German exploitation of Russian communications through Traffic Analysis during World War II

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

INTRODUCTION

The contents of this volume deal with German exploitation of Russian communications through Traffic Analysis. There is not as much source material available on Russia as there is on United States and England. The main interest of the interrogation officers normally was centered on gaining intelligence concerning American and British communications, and consequently, interest concerning German activity on the communications of other countries had to be of secondary importance. In addition, because of the conditions under which many of the interrogations were conducted—a number of them being made in active combat zones—there were often times great difficulties encountered in carrying out even the necessary routine line of questioning. Even had there been ideal conditions under which to work it is probable that not much more intelligence could have been obtained on Russian communications because the German personnel who were engaged in that work were in the Russian zone of operations. Only a few of these fell into English or American hands—the Russians capturing the others. However, the material which is, available does give a fairly adequate, though not complete, picture of Russian communications as seen by the German Traffic Analyst.

Chapter 1. SECURITY OF RUSSIAN COMMUNICATIONS

1. General Security

Although the Russians monitored their own military communications for the more outstanding breaches of cryptographic and transmission security, company and secondary commands were very careless with their radiotelephone transmissions. Code cover names were rarely heard by German listening operators. However, many private conversations were intercepted as the Russians had a tendency to use radio-telephone facilities as an ordinary telephone. Also the Russian radio operators committed violations in security which greatly facilitated the work of the German Signal Intelligence.[I-75, p.4]

The Russian radio and radio-telephone operators habitually engaged in “operator chat". One instance of such conversations, and the subsequent value to German Signal Intelligence, occurred in January 1943 when the Germans learned that a British-American delegation was visiting the Russian Central front. In other instances the arrival of high-ranking officers was disclosed in private radio-telephone conversations as well as dates for planned offensives.[I-75, p.4]

Although their radio-telephone traffic was on a very low level of security, the Morse and non-Morse radio traffic of the Russian military forces reached a high degree of security during the later periods of the war. This appears to have been due to the increased amount of radio training given the operators; the increased amount of traffic which they had to send; and the subsequent efficiency which came from practice.[I-75, p.4]

2. Security on Partisan Nets

On the Russian Partisan radio nets good operators were employed and the Germans were unable to learn much about the operation and activity of these nets. In the winter of 1943 the Germans formed a detachment to trace the activity of the Partisan nets. These attempts however were unsuccessful owing to the fact that messages transmitted were very brief and there was only a short duration of radio activity when the nets were in operation.[I-75, p.4]

3. Army and Air Forces Nets

The set-up of the Russian radio nets was a reflection of the organization of the Soviet Armed Forces. As radio facilities were used without restrictions, on account of inadequate line communications, traffic intercept and analysis, as a primary source of intelligence to the Germans, reached a high degree of efficiency. Ah insight into the makeup of the radio nets was facilitated by imperfect changes in the radio discipline.[I-70, p.4]

The air units of the Russian armies were forced, due to inadequate line communications, to exercise command from Air Army downwards by radio.[I-70, p.3]

In nets from division downwards in the Army composition radio-telephone channels were used for the passing in of communications in addition to the use of Morse radio traffic. During the latter days of the war this use of radio-telephone increased. At the beginning of the war radio-telephone transmission in regard to opening of nets, message warning signals, and the use of the alphabet in spelling out names and code groups was carried out strictly in accordance with existing regulations. Such was not the case later: the traffic then sometimes assuming a very free form. Radio-telephony was used for passing messages, fire orders for artillery, reports for the Air Warning Service, and also for general conversation between officers and commanders. The traffic consisted mostly of two-and-three-figure message-text, plain-text, and mixed figure-plain-text. Radio stations used cover names which were easily analyzed by the Germans. Call signs of these stations were mostly formed from the cover names of the stations. (Thus the call sign "HAP" was formed from the cover name of "MAPKA").[I-173, p.10]

In analyzing Russian traffic the Germans used all the data available: pad numbers, originators' serial numbers, call sign system composition, coordination and knowledge of map coordinates, any results obtained from decrypted materials, and any direction-finding information.[I-19b]

