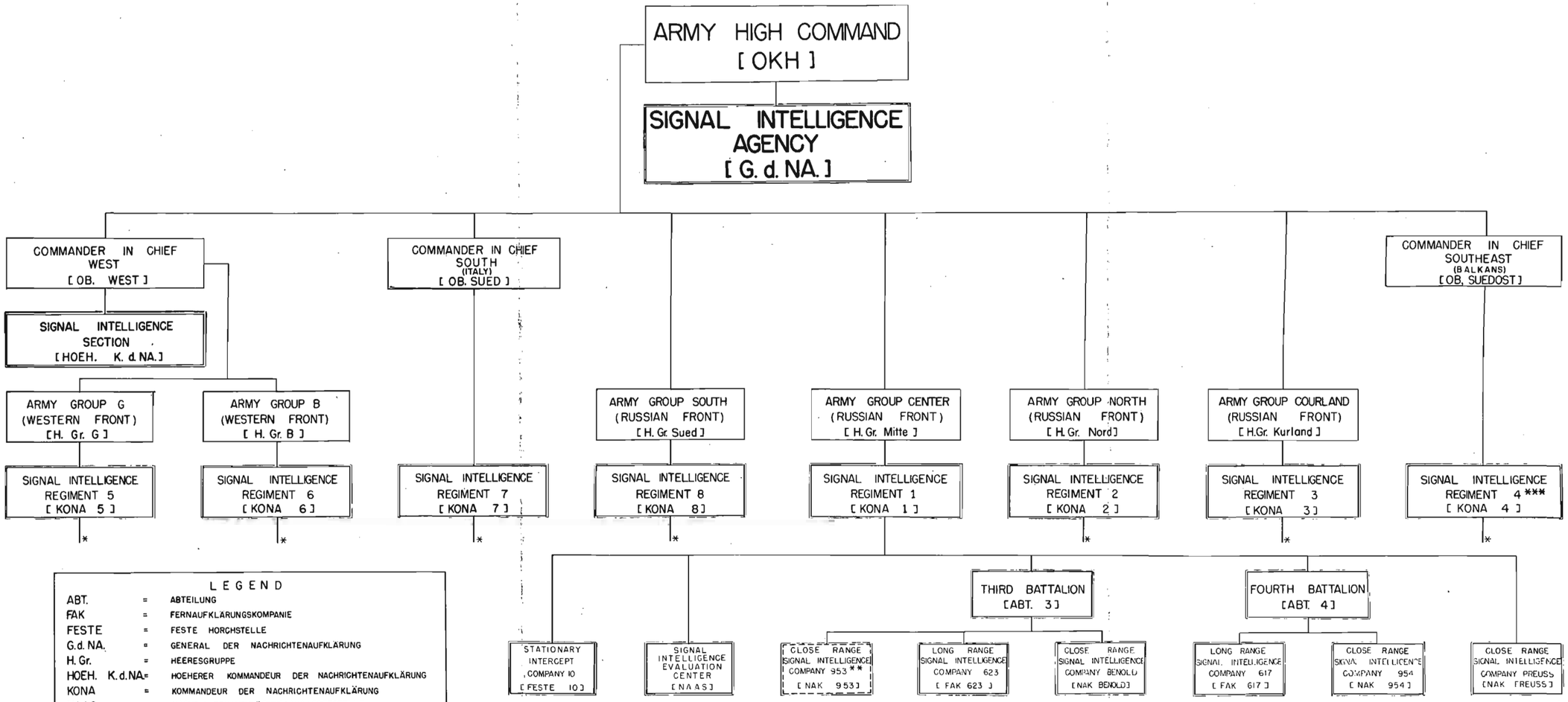
ESTIMATED PERSONNEL (including intercept) — 700

CHART NO.

GERMAN ARMY SIGNAL INTELLIGENCE SERVICE

CHAIN OF COMMAND

JANUARY 1945



LEGEND

ABT.	=	ABTEILUNG
FAK	=	FERNAUFKLÄRUNGSKOMPANIE
FESTE	=	FESTE HORCHSTELLE
G.d. NA.	=	GENERAL DER NACHRICHTENAUFKLÄRUNG
H. Gr.	=	HEERESGRUPPE
HOEH. K.d.NA.	=	HOEHERER KOMMANDEUR DER NACHRICHTENAUFKLÄRUNG
KONA	=	KOMMANDEUR DER NACHRICHTENAUFKLÄRUNG
NAAS	=	NACHRICHTENAUFKLÄRUNGSAUSWERTESTELLE
NAK	=	NAHAUFKLÄRUNGSKOMPANIE
OB.	=	OBERBEFEHLSHABER
OKH	=	OBERKOMMANDO DES HEERES
*	=	SIMILAR TO KONA 1
**	=	CLOSE RANGE SIGNAL INTELLIGENCE COMPANY 953 SENT TO WESTERN FRONT. RUSSIAN SPECIALISTS RETAINED TO FORM NAK BENOLD AND NAK PREUSS
***	=	LOCATED AS SHOWN THROUGH FALL 1944

GRAND TOTAL PERSONNEL — ESTIMATED AT 12,000

CHART NO.

WNV/Fu/III (Wehrmacht Nachrichten Verbindungswesen Funkueberwachung III).--Radio Defense Corps.
Wollny, Oblt. Commanding Officer of Feste 6; formerly Commanding Officer of NAZ W of KONA 4.
Zillmann,_____, Senior Inspector. Head of British section of In 7/VI 1941.
Zipper,_____, Inspector. Head of section 1, Group V GdNA.