DOCID: 3560861

~~TOP SECRET CREAM~~

~~SECRET~~
By Authority of the
Commanding General
Initials Date

ARMY SECURITY AGENCY

Washington, D. C.

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

EUROPEAN AXIS SIGNAL INTELLIGENCE IN WORLD WAR II AS REVEALED BY "TICOM" INVESTIGATIONS AND BY OTHER PRISONER OF WAR INTERROGATIONS AND CAPTURED MATERIAL, PRINCIPALLY GERMAN

In Nine Volumes

Do NOT Destroy Return to the
NSA Technical Library when no longer needed
5-3724 Copy No. 1
FHV

VOL. I

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

DO NOT DESTROY OR MUTILATE
RECORD COPY

~~TOP SECRET CREAM~~

DOCID: 3560861

VOLUME 1	SYNOPSIS
VOLUME 2	NOTES ON GERMAN HIGH LEVEL CRYPTOGRAPHY AND CRYPTANALYSIS
VOLUME 3	SIGNAL INTELLIGENCE AGENCY OF THE SUPREME COMMAND, ARMED FORCES
VOLUME 4	SIGNAL INTELLIGENCE SERVICE OF THE ARMY HIGH COMMAND
VOLUME 5	THE GERMAN AIR FORCE SIGNAL INTELLIGENCE SERVICE
VOLUME 6	THE FOREIGN OFFICE CRYPTANALYTIC SECTION
VOLUME 7	GOERING'S "RESEARCH" BUREAU
VOLUME 8	MISCELLANEOUS
VOLUME 9	GERMAN TRAFFIC ANALYSIS OF RUSSIAN COMMUNICATIONS

DOCID: 3560861

VOLUME 1--SYNOPSIS

DOCID: 3560861

VOLUME 1 SYNOPSIS

Paragraph

Origin of "TICOM"..... 1
The European Axis cryptanalytic effort against United States communications..... 2
Organization of German Signal Intelligence Agencies.... 3
The Signal Intelligence Agency of the Army High Command..... 4
The Signal Intelligence Agency of the Air Force High Command..... 5
The Signal Intelligence Agency of the Navy High Command..... 6
The Signal Intelligence Agency of the Supreme Command Armed Forces..... 7
The German Foreign Office Cryptanalytic Section..... 8
Goering's "Research" Bureau..... 9
Collaboration between German Signal Intelligence Agencies in Cryptographic Matters.....10
Collaboration between German Signal Intelligence Agencies in Cryptanalytic Matters.....11

a. Relationships between Foreign Office Cryptanalytic Section, Goering's "Research" Bureau, and the Signal Intelligence Agency of the Supreme Command Armed Forces.
b. Military Agency Relationships--exchanges of cryptanalytic information.
c. Military Agency Relationships--exchanges of personnel.
d. Military Agency Relationships--cooperation with regard to IBM and Rapid Analytic Machinery.
e. Military Agency Relationships--cooperation with regard to interception.
f. Cooperation between Military and Civilian Agencies on solution of Agents' systems.

DOCID: 3560861

Paragraphs
Other Axis (European) Cryptanalytic Agencies..... 12
a. Italian Cryptanalytic Agencies.
b. The Hungarian Cryptanalytic Agency.
c. The Austrian Cryptanalytic Agency.
d. The Finnish Cryptanalytic Agency.
e. The Bulgarian Cryptanalytic Agency.
Liaison between German Signal Intelligence Agencies and other Axis Cryptanalytic Agencies..... 13
a. Liaison with Japan.
b. Liaison with Italy.
c. Liaison with Hungary.
d. Liaison with Finland.
e. Liaison with Spain and Bulgaria.
Chart summarizing results of European Axis Cryptanalysis..... 14

1. Origin of "TICOM".-- The word "TICOM" served as a cover name for a special project and for an organization, the "Target Intelligence Committee." The project, which was originally conceived by Colonel George A. Bicher, Director of the Signal Intelligence Division, ETOUSA, in the summer of 1944, aimed at the investigation and possible exploitation of German cryptologic organizations, operations, installations, and personnel, as soon as possible after the impending collapse of the German armed forces. Colonel Bicher elicited and secured the support of the U. S. Navy and of the British, and accordingly a joint and combined "Target Intelligence Committee" was established in England in October 1944, by the authority of the Chief of Staff, United States Army; the Commander-in-Chief, United States Fleet; and the Chairman, London Sigint Board.

DOCID: 3560861

The Target Intelligence Committee originally planned airborne operations, even before the German collapse, to seize important German signal intelligence targets, known from Ultra material and prisoner of war interrogations. There were four objectives:

a. To learn the extent of the German cryptanalytic effort against England and America;

b. To prevent the results of such German cryptanalysis against England and America from falling into unauthorized hands as the German Armies retreated;

c. To exploit German cryptologic techniques and inventions before they could be destroyed by the Germans; and

d. To uncover items of signal intelligence value in prosecuting the war against Japan.

The TICOM mission was of highest importance. American cryptographers did not then know with certainty the extent to which United States communications were secure or insecure, nor did they know the extent of the enemy's cryptanalytic abilities, strength, and materiel, except by conjecture, by inference from Anglo-American cryptanalysis of German systems and from prisoner of war interrogations. German cryptanalytic successes were obviously unpublicized. They were reflected instead in higher casualty lists and lessened success on the part of Allied tactics and strategy.

In the Spring of 1945, however, conditions for the proposed operations became rapidly unsatisfactory. The known German signal intelligence agencies were dispersing or retreating to other localities in greatest disorder. Pinpoint locations could not be established. The possibility was remote that Anglo-American parachute units could seize worthwhile personnel and material and hold them through the confusion of major battles. Therefore, in March, 1945, TICOM decided instead to alert six United States-British target exploitation teams in England, these teams to be sent into enemy territory as either United States or British troops overran it, where they were to take over and exploit known or newly discovered targets of signal intelligence interest and to search for other signal intelligence targets and personnel.

The first exploitation team was dispatched in April 1945 to the Neumuenster-Flensburg area, and other teams were quickly dispatched to other areas as soon as overrun. The odyssies of the TICOM teams striving to locate and exploit signal intelligence targets during the confused days before and after the German capitulation, make entertaining as well as instructive reading. They are fully recorded in the TICOM publications.[1] A short summary of these operations is given in Volume 8, Chapter X, of this report.

The results obtained from these TICOM efforts were impressive. Approximately 4000 separate German documents were captured.[2] This material weighed 5 tons. Many cryptographic devices and machines were captured. One hundred and ninety six reports, based on interrogation of German signal intelligence personnel, together with other miscellaneous reports and translations were issued by TICOM.