Chapter 2. GERMAN EXPLOITATION OP RUSSIAN COMMUNICATIONS

4. Russian Radio Procedure

During the first days of the Russian-German war the speed of the transmitting operators was very low, but as time went on they developed their speed until at the end of the war the average speed attained was 16 to 18 words per minute. On some of the more important point-to-point radio nets the average speed was 25 words per minute.[IF-187, p.48]

a. Procedure Signals. —The International "Q" and "Z" signal groups were used as procedure signals by the Russians. The Germans assumed that some of the Russian operators had been trained by the British because some well-known British abbreviations such as "ok", "pse", "for", "fm", "tks", etc., often were found in traffic. There was also a certain amount of amateur radio procedure used. In addition, as a separator between call signs the Russians used both "de" and "a". The letter "r" was used as a break between numbered groups in cipher text while a comma was used in clear-text messages. No break sign was used in the radio nets of higher headquarters, the only indication of a break sign being a pause after a word or code group had been completed. This was one radio characteristic which aided the German traffic analyst in identifying the traffic of higher Russian headquarters.[IF-187, p.48]

b. Radio Discipline.--When Russian nets underwent call sign changes or frequency changes, the German intercept operators had little difficulty in identifying the nets since a lack of security in turning on of radio sets and checking of frequencies (known as "tuning") invariably permitted recognition of the changes In the nets.[IF-187, p.49]
Security violations were often committed when work shifts were changed. An excellent example of the type of information thus made available to the Germans is to be found in the following intercepted message.

"This is Mishka, how did you sleep?"

"We could not decode the third group in your message number 25 of last evening."

"You must transmit it again."

Thus Mishka and his request not only gave the Germans the identity of the net but enabled them possibly to obtain a previously intercepted message in a new key if the second operator complied with the request to re-transmit the message.[IF-187, p.49]

Some Russian operators furnished the Germans with a good insight into Russian morale by "griping" over the radio. Some of the operators were so obliging as to inform other operators of the new frequency which they would begin using at a specified time.[IF-187, p.49]
Russian lapses in radio discipline often led to obtaining by the Germans of valuable intelligence. At one time the scarcity of traffic from a part of the Leningrad front led the German Signal Intelligence to think that the Russians were planning a new offensive. The German Signal Intelligence already knew the identity of Air Combat units which were based in that area. Therefore, when messages from the Finnish area were

intercepted containing the names of escadrille leaders and instructions for future operations, it was established by the German Signal Intelligence that those units formerly located on the Leningrad front had moved to the Karelian front in Finland. This intelligence, which was subsequently proven correct, was obtained by the Germans although a complete change of call signs and frequencies had been made by the Russians.[IF-187, p.49]

5. Special Traffic Characteristics.

a. Call Signs.—The following information concerning work which the Germans did on the Russian Call Sign Books was written by Uffz. (Non-commissioned officer) Wilhelm HEIMANN. The Russian call sign system, according to HEIMANN, is a continuation from a previously known system which the Germans had analyzed. The production of the call sign books was by the same method as had been used with the older system, but the manner of selection of the call signs by encipherment of the radio station basic numbers was different and new. This latter method was almost identical to the system used by the Germans after November 1944 when all the call sign systems used by the Germans were changed. HEIMANN thought perhaps the Russian method may have influenced the adoption of the same method by the Germans. One difference between the two methods was that while the Germans enciphered a call sign which was determined by the enciphered basic radio station number, the Russians merely used the enciphered basic number for determining directly the page, row, and column in the call sign book where the new call sign would be found. "Consequently", said HEIMANN, "the German system is unbreakable without, say, captured data; the Russian is quite breakable given sufficient call signs and day-to-day continuity."[IF-19f, p.6]

When the Germans first began studying the Russian system of call signs their purpose was to establish the call sign books or systems (Unterlagen) from which call signs were taken; the method of selection of the call signs from the book; and the various groups of call sign users. The objective of the Germans in making the study was to determine, on the basis of the call signs used, the character and composition of any given radio net; to identify in that net the various formations and to maintain continuity throughout call sign changes.[IF-19f, p.1]

The following methods and results of this study are given by HEIMANN:
"Call Sign Systems.

"There were found to be two tables (different of call signs:

"TPR 43: a list of 1,200 words, the first three letters of which were used in keying traffic.

"Call Sign Books: each with 1,100 - 1,200 call signs, which were compiled of letters and figures in such a manner that (excepting compilers' errors) identical call signs could not occur.

"TPR 43 had 16 pages, 74 call signs per page, divided into three groups, each of 25 call signs. Each group had 5 lines, each with 5 call signs. (The above is based on captured documents.)

"A Call Sign Book contains 100 call signs, in 10 lines with 10 columns, on each of its 11 or 12 pages. (Confirmed also by captured documents.)

"Prom the numbering of captured documents the approximate scope of this material can be estimated at about 17 to 18 books. Up till now, about 12 or 13 books have been in use. Books were not compiled as complete books, but approximately 200 pages were first compiled and then split up into books. Each page contains 96 call signs beginning with 32 different characters, 3 call signs per character, and 4 call signs beginning-with 2 other characters, 2 call signs per character.[The translation here is very poor. What appears to be meant is: "Each page contains 100 call signs per page. 96 of these are 3-letter call signs which begin with 32 different possible characters. The remaining four call signs are 2-letter call signs and must begin with the remaining two letters of the Russian alphabet. The Russian alphabet with the English equivalents, together with the International Morse characters, are given below.]

Russian	English	Morse	Russian	English	Morse
А	A	.-	П	P	.--.
Б	B	-...	Р	R	.-.
В	V	.--(W)	С	S	...
Г	G	--.	Т	T	-
Д	D	-..	У	OO	..-
Е, Э	E	.	Ф	F	..-.
Ж	ZH	...-(V)	Х	KH	....(H)
З	Z	--..	Ц	TS	-.-.(C)
И	I	..	Ч	CH	---.
Й	I*	.---(J)	Ш	SH	----
К	K	-.-	Щ	SHCH	--.-
Л	L	.-..	Ь,Ъ	HARD, SOFT SIGN	-..-
М	M	--	Ы	YE	-.--
Н	N	-.	Ю	YU	..--
О	O	---	Я	YA	.-.-

*** With another vowel.**

"No call signs began with E, Z, R, U, SHCH ((Q)), and 0. The 34 characters, therefore, used as beginners ((i.e., initial characters)) were:

"A, B, V ((W)), G. D, ZH ((V)), I, J, K, L, M, H, 0, P, S, T, F, KH ((H)), TS ((C)), CH, SH, Y, X, IU, IA, 1, 2, 3, 4, 5, b, 7, 8, 9.

The unused beginners are obviously those likely to be confused with Russian International Call Signs, operating signals, etc.

"Since the 34 beginners would have yielded 3 x 34 = 102 call signs, 2 beginners in rotation were selected to form 2 call signs each.

"The affiliation of the books could thus be recognized by knowing which 2 initial characters on each page were those limited to form 2 call signs each.

"To keep check on the allocation of call signs to individual pages the compiler used a list in which the 34 initial characters each had two sheets, one extending from A to TS ((C)) and the other from CH to 9.[See Figure 1, p 16]

"The compiler, having derived the call sign, say AAA, entered it in any position on the page which was then apportioned to one of the 17 or 18 books. The designation of its location, in terms of page and coordinates on that page, e.g., page 07, coordinates 23,[Figure 2, p 1.6] were then entered in the space for AAA. Some pages would then appear diagonally adjacent, while others would be vertically or horizontally adjacent.[Figure 1, p 16]

"The printed text of 11 or 12 pages was so arranged that two pages were printed on one side of a sheet of paper. Thus two pages were permanently associated.

"After some time these sheets, each of two pages, could be unbound and reshuffled so that a completely new arrangement of books resulted. Reshufflings of this type took place at the beginning of October 1944 and in the middle of February 1945.

"Manner of Selection."

"Formations working with TPR 43, especially from the division forward, were allotted a page by the chief signals officer; selection was made according to the individual's fancy hut often the page was used line by line. Such stereotyped usage led to the recognition of call signs."[I-19f, p. 2]

b. Russian Secret Police Nets.—The High Command nets of the Russian Secret Police (MKVD), often including the nets of regiments forward to battalion, entered the call sign selected from TPR (either consecutively or at random) in 10 x 10 squares (100 call signs). By means of daily changing digit coordinates for the squares it was possible to issue a maximum of 100 call signs to a radio station provided with a 2-digit basic number. This system was valid for three months.

For example, consider a radio station with the basic number 31. The call sign for the first day is SHOP. The call sign for the second day is NASH, and the call sign for the 96th day is STA.[Figure 3]

For enciphering the 10's digits of the radio station basic number there were 6 vertical coordinate columns and for enciphering the 1°s digits there were 6 horizontal coordinate rows, thus yielding 6 x 6 = 36 possible encipherments per month. The columns and rows changed monthly; the contents of the square changed quarterly.[I-19f, p. 3]

c. Air Force Ground Nets.—The nets of the Air Force Ground areas (RAB) entered the call sign selected consecutively from TPR 43 in similar squares and then used these squares, line by line, for 31 days. For the RAB which used this procedure the same call sign and meaning recurred every calendar month. [I-19f, p. 3]