The true value of the TICOM effort is not measurable in such statistics. Its importance lies rather in what the TICOM effort revealed to American cryptologists concerning German signal intelligence, with particular reference to American systems. The TICOM prisoner of war interrogations and captured documents, with the interrogations conducted by other Anglo-American agencies (notably the Combined Services Detailed Interrogation Centre, or "CSDIC") have given Anglo-American investigators a reasonably complete picture of German signal intelligence. The United States Army Security Agency has obtained from these interrogations and documents information useful in assessing its own cryptanalytic and cryptographic achievements, especially its own development of rapid analytic machinery, the state of its research in cryptography, and the cryptographic security of American systems.

1. See IF 15, IF 40, IF 51, IF 101, IF 165, IF 166, IF 167, and I-1.

2. By "document" is meant either one or a collection of papers, books, files of correspondence, messages, films, worksheets or other items of intelligence value, to which a TICOM document number was assigned for convenience in classification and handling.

DOCID: 3560861

2. The European Axis cryptanalytic effort against United States communications.--From TICOM sources it is learned that European cryptanalysts were unable to read any U. S. Army or Navy high-level cryptographic systems. The Army Converter M134C (SIGABA), the Army Teletypewriter Cipher Attachment known as the Converter M-228 (SIGCUM), the Army Teletypewriter Privacy Set (SIGIBS), the Army High Security Teletypewriter Cipher System (SIGTOT), the Army Speech Equipment RC-220-T1 (SIGSALY), the Combined Cipher Machine (CCM), the Navy Electric Cipher Machine Mark III (ECM, identical with SIGABA), and the Navy Teletypewriter Cryptographic Attachment (C. S. P. 1515, identical with the Army Converter M-228) were completely secure. One Army Strip system (System No. 47 or 67) and one Navy strip system (probably C. S. P. 1404) were read for short intervals until the principle of strip elimination was introduced. The low-grade ciphony device (Speech Equipment AN/GSQ-1, or SIGJIP) was not read, although theoretical solutions were worked out.

Both of the unenciphered War Department Telegraph Codes (SIGRIM and SIGARM) were read by the Germans. Hungary received photostatic copies of War Department Confidential Code Number 2, probably from the Bulgarians, together with at least one set of cipher tables, and the Italians reconstructed subsequent editions of the enciphering tables. The compromise appears to have been shared with other Axis powers, notably Germany, Finland and Japan. Military Intelligence Code No. 11 (physically compromised), used by the Military Attache in Cairo, was read throughout the summer of 1942. The Germans read messages in several versions of the Division Field Codes.

German cryptanalysts solved from 10 per cent to 30 per cent of intercepted U. S. Army M-209 messages. Save where keys were captured, it was usually read too late to be of tactical value. Messages sent by the U. S. Army in Slidex, Codex, Bomber Code, Assault Code, Aircraft Movement Code, Map Coordinate Codes, and Cipher Device M-94 where employed, were read regularly and almost 100 per cent.

Combined Naval Cypher No. 3, used by the U. S. Navy and the Royal Navy for Atlantic Convoy operations, was read almost 100 per cent by the Germans from the end of 1941 through the middle of 1943. The solution of this system was perhaps for the allies the most disastrous signal intelligence success achieved by the Germans. Allied convoy shipping losses suffered during this period were six times as great as during any other comparable period.

The Germans engaged in intensive and successful traffic analysis activities against United States Army and Army Air Force radio communications. This included direction-finding, analysis of call sign and frequency allocation systems, analysis of plain text and operator's chat, as well as more complex operations, such as air-borne radar route tracking, and monitoring of transmitter zero beat tuning.

The U. S. Army Converter M-134A (SIGMYC), and the U. S. Navy Cipher Machine (HCM), furnished by the Navy to the State Department, were not read by the Germans. The State Department Strip systems O-1 and O-2 were solved, the former probably through a compromise, and the latter through cryptanalysis. Several State Department codes, including the Brown Code (unenciphered) and Code A-1 (enciphered), were compromised and read, probably from 1938 and 1939, respectively.

From an intelligence standpoint the results obtained by the German cryptanalytic successes were important, but not decisive. American Army and Navy strategy was secure as long as high level systems were employed. Tactical operations, however, did suffer. The Anglo-American convoy shipping losses during 1942 and early 1943 were huge, largely because of German successes with Combined Naval Cypher No. 3. German traffic analysis and cryptanalysis provided a comprehensive order of battle for the U. S. Army and Army Air Forces in the United Kingdom, in the Mediterranean, and on the continent. According to a German air force officer, "no attack of the Eighth Air Force came as a surprise." The value of the intelligence which the Germans got from State Department codes and strip ciphers is not accurately known. The strip systems were probably read too late to be of any great value. The compromise

DOCID: 3560861

of Military Intelligence Code No. 11 did provide intelligence of unquestioned tactical value, particularly in the summer of 1942 during Rommel's advance to Egypt.

The German cryptanalytic effort against Russian military communications was even greater than that made against the United States. The German successes in solution of medium and low grade English military and naval communications systems were considerable. The cryptanalysis of the diplomatic communications of Italy, Japan, France, Turkey, Bulgaria, Greece, Portugal, Spain, Switzerland, and other smaller nations also achieved important results.

A tabulation of the results of German and other European Axis cryptanalysis, country by country, is given in Chart 1-2, at the end of this Volume. These results will be discussed also in the subsequent volumes on the separate German agencies.

3. Organization of German Signal Intelligence Agencies.-- Germany possessed six main cryptologic organizations during World War II, with a total strength, including field units and overhead, of approximately 30,000 persons. Italy possessed two main signal intelligence organizations; Finland, Austria, and Hungary each had one. The grand total of European Axis personnel engaged in signal intelligence in World War II is estimated as 36,000.

This number is small when compared with the numbers engaged in the Anglo-American effort. The grand total of Anglo-American signal intelligence personnel at the end of the War, including all services and including field and overhead personnel, was in excess of 60,000 persons. Out of this total, the United States Army employed approximately 28,000 persons.

Of the six main German cryptologic organizations, four were military, and two were civilian.

The four military organizations were:

a. The Signal Intelligence Agency of the Army High Command (OKH/GdNA), which dealt with enemy Army traffic.

b. The Signal Intelligence Agency of the Navy High Command (OKM/4SKL III), which dealt with enemy naval traffic.

c. The Signal Intelligence Agency of the Air Force High Command OKL/LN Abt 350), which dealt with enemy Air Force traffic.

d. The Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi), which dealt with enemy, neutral or friendly diplomatic traffic, commercial traffic and news broadcast

The two civilian organizations were:

a. The Foreign Office Cryptanalytic Section (Pers Z S) which also dealt with diplomatic traffic, enemy, neutral, or friendly.

b. Goering's "Research" Bureau (FA), a Nazi party agency which also dealt with diplomatic traffic, news releases, broadcast monitoring, telephone monitoring, and other types of communications intelligence, enemy, neutral, or friendly.

Chart number 1-1 at the end of this volume shows how the above six agencies were related. Brief descriptions of these agencies and their work follow.

4. The Signal Intelligence Agency of the Army High Command.-- The Signal Intelligence Agency of the Army High Command (Oberkommando des Heeres, General der Nachrichten Aufklaerung, abbreviated OKH/GdNA) was located at Jueterbog, about 60 miles southwest of Berlin. Its mission included cryptanalysis and evaluation of Allied army traffic, at any level, whether strategic or operational. It also did a small amount of radio broadcast monitoring.

This Agency was the main unit of the German Army signal intelligence service in 1945. Other units were:

a. Two intercept stations operating directly under the Signal Intelligence Agency, and supplying it with intercepts of Allied high-level traffic.

b. Nine field Signal Intelligence Regiments assigned to various Army Groups for the purpose of interception, traffic analysis, cryptanalysis, and evaluation of Allied Army low-level tactical traffic in the Army Group areas. These Regiments were independent of the Central Signal Intelligence Agency, but supplied the latter with intercepts and reports.

c. A small Signal Intelligence Section, assigned to the Army Commander in Chief, West, which acted as a coordinating section for the two Signal Intelligence Regiments on the Western front.

An estimated total of 12,000 persons was employed in the Army signal intelligence effort described above.

DOCID: 3560861

The main successes of the German Army signal intelligence organization from its formation to the end of the war included the following:

a. Before 1939 it was able to establish French, Dutch, and British order of battle. This was done by cryptanalysis of French codes and Dutch Army double-transposition ciphers, and through direction-finding and traffic-analysis directed against British Army communications systems.[3]

b. During the 1940 French campaign it established French mobile order of battle. This was done by cryptanalysis of French codes (unnamed).[4]

c. It established Russian army order of battle and location of strategic reserves, from early in the war through 1943. This was accomplished through traffic analysis and cryptanalysis of Russian 2, 3, 4, and 5-figure codes (both Army and Peoples Commissariat (NKVD)).[5]

d. It gave Rommel intelligence of great operational value during the fighting around Tobruk. This was done by solving the super-encipherment of a compromised British code (unidentified).[6]

e. Information on operations undertaken by the American Army in North Africa, and thereafter through the war, was obtained through solution of Converter M-209 traffic.[7] During the fighting in Sicily the Germans captured two weeks after it went into effect, a key list valid for one month[8] and were enabled thereby to read the system completely for the remaining two weeks.[9] On other nets when sufficient depth

[3] I 78

[4] I 78

[5] I 78; I 26; I 21; I 19

[6] IF 107; I 113. Germans called this "the British War Office Code."

[7] I 154; IF 107; I 60; I 113

[8] IF 107

[9] I 60

was available, from 10%[10] to 30%[11] of M-209 traffic was readable, though most of the traffic was read too late to be of tactical value.[12]

f. Information concerning U. S. Army activities in Iceland, England, Central America, and North Africa, was obtained by reading the U. S. Army Division Field Codes (DFC 15, 16, 17, 21, 25, and 28, and possibly others).[13]

g. Tactical information concerning Allied bombing and artillery targets,[14] weather reports,[15] and reports on the size and location of Allied units passing Military Police control points in France,[16] were obtained from solutions of "Slidex," a British device for protecting operational low-level traffic. This device was used by both British and American forces and various versions of it were solved, usually in from one to three hours.[17]

h. Solution of traffic passed on Hungarian internal networks in 1941 gave evidence that transportation of German troops over Hungarian railroads could be safely undertaken.[18]

i. Successful cryptanalysis was carried out against the traffic of Yugoslav partisans, Greek partisans, Czech agents, Russian agents, and the Polish resistance movement.[19]

The Signal Intelligence Agency of the Army High Command issued three daily reports. These were sent to the Army High Command, Navy High Command, Air Force High Command, and to the Supreme Command, Armed Forces; to Himmler as chief of the Elite guard; and probably to the Reich Security Office (RSHA).

[10] I 60

[11] I 113

[12] I 142

[13] IF 120 and IF 107

[14] IF 107 p 8

[15] I 74

[16] I 80

[17] I 74, I 76, I 80, I 109, IF 107

[18] IF 126 p 10

[19] I 115, I 76, D 60, I 170, I 58, and others.

Each of the nine Signal Intelligence Regiments in the field supplied intelligence directly to commanders at Army Group, Army, and Corps levels, looking to them for primary directives on missions and priorities. They cooperated closely with the local Air Force Signals Regiments.

The Signal Security Agency of the Army High Command (Inspektion 7/IV, abbreviated In 7/IV) issued Army Codes and Ciphers until 1944, when this function was taken over by the Signal Intelligence Agency of the Supreme Command, Armed Forces (OKW/Chi).

Volume 4 is a detailed account of the German Army Signal Intelligence Agency, its field units, and their activities.

5. The Signal Intelligence Agency of the Air Force High Command-- The Signal Intelligence Agency of the Air Force High Command (Oberkommando der Luftwaffe, Luftnachrichten Abteilung 350, abbreviated OKL/LN Abt 350; previously Chi Stelle, O B d L), was the principal unit of the German Air Force Signal Intelligence Service in 1945. Field units were:

a. Three autonomous Signal Intelligence Regiments with a total of eight battalions.

b. Five autonomous Signal Intelligence Battalions. Thirteen thousand people, including overhead, were employed in all the above units.

The German Air Force Signal Intelligence Service successes against the Royal Air Force and the United States Army Air Forces were outstanding.

a. The Service furnished a comprehensive and continuous picture of the battle order and deployment of United States Army Air Force and Royal Air Force units in the United Kingdom, in the Mediterranean Theater, and, after D-day, on the continent. This information came mainly from traffic analysis, radio-telephone monitoring, and monitoring of air-borne radar devices. The solution of Royal Air Force 4-figure codes (from March 1940 until 1 November 1942) gave basic data which was enlarged upon and used until the end of the war.[20]

[20] I 70, IF 182, IF 175 p 19

b. It gave prompt and accurate warning of United States Army Air Force and Royal Air Force heavy bomber missions. This resulted from advanced methods of traffic analysis, from radio-telephone monitoring, and from radar monitoring.[21]

c. It gave immediate warning to German ground forces and fighter squadrons of tactical operations by Allied ground support aircraft.[22]

d. In connection with its western front activities, the solution of the Bomber code, Slidex, Syko, and Rekoh (used by the Royal Air Force and, for a short time, by the United States Army Air Force), both by capture and cryptanalysis, was important throughout the war.[23]

The German Air Force Signal Intelligence Service successes against the Russian Air Force were also great.

a. Its cryptanalysis of Russian Air Force ground-to-ground 2-figure, 3-figure, and 4-figure administrative and operational codes, and some 5-figure codes, provided a complete order of battle for the Russian Air Forces from 1937 until the end of the war. A large amount of intelligence on Russian Army battle order was also obtained from a study of air networks.[24]

b. From partial decipherment of air-ground traffic, from plane-to-ground radio-telephone monitoring, and from radio-direction finding of bombers when airborne, it was able to give accurate warnings of all Russian long-range strategic bombing raids.[25]

c. From cryptanalysis of each Russian Air Army's 2-figure, 3-figure, and 4-figure traffic, from traffic analysis, from plane-to-plane radio-telephone monitoring, and from radio direction-finding of planes in flight, it was able to warn German ground forces and fighter squadrons of impending operations by Russian fighters and fighter bombers.[26]