For radio stations with call sign books 3-digit radio station numbers were issued. Thus up to 1,000 stations could make a daily change of call signs by means of one call sign bock. The basic radio station number was changed daily by enciphering it by means of a simple substitution table which would then give the page In the call sign book; the vertical coordinate; and the horizontal coordinate. The intersection of these coordinates would then indicate the dally call sign.[Figure 4, Figure 3]

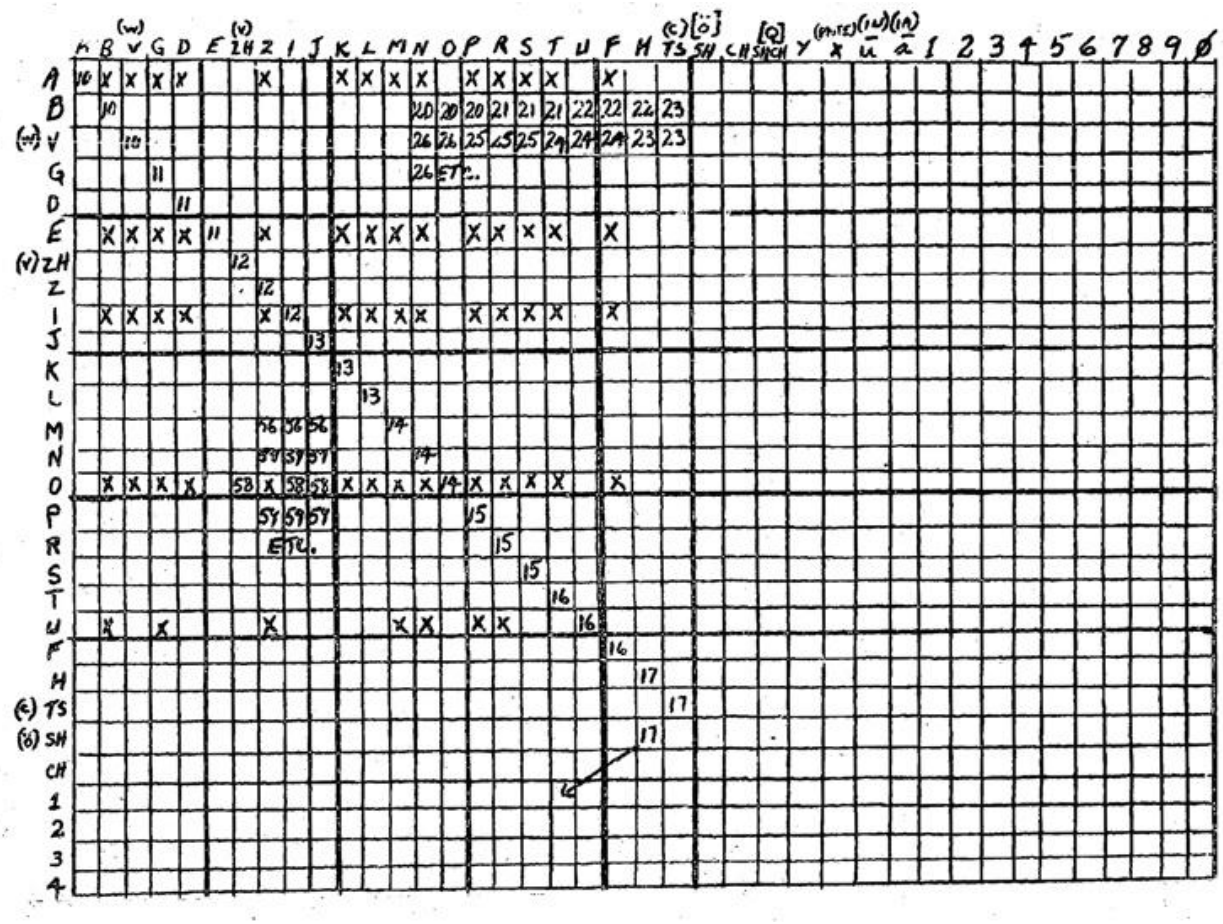

Figure 1. X- PRONOUNCABLE Type CALL GENERALLY TPR. 43

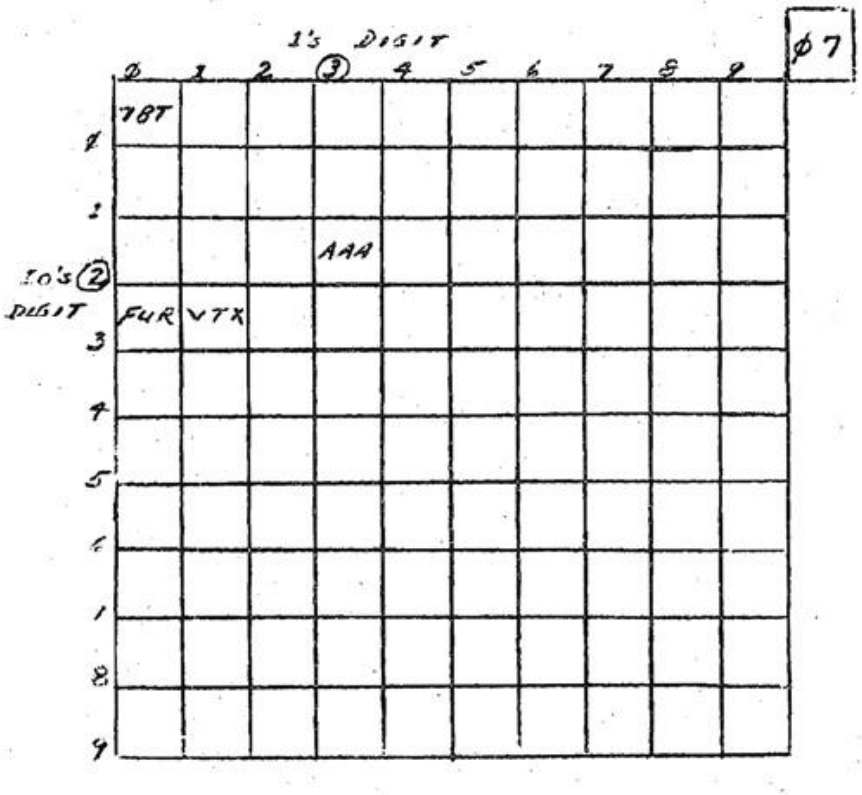

Figure 2. PAGE IN CALL SIGN BOOK.

DAY OF MONTH

DAY OF MONTH

			2	17	96	3	1	9	8	5	
			61	1	7	8	9	1	Ø	7	
			3	48	10	7	3	5	1	9	
			9	5	6	BAC	FAL	DOM	SOM		
			Ø	3	1	POM	TUR	SHUF	LEN		
			4	7	5	MO3	STA	YOS	BOL		
			5	6	9	WOL	NKT				
			3	2	Ø						

Figure 3. PAGE OF THE TPR 43 CALL SIGN BOOK

1. Find day of month in 6 x 6 square in upper left hand corner.
2. Locate first digit (10's) of basic station number in vertical column in which day of month is located.
3. Locate second digit (1's) in horizontal row in which day of month is located.
4. Intersection of these coordinates gives call sign.

Digits of basic radio station number	0	1	2	3	4	5	6	7	8	9
100's digit substitution	5	7	2	6	0	8	1	3	9	4
10's digit substitution	6	4	5	2	7	3	0	8	9	1
1's digit substitution	2	8	4	6	0	7	5	3	1	9

Figure 4. SUBSTITUTION TABLE FOR BASIC STATION NUMBER

1. Locate digits of basic radio station number at top.
2. Substitution for digit will be found in column underneath each digit according to 100's, 10's, or l's position.

3. EXAMPLE:
Radio station basic number - 587
Substitution for first digit (5) in 100'th position is "8".
Substitution for second digit (8) in 10's position is "9".
Substitution for third digit (7) in 1's position is "3".
Enciphered number is therefore 893 and gives:
8 = page of book
9 = vertical coordinate
3 = horizontal coordinate.

The rows of 10 digits used in the substitution table (see Figure 4) were taken from a large table of 100 rows which were derived by cyclical substitution from 17 basic rows. The three rows of digits to be selected dally were found from a table which was valid for three months. This table consisted of a column indicating the day of the month. Opposite each day of the month were three columns. In each column was the number of the row which was to be selected from the large table of 100 rows. The table was 9 columns wide; the first 3 columns designating the first month; the second 2 columns the second month and the last 3 columns the third month. The arrangement was such that in any one column no row of the 100 row table was repeated during the three months effective period. [I-19f, p. 3]

d. Groups of Call Sign Users.—The General Staff radio nets used their own call sign book up till about February 1945. After this date the call sign book was not identified by the Germans in other traffic. The High Command nets: i.e., the Front Armies and the Front Corps, used their own call sign book only from July 1944 until March 1945.