[21] I 70

[22] IF 182

[23] IF 175

[24] I 120

[25] IF 187

[26] IF 187

Intelligence from both Western and Russian fronts, in the form of daily, weekly, or monthly reports, was furnished by the Signal Intelligence Agency (OKL/LN Abt 350) to the Air Force High Command and to the local Air Forces (Luftflotten). Daily and monthly reports were also sent to the local Army Signal Intelligence Regiments. Monthly reports were sent to the Army Commander in Chief West, to the Signal Intelligence Agency of the Army High Command (OKH/GdNA), to the Signal Intelligence Agency of the Navy High Command (OKM/4 SKL/III), to the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi), and also to the Air Force Signal Intelligence units in the field.[27]

Field units, charged with the responsibility for warnings on allied air raids, telephoned their warnings and reports directly to fighter squadrons, anti-aircraft batteries, and the local Gauleiters in charge of civilian air raid warnings.[28]

Group IV of Division II in the Office of the Chief Air Force Signal Officer (Oberkommando der Luftwaffe/Generalnachrichtenfuehrer II, Gruppe IV, abbreviated OKL/Gen Nafue II/IV) issued codes and ciphers for the Air Force. Group IV of Division III (OKL/Gen Nafue III/IV) checked them for cryptographic security.

A detailed description of the Signal Intelligence Service of the Air Force is given in Volume 5 of this report.

6. The Signal Intelligence Agency of the Navy High Command--The Signal Intelligence Agency of the Navy High Command (Oberkommando der Kriegsmarine, 4 Seekriegsleitung III, abbreviated OKM/4 SKL/III) was responsible for traffic analysis, cryptanalysis, and evaluation of British, American, Russian, French, and Swedish naval traffic. It had a strength of approximately 1,000 persons. It also had operational control over a field organization of approximately 2,500 persons. The field units were as follows:

a. Four detachments in Flanders, Brittany, Wilhemshaven and Pomerania engaged in cryptanalysis on low-level systems, interception and direction-finding. Each detachment had a total complement of 200 men, including 100 intercept operators and 10 cryptanalysts.

27 IF 180 p 31 a

28 IF 181

DOCID: 3560861

b. Eighteen "primary direction-finding stations", whose main duties were interception rather than direction finding. Each station had a strength of 100, including 60 intercept operators, and 5 cryptanalysts.

c. Twenty five "secondary direction-finding stations", whose duties were direction finding and traffic analysis. Each station had a strength of 26 persons.

d. Small detachments were occasionally set up for special missions.

The main successes of the Signal Intelligence Agency of the Navy High Command (OKM/4 SKL/III) included the following:

a. In 1939 it was able to establish the war-time organization and disposition of the British Fleet, through solution of British Naval Code No. 2.

b. In the spring of 1940 it obtained complete information concerning the proposed British and French Norway expedition ("Operation Stratford"). This was done by solution of British Naval Cypher No. 4.[29] The German invasion of Norway followed immediately. During the subsequent Norwegian campaign, solution of traffic sent in British Naval Cypher No. 4. gave detailed information on Allied counter-measures, such as proposed British landing fields, transport arrival schedules, and the disposition of British and French surface forces.[30]

c. Throughout 1942 and part of 1943 it provided important intelligence on Atlantic convoys by a current (and nearly 100%) solution of Combined Cypher No. 3 used by British and U. S. North Atlantic Convoys.[31] The average monthly allied shipping losses in the Atlantic during this period were approximately six times the average monthly losses in later periods.

Minor successes of the Signal Intelligence Agency of the Navy High Command (OKM/4 SKL/III) included the solution of the British Interdepartmental Cypher;[32] solution in 1943 of a Royal Air Force torpedo-bomber transposition cipher used for practice exercises in the English Channel;[33] and solution of various minor Navy and Merchant Navy codes and ciphers.

[29] T-517

[30] T-517

[31] I 12

[32] Performed jointly with Goering's "Research" Bureau (FA), the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi), and with the Signal Intelligence Agency of the Commander in Chief German Air Force (Chi Stelle, OBdL) I 147.

[33] D 6 D 15 D 41

The Naval Signal Intelligence field units described above carried out direction-finding activities against Allied naval and merchant ships, plotted their positions and movements, and passed the information to local commanders. Detachment Flanders, at Bruges, assisted in the 1942 "escape" of the pocket battleships Schernhorst and Gneisenau when they made their dash from Brest through the English Channel to Kiel. This same detachment read British naval traffic to advantage during the Dieppe raid.

The Signal Security Agency of the Navy High Command (OKM/4 SKL/II), as opposed to the Signal Intelligence Agency(OKM/4 SKL/III), issued German naval codes and ciphers, and made cryptographic security studies of these systems. Its exact strength is unknown.

The detailed organization and history of the two signal agencies of the Naval High Command (OKM/4 SKL/III and OKM/4 SKL/II) are not discussed further in this report. Their use of punch-card book-keeping machinery ("I. B. M."), their security studies, and their chief cryptanalytic methods, however, are discussed in Volume 2.

7. The Signal Intelligence Agency of the Supreme Command Armed Forces.- The Signal Intelligence Agency of the Supreme Command Armed Forces (Oberkommando der Wehrmacht, Chiffrierabteilung, abbreviated OKW/Chi) had three main functions:

a. It intercepted, studied, and evaluated diplomatic, military attache, and "agent" traffic.

b. It monitored, and evaluated commercial radio traffic and news broadcasts.

c. It made security studies of the codes and ciphers used by the Supreme Command, Armed Forces, the Army, the Air Force and the Navy, and many government departments, vetoing (after 1944) the use of those it deemed insecure.

The Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) operated at least thirteen radio intercept stations of its own, and received radio traffic from other agencies as well (notably Goering's "Research" Bureau (FA)). It also received land-line traffic from sources not stated.[34]

[34] DF 9, p 3

With the exception of military attache systems, it did not work on enemy Army, Navy or Air Force traffic. Documentary evidence as to its cryptanalytic successes is limited. The following summary covers its most important known cryptanalytic achievements:

a. The most extensive 1939-1944 successes seem to have been achieved with French systems. The electrical Hagelin Cipher Machine B-211 (adopted by the French - now obsolete) was solved, and limited success was also achieved in the solution of the French Hagelin Machine BC-38.[35] An important military attache code (ASA trigraph FVD) was solved at the beginning of the war.[36] After 1940 all Vichy-French systems were automatically compromised when filed with the German Armistice Commission in Wiesbaden.

b. At least four Japanese diplomatic codes (including those designated by ASA trigraphs JAE, JAH and JBA) were solved. In 1938 and 1939 the Agency collaborated with the Cryptanalytic Section of the Foreign Office (Pers Z S) in a current solution of daily keys for the Japanese "Red" Machine.[37]

c. Precise details on solution of U.S. systems are not available. The agency had compromised copies of at least two U.S. State Department codes, namely "Brown" and "Al". Work was also done on the U.S. State Department Strip Ciphers O-1 and O-2, the lead in O-2 solution being taken by the Foreign Office Cryptanalytic Section.[38]

d. Croatian Enigma traffic was solved through compromised machine wirings.[39]

[35] I 45 p 7; I 160 p 6

[36] I 31 p 8

[37] I 31 p 11

[38] I 89

[39] I 58 p 3; I 92 p 2

DOCID: 3560861

e. Little information is available on successes in solution of English systems. Polish, Turkish, Greek and Latin American systems were solved extensively. Prior to 1943, appreciable success was achieved in the solution of Italian diplomatic codes.