There were four call sign books for the Armies, Air Army, and Corps nets. The Armies of two or three widely separated fronts employed one call sign book jointly so that only by direction finding was it possible to establish on which front any particular Army was located. While the various groups of users had to be determined after every re-shuffling of the pages of the call sign books, this gave the Germans little trouble and often brought additional Intelligence. For example, the last re-shuffling in April 1945 brought to light that the call sign books of the command nets contained an additional 11th page in place of the usual 10 pages "which was not affected by the enciphering process and served to select emergency call signs, which then were used as permanent call signs. The books of the Army nets even had two additional pages." [I-19f, p. 4]

e. Another German prisoner, Corp. HEUDORF, who was a radio and intercept operator on the Eastern front, also was interrogated on Russian use of call signs. He stated that until July 1944 the Germans knew the Russian call sign system wery well and were able to make predictions which were reliable. At the beginning of July 1944 the Russian radio nets maintained radio silence for seven weeks preceding the Russian offensive which took place in the late summer. When radio silence was lifted all the Russian call sign systems had been changed. From that time on it was very difficult for the Germans to have much success with the call sign

systems. However by the end of April of 1945 HEUDORF stated that good progress had been made in solving the system.[I-75, p.8]

f. Five other German prisoners, Sgts. Erich KARRENBERG, Dietrich SUSCHOWK, SCHMITZ, HEMFEL, and Corp. GRUBLER, described the technique used by the Germans in identifying radio stations in the People's Commissariat for River Shipping (NKRF). They stated they had no particular difficulty in locating the stations

"About 50% of the messages are not sent direct from the station of the sender to the recipient but are passed on, in some cases by way of three or four stations. For example, suppose that Saratov (RBUU) has some urgent messages for Moscow (RBFC). But the next traffic time between Saratov and Moscow is not until two hours later. However, Saratov has traffic at that moment with Kuibeshev (RBFR) and knows that because of its traffic schedule Kuibeshev will be working with Moscow immediately after it has finished with Saratov. So Saratov sends its messages to RBFR Kuibeshev:
IZ RBUU 465 68 3/10 1200 MOSKWA A/P POLKOWNIKU PRONINU 465 143 476.....243/2 G0RBACEW.[The message reads: FROM RBUU 3/10 1200 hours
Moscow. For Artillery Regiment, Lt. Col. PRONIN
Signed GORBACEW]

"On conclusion of the traffic RBFR acknowledges receipt of the messages to Saratov, calls Moscow and begins:

IZ SARATOV 465 68 3/10 1200 MSK A/P PRONINU 465 143 476….. 243/2
G0RBACEW.

"This shows clearly that RBUU is Saratov. Naturally one is not always so fortunate as to be able to follow such a pass-on in its entirety. A simple expedient is to collect signatures in conjunction with the call signs and places which come up with them. For example:

RBUU GORBACEW OEOERIN
SARATOV OEOERIN GORBACEW

"If one has at least two names which come up together one can say certainly that the call sign and location have been identified. One name alone is not sufficient for identification, as in a large net there might easily be people with the same name working at different places."[I-168, p 7]

g. German personnel working on identification of Russian call signs, stations, and nets kept elaborate card indexes which contained all known and unknown call signs picked up on the entire Eastern front. These cards showed whether, and in what connection, the call sign had previously appeared. A cover name index was also kept which contained all the cover names that had been collected, and indicated the source and date of occurrence. With the assistance of these card indexes almost complete cover name tables for the Russian fronts were recovered.[1-187, p 2]

h. The call signs of all Russian ground stations were made up of three characters, either of letters, or letters and figures. An exception was the fixed 4-letter call sign used on several transport nets. For the greater part the call signs were taken from a call sign book used by the Russian Army after April 1944.

To form the call signs all the letters and the digits from 1 to 9 were used. However as in the case with the book TPR 43 the letters E, Z, R, U, SHCH((Q)) were not used as the first element of the call sign. Each page of the book contained 1,000 call signs. These call signs were changed at irregular intervals, sometimes daily and at other times at longer periods. When units and headquarters moved, a suffix was added to the call signs of the various echelons. Thus, "BEM"—rear echelon; "BEM-1":—advanced echelon.[1-187, p.50]

Call signs used by the Russian Army, Air Forces, and the Russian Secret Police (NKVD) down to division nets had the general form of "XXB", where X could represent any letter of the roman alphabet or any digit from 1-9 (0 not being used), while B could only represent a letter. Letters of the Russian alphabet such as r'IA" {.-.-), "IU"(..--), "CH"(---.), and "SH