During the first half of the year 1944 important decodes designated as "VN's" (Verlaessliche Nachrichten) totaled 3,000 per month.[40] Selected decodes were sent to Field Marshal Keitel, Chief of Armed Forces; to Hitler; and by Keitel to General Jodl, Chief of the Armed Forces Operations Staff. They were also sent to the Army, Navy and Air Force High Commands,[41] and probably to the Signal Intelligence Agencies of these commands.[42] In addition, approximately 45 special reports were sent each day to special recipients, such as the Field Economic Office, the Department of Armed Forces Propaganda, the Western Armies Branch and Joint Intelligence.[43]

After 1944 the Signal Intelligence Agency of the Supreme Command Armed Forces issued cryptographic systems for the Army and interservice communications. One of its most important responsibilities by the end of the war was the evaluating of the cryptographic systems of other services. A file belonging to Dr. Erich Huettenhain, its chief cryptanalyst, indicated that cryptographic studies were made on cipher teleprinters, Enigma machines, specially designed Hagelin machines, small cipher devices and hand systems.[44]

[40] DF 9

[41] I 143, p 9

[42] I 13, p 3

[43] DF 9 p 2

[44] D 59

In connection with its security commitments, the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) was responsible for the two most serious German cryptographic mistakes of the war: the continued use in high level German military communications of the plugboard Enigma machine and the teleprinter cipher attachment SZ 42 in their insecure forms. OKW/Chi rejected the 1943 proposals of the Army Signal Security Agency (IN 7/IV) that the (insecure) SZ 42 be replaced by the cipher teleprinter T52d, a secure device.[45] It also frowned on suggestions that the insecure plugboard Enigma be used with pluggable reflector wheels, a change which would have made it secure.[46]

Approximately 800 persons were employed in all duties except intercept.

Volume 3 of this Report gives a more detailed account of this agency.

8. The German Foreign Office Cryptanalytic Section.-- The German Foreign Office had two cryptologic sections, the Cryptanalytic Section (Personal Z Sonderdienst des Auswaertigen Amtes, abbreviated Pers Z S) and the Cryptographic Section (Personal Z Chiffrierdienst des Auswaertigen Amtes, abbreviated Pers Z Chi).

The Cryptanalytic Section of the Foreign Office (Pers Z S) was the senior German cryptanalytic agency. It was organized in 1919 or before. At its greatest strength it employed approximately 200 persons. Its mission was the solution of foreign diplomatic codes and ciphers. The Section had one small intercept station at Dahlem.[47] For the rest of its intercept it was dependent upon the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi), Goering's "Research" Bureau (FA) and the German Postoffice.

[45] D59, p 17

[46] D 59, p 10; see also I 31

[47] I 22, para 103

[48] I 22, para 103

The Cryptanalytic Section achieved its greatest successes with diplomatic codes, both one-part and two-part, enciphered and unenciphered.

a. From 1935 until 1942 it achieved practically 100 per cent success in the solution of Italian diplomatic codes.[49]

b. It read the United States State Department Grey, Brown and A-1 Codes.[50] It also succeeded in solving the American Diplomatic Strip Ciphers O-1 and O-2, the former in partial fashion based upon a compromise.[51]

c. The Section solved two British Foreign Office "R" Codes and the British Government Telegraph Codes.[52]

d. In 1940 success in solution of French diplomatic codes was estimated at seventy five per cent.[53]

e. A number of major Japanese diplomatic codes were read, and there is some evidence that at least one major Chinese system was solved.[54]

f. The Section also solved two machine ciphers. The Japanese Red Machine was solved in 1938 and read currently until February, 1939.[55] The Section collaborated with the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) in this solution, and it is not known which agency deserves credit for the original solution.[56] In 1941, after a partial solution by Goering's "Research" Bureau (FA), the Swiss diplomatic Enigma traffic was solved.[57]

Little information is available on the Section's achievements in terms of intelligence. The distribution it gave its decodes is unknown. The Section's personnel seem to have thought primarily in terms of cryptanalysis as a science, rather than in terms of what their intelligence contribution meant to a successful German diplomacy.[58] The Section seems to have been badly neglected by higher Foreign Office authorities, both with respect to needed personnel, and with regard to interest in its work.

[49] I 22, para 25

[50] I 22

[51] I 22, para 54; DF 15, p 4, 5; I 89

[52] D 16, Reports 2, 3, 4

[53] D 54, p 13

[54] I 22, para. 176

[55] I 22, para 19

[56] I 22, para. 19

[57] D 54, p 18

[58] See Vol. VI. Ch. 5

Some of the Section's senior personnel acted in an advisory capacity to the Foreign Office Cryptographic Section (Pers Z Chi).59 The latter section was responsible for the preparation, compilation,distribution and security of Foreign Office codes and ciphers. Few details are available concerning its security studies or its personnel. It was presumably responsible for the use in German diplomatic correspondence of the code systems known as the "Deutsches Satzbuch", the Deutsches Satzbuch enciphered by"Floradora" (Army Security Agency trigraph GEC), and the "one-time pad"(Army Security Agency trigraph GEE),all of which were read by Anglo-American cryptanalysts.Volume 6 of this paper gives an account of the cryptologic Sections of the German Foreign Office.

9. Goering's "Research" Bureau. -- Goering's "Research" Bureau (Reichsluftfahrtministerium Forschungsamt,abbreviated as FA) was formed in 1933. According to Goering,it supplied the new Nazi government with a signal intelligence organization of its own which had "no political axe to grind nor ideology to follow." 60

In addition to non-military cryptanalysis,the "Research" Bureau had the following functions:

a. As a Nazi censorship organization in peace-time it monitored telephone conversations in all large German cities at first only in the Reich but later extending into Austria, Denmark,and"German" Poland.61. It had access to messages sent over all German commercial teletype and telegraph facilities,62 and maintained investigators in all main postal censorship offices.63

b. In war-time it liaised closely in the censorship of all communications as directed first by the Abwehr and later by Himmler's Reich Main Security Office. It is known to have served the latter agency as a cryptanalytic agency for Russian Agent messages.(As no cryptanalytic organization within the Reich Main Security Office is known to TICOM it is probable that the"Research" Bureau filled this function). 64

59
I 172; I 22
60
I 143
61
TF 29; T 240
62
I 143; IF 15
63
IF 132
64
TF 29; T 240

c. It monitored world-wide radio news broadcasts, in particular the British Broadcasting Company (London) broadcasts.[65]

d. It operated six wireless intercept stations of its own, for intercepting foreign diplomatic and commercial traffic. In addition, it exchanged copies of wireless intercepts with the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi), the Signal Intelligence Agency of the Navy High Command (OKM/4 SKL/III), and probably with the Signal Intelligence Agency of the Commander in Chief German Air Force (Chi Stelle OBdL).

As can be seen from the functions outlined above, the "Research" Bureau was not primarily concerned with cryptanalysis. No documentary evidence bearing on its cryptanalytic successes was found by TICOM. Based upon secondary evidence and scattered TICOM interrogations, the bureau's chief cryptanalytic achievements seem to have been as follows:

a. In 1941 the agency collaborated with the Cryptanalytic Section of the German Foreign Office (Pers Z S) in solving the Swiss Enigma.[66] Personnel from the Bureau claimed to have broken Finnish (or Swedish) Hagelin traffic.[67]

b. According to newspaper reports, 1938 decodes of French traffic revealed that, lacking English support, the French Government did not intend to oppose the Austrian Anschluss with force.[68]

c. In 1938, during the Munich Conference, the "Research" Bureau is said to have solved the British system which carried Chamberlain's messages to London. Hitler once delayed a conference with Chamberlain for several hours in order to get such decodes.[69]

d. Solution of Russian internal wireless messages revealed bottlenecks in the Russian military supply system. The dates of this solution are unknown.[70]

[65] IF 132

[66] I 25; I 54; D 54 Report 8

[67] I 25 p 6

[68] IF 188

[69] IF 132

[70] I 25

The "Research" Bureau circulated its intelligence in the following forms:

a. Decode bulletins were sent regularly to Hitler, Goering, Field Marshal Keitel and General Jodl of the Supreme Command Armed Forces (OKW), Foreign Minister Ribbentrop, and Admiral Doenitz of the Navy High Command.

b. Individual items of current interest, collected items on single subjects, and consolidated special reports were sent to interested ministries.

c. Special liaison officers were assigned to the Foreign Office, the Supreme Command of the Armed Forces, the Reich Security Office, the Economic Ministry and Ministry for War Production, and the Propaganda Ministry.[71]

Goering's "Research" Bureau had over 2,000 personnel. Less than one per cent of these were apprehended by TICOM for interrogation.

Volume 7 of this report is a detailed account of this agency.

10. Collaboration between German Signal Intelligence Agencies in Cryptographic Matters-- It seems probable that, prior to 1943, there was some sort of collaboration between the various branches of the German Armed Forces in cryptographic matters. The widespread usage of the Enigma machine, the universality of the teleprinter systems used, the allocation of similiar hand cipher systems to army, air force and police units, all point either to an excellent cooperation in the cryptographic field, or to the existence of some shadowy interservice agency or higher authority whose responsibility it was to study, test and recommend the introduction of such devices and systems. There is no reference in the TICOM material to such an agency, other than a passing 1942 reference to "the big executive committee," a group which apparently had some responsibility for cryptographic changes and improvements in a cipher type teleprinter.[72] From the headings

[71] IF 135

[72] D 59, p 6

on various memos belonging to Dr. Huettenhain (chief cryptanalyst for the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi)), it could be assumed that the Chief Armed Forces Signal Communications Group (OKW/Chef Ag WNV) acted as a senior military cryptographic authority, approving or disapproving the introduction of various systems, and using the facilities of the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) and the army agencies (Inspectorate 7/VI (In 7/VI) and the Army Ordnance Development and Testing Group Signal Branch (Wa Pruef 7)) as its staff or advisory agencies.[73]

An order from Field Marshal Keitel, Chief of Staff of the Supreme Command Armed Forces (OKW), dated October 1943, made the introduction of new ciphers for branches of the Armed Forces contingent upon the agreement of the Supreme Command Armed Forces (OKW), and probably upon the agreement of the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi).[74]

In 1944 General Praun, who was both Chief Signal Officer of the Supreme Command Armed Forces (OKW/WFSt/Chef WNV) and the Chief Signal Officer of the Army (OKH/Chef HNW), made the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) a central clearing house for all German cipher development and security scrutiny work. This was easily done with reference to the Army. On September 5, 1944, General Praun signed an order directing that the cryptographic development and testing functions of the Army be turned over to the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi). Personnel from the Army Security Agency (In 7/IV),

[73] D 59, various letters and memos. From the headings of cryptographic manuals, it could be assumed that Ag WNV/Fu I, as issuing authority, was responsible until 1944, when OKW/Chi apparently replaced it. See OKW/Ag WNV/Fu I "Schluesselanleitung zum RS 44" dated March 27, 1944 and OKW/Chef WFSt/Ag WNV/Chi "Rasterersatzverfahren" of Dec. 7, 1944, TF 31 and TF 32 respectively.

[74] D 68, p 11; D 57 p 14

including Technician Dr. Fricke, and the personnel of Inspectorate 7/VI (In 7/VI) who were engaged in cryptographic work, were transferred into the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi).[75] Thereafter, while the actual production of keys was left as an Army responsibility, the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) devised the cipher systems and provided the material for Army key production.[76]

With the Navy and the Air Force the picture was somewhat different. They were permitted to continue their cryptographic development work, and retained the right to say which of their systems was to be used in what place--so long as the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) concurred from a security standpoint in the original introduction of the systems. As Admiral Krause of the Signal Intelligence Agency of the Naval High Command (OKM/4 SKL/III) pointed out, "OKW/Chi recommendations could only lay down the (security) limits within which it was possible to use a system." The responsibility for whether and where a Navy system was to be used lay with the Navy.[77]

With regard to ciphers used by the Waffen SS, the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) had consultative powers only. While General Gimmler, successor to General Praun as Chief Signal Officer, publicly characterized the cooperation between the two services as "perfect",[78] Col Mettig, chief of the cryptographic division in OKW/Chi, indicated that an effective supervision was never introduced.[79]

[75] D 68 p 3
[76] D 55, p (43)?
[77] D 68, p 14
[78] D 68, p 13
[79] I 96, p 19

The preeminence of the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) in cryptographic matters and security was apparently official only with the military services. In his speech of ~~December 20~~ 14 November, 1944, General Gimmler pointed out that primacy in the civilian field was dependent upon voluntary concurrence from the agencies affected. He could only plead that "OKW was prepared to take the lead in this matter, providing that the Party and State concurred" and requested that "the Party and Reichs authorities" cooperate.[80] Goering's "Research" Bureau (FA) developed its own codes and ciphers,[81] although the Bureau did use cipher teleprinters adopted by the military services.[82] Evidence is available that in 1945 administrative hand ciphers (Behoerdenhandschluessel) were issued to Senior Specialist Wenzel of the "Research" Bureau (FA).[83] A similiar situation prevailed with the German Foreign Office. The Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) was never allowed to know the details of the ciphers used by the Foreign Office.[84] The Foreign Office, however, did use cipher teleprinters and Enigma machines.[85]

11. Collaboration between German Signal Intelligence Agencies in Cryptanalytic Matters.-- The collaboration between Agencies in cryptanalytic matters varied. In general relationship between Goering's "Research" Bureau (FA) and the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) were not overly cordial. The Signal Intelligence Agency of the Naval High Command (OKM/4 SKL/III) maintained a traditional

[80] D 68 p 14
[81] IF 132
[82] I 25, page 9
[83] T 240
[84] I 31, page 15
[85] I 22, para 115

navy reserve in dealing with other agencies. There was no high-level signal intelligence coordination, and there was frequent overlapping and duplication of effort between the agencies dealing with diplomatic cryptanalysis. But, with the exceptions noted above, there seems to have been as much liaison and as much cooperation as were necessary. This was especially true in the case of the military field organizations, the Army Signal Intelligence Regiments ("KONAs") and their Air Force equivalents, the Air Signal Regiments (LN Rgts).

a. Relationships between Foreign Office Cryptanalytic Section, Goering's "Research" Bureau, and the Signal Intelligence Agency of the Supreme Command Armed Forces.-- The Cryptanalytic Section of the Foreign Office (Pers Z S) enjoyed reasonably good working relationships with both Goering's "Research" Bureau (FA) and the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi). As stated, however, the relationships between the latter two agencies do not appear to have been cordial.

The Foreign Office (Pers Z S) received the bulk of its intercept from Goering's "Research" Bureau (FA) and the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi).[86] It received numerous compromised codebooks and keys from both agencies.[87] Cooperative attacks on difficult problems were not uncommon. In the case of an unspecified U. S. Strip System, the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) worked on the point-to-point traffic, while the Foreign Office (Pers Z S) worked on the circular traffic,[88] with a complete exchange of results. In the case of the Japanese Red machine, the Foreign Office (Pers Z S) attempted to solve messages sent on even days, while the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) attempted to solve messages sent on odd days, a "practical arrangement" reached also between the U. S. Army and the U. S. Navy prior to the Pearl Harbor disaster. Results

[86] I 22, para 103

[87] T2038; D16, pages 3, 5; DF 15, pages 4, 5

[88] I 31, page 10

were exchanged.[89] Goering's "Research" Bureau (FA) and the Foreign Office Cryptanalytic Section (Pers Z S) cooperated on the solution of the Swiss Enigma.[90] Exchange of code group identifications, additives and enciphering keys between these two agencies were frequent, especially on English, Italian and Vatican systems.[91] Personnel were exchanged between the Foreign Office Cryptanalytic Section (Pers Z S) and the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi).[92]

Goering's "Research" Bureau (FA) was formed by a small group of cryptanalysts who left the Cipher Department of the Reich Defense Ministry (Reichswehrministerium), the predecessor agency of the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi). This defection may account for the bad feeling between the two agencies.[93] There are no known examples of direct cryptanalytic exchanges between the two agencies, nor were there subsequent exchanges of personnel. Goering's "Research" Bureau (FA) was not given access to the special cryptanalytic machinery developed by the Signal Intelligence Agency of the Supreme Armed Forces (OKW/Chi),[94] although this machinery was made available to other agencies. Relationships could probably have been improved had not Goering's "Research" Bureau (FA) sought to take over the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi).[95]

[89] I 31, para 53

[90] D 54, page 18

[91] D16, pages 1, 2; I 172, paras. 11, 13, 14; T2252, various report

[92] I 22, paras. 20, 84

[93] I 21, p 1; I 131, p 3

[94] DF 9 p 3

[95] I 131, p 3; I 78 p 4

With reference to the exchange of traffic, however, collaboration was apparently complete. It is known that in early 1944 approximately one third of the intercept received by the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) came from Goering's "Research" Bureau (FA).[96] The latter always received copies of all the traffic intercepted by Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) stations.[97]

b. Military Agency Relationships-- exchanges of cryptanalytic information.-- Collaboration between the Army Signal Intelligence agencies (OKH/GdNA and its predecessors, In 7/VI and HLS Osk) and the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) was excellent. The Chief Signal Officer of the Supreme Command Armed Forces (OKW/Chef WNV) was also the Chief Signal Officer of the Army (OKH/Chef HNW).[98] However, since the Supreme Command agency's commitment was diplomatic and military attache traffic, no broad basis for cryptanalytic liaison existed.

The Army and Air Force Signal Intelligence Agencies maintained permanent liaison on English Naval and Air systems (SYKO, M209).[99] In 1943 the Army Agency (OKH/In 7/VI) had discovered how to recover true M-209 settings from relative settings, and they had passed the technique on to the Navy and Air Force agencies.[100] According to Senior Specialist Tranow of the Naval Agency, however, the Army-Navy cooperation was given up in early 1944 since "no results of value were obtained."[101] In 1943 the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi), the Cryptanalytic Section of the German Foreign Office (Pers Z S), and the Signal Intelligence Agency of the Commander in Chief German Air Forces (Chi-Stelle OBdL) collaborated on solution of an unidentified US strip system.[102]

[96] DF 9, p 3
[97] I 85 , p 3
[98] IF 108
[99] I 93, p 3, 4
[100] I 144, p 2
[101] I 93, p 3
[102] D60, p 5

The Army-Navy- Air Force field collaboration was usually excellent.[103] It embraced on occasion exchange of personnel and equipment, a complete exchange of reports, and a close cryptanalytic liaison on operative systems.[104] Eastern front reports show a detailed operational collaboration between Air Force Signal Regiment 353 (LN Regt 353), the Army Signal Intelligence Regiment 1, (KONA 1), and the Naval units dealing with Russian Black Sea Fleet traffic.[105] Army Signal Intelligence Regiment 5 (KONA 5) worked closely with the Air Force Signal Intelligence organizations in the West (at Paris and Noisy).[106]

During the period 1940-1942 the Signal Intelligence Agencies of the Navy (OKM/4 SKL III) and the Air Forces (Chi-Stelle OBdL), and the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi), and also Goering's "Research" Bureau (FA), all collaborated on solution of the English Interdepartmental Cipher.[107] There was "Research" Bureau (FA)-Naval (OKM/4 SKL/III) cooperation on the solution of the British Government Telegraph Code (South Africa) and Bentley's Code.[108] The Army Agency, Inspectorate 7/VI (In 7/VI) actually worked on Turkish diplomatic traffic, by agreement with Goering's "Research" Bureau[109] and had Army Signal Intelligence Regiment 4 (KONA 4) intercept this traffic for them. This work probably duplicated efforts of the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) however.

[103] I 26, p 2

[104] US M-94, M-209, Slidex, Russian codes, etc.

[105] I 130, p 15

[106] I 113, p 8

[107] I 93, p 4; I 147, p 11, 12

[108] I 93, p 3

[109] IF 126, p 8

DOCID: 3560861

c. Military Agency Relationships--exchange of personnel.-- In 1942 Prof. Nowopaschenny of the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) and a group of his cryptanalysts were transferred to Intercept Control Station East (HLS), one of the predecessors of the Signal Intelligence Agency of the Army High Command (OKH/GdNA) for work on the main Russian army five-figure code.[110] At one time the Naval commander in the Aegean area placed his radar intercept personnel and equipment under the command of Air Signal Regiment (LN Rgt) 352.[111] On one occasion personnel from Air Signal Regiment (LN Rgt) 353 went aboard the cruiser "Prinz Eugen" to monitor traffic from the Air Arm of the Russian Baltic Fleet.[112] In the spring of 1942 the Signal Intelligence Agency of the Naval High Command (OKM/4 SKL III) exchanged personnel with the Army and Air Force in order to get trained Hollerith operators.[113] In 1939 Dr. Huettenhain of the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) was detailed to the Army agency to work on solution of French military systems.[114]

d. Military Agency Relationships--Cooperation with regard to IBM and Rapid Analytic Machinery.-- The Army Signal Security Agency (Inspektion 7/IV abbreviated In 7/IV) pioneered in the use of IBM (Hollerith) equipment. Its installations were set up in the winter of 1939 and 1940, and later transferred to Army Inspectorate 7/VI (In 7/VI), one of the predecessors of the Signal Intelligence Agency of the Army High Command (OKH/GdNA).[115]

[110] IF 123 p 3
[111] I 126 p 14
[112] I 163 p 3
[113] I 146 p 17
[114] D 60 p 4, 5
[115] I 67 p 2

In March, 1942, representatives of Goering's "Research" Bureau (FA), and of the Signal Intelligence Agencies of the Commander in Chief Air Forces (Chi Stelle OBdL) and the Navy High Command (OKM/4 SKL/III) visited the Army installations and obtained valuable information as to the possibilities of IBM in cryptanalysis.[116] The Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) never owned its own Hollerith machinery and used the Army installations.[117]

In 1944 the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) developed a number of "decoding devices," some of which were handed over to the Army, Navy and Foreign Office agencies.[118] The Digraph Weight Recorder (Bigrammsuchgeraet) was made available to the German Weather Service (WENUEB).[119]

e. Military Agency Relationships--cooperation with regard to interception.-- Goering's "Research" Bureau (FA) occasionally furnished the Signal Intelligence Agency of the Commander in Chief of the Air Force (Chi Stelle, OBdL) with traffic.[120] The amount of this traffic is not known. Goering's "Research" Bureau (FA) also passed some intercepted commercial traffic of naval interest to the Signal Intelligence Agency of the Naval High Command (OKM/4 SKL/III).[121] The German Navy passed its weather intercept to the Air Force, who had some interservice responsibility for the solution of weather traffic.[122] On operational fronts, when army search receivers found air force frequencies, information concerning these frequencies was supplied to the appropriate air force field intercept units.[123] The Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) controlled a naval direction finding station in Spain.[124]

[116] I 146, p 17
[117] I 67, p 2, 3
[118] DF 9, p 3
[119] I 31, p 4
[120] I 29, p 3
[121] I 93, p 12, 18
[122] I 93, p 4
[123] I 130, p 15
[124] I 96, p 7

f. Cooperation between Military and Civilian Agencies on solution of Agents' systems.-- The extensive German effort against agent-partisan systems warrants separate discussion. This effort was shared by at least three organizations, and perhaps a fourth. The organizations were: the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi), Army Inspectorate 7/VI (OKH/In 7/VI), perhaps Goering's "Research" Bureau (FA), and a small organization which did little or no cryptanalysis, the Radio Defense Corps of the Supreme Command Armed Forces (OKW/WNV/FU III). The relationship between these agencies illustrates collaboration in both intercept and cryptanalysis, and an allocation of primary responsibility which varied from problem to problem.

At the beginning of the war, responsibility for monitoring clandestine transmissions in Germany and the occupied territories was borne by the Radio Defense Corps (OKW/WNV/FU III).[125] In the spring of 1942 the Radio Defense Corps pressed for the establishment of its own cryptanalytic section. Neither the Army nor the Supreme Command signal intelligence agencies were anxious to see the establishment of a new cryptanalytic agency for agent traffic. Accordingly, a section for cryptanalysis on agent transmissions was established in the Army Inspectorate 7/VI (In 7/VI).[126] This section was known (from its chief) as "Referat Vauck".

Originally located in Berlin, Referat Vauck moved in the fall of 1943 with the Radio Defense Corps (FU III) to Dorf Zinna, near Jueterbog. It was transferred in the fall of 1944 from Inspectorate 7/VI (In 7/VI) to the newly formed Signal Intelligence Agency of the Army High Command (OKH/GdNA) and was transferred again in early 1945 to the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi/Gr. IV). Both these latter changes were administrative only, since the section remained with the Radio Defense Corps at Jueterbog.[127]

[125] I 115, p 2

[126] I 115, para 15

[127] I 115, paras 12, 31

DOCID: 3560861

Referat Vauck did not enjoy a monopoly on agent cryptanalysis. Most of its and the Radio Defense Corps' (FU III) effort was concentrated on western agent networks (France, Belgium). In the eastern and Balkan theaters, other agencies handled the bulk of agent intercept and cryptanalysis, as follows:

(1) Russian Partisan Traffic-- The work done by Referat Vauck on this problem covered only the period mid-1942 to mid-1943. Its work was then taken over by a section under Lt. Schubert of Army Signal Intelligence Regiment (KONA) 6.[128] Schubert was ultimately transferred to the Signal Intelligence Agency of the Army High Command (OKH/GdNA), where he took over "eastern" cryptanalysis on the NKVD-partisan networks.[129]

(2) Yugoslav systems-- Most of the interception and cryptanalysis on Yugoslav systems was done, not by the Radio Defense Corps (FU III), but by a special detachment of Army Signal Intelligence Regiment (KONA) 4, stationed in Belgrade.[130] Cryptanalytic work on the more difficult Balkan systems was done in Berlin by Balkan Section (Referat Bailovic) of Army Inspectorate 7/VI (In 7/VI), who thus complemented the activities of Referat Vauck.[131]

(3) Polish Resistance Movement Systems-- In 1943 Referat Vauck solved the principal system used by the Polish Government in Exile (London) for communication with the Polish Resistance Movement (Warsaw). So important was this traffic that, in the fall of 1943, eight members of Vauck's Section were transferred to the Polish Section in the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi, Gr. V). The intercept work done by the Radio Defense Corps (FU III) was augmented by the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) intercept station at Lauf,[132] and I.B.M. assistance was given by Army Inspectorate 7/VI (In 7/VI).

[128] I 115, p 7
[129] I 26, p 1
[130] I 115, p 8
[131] I 115, p 8
[132] I 115, p 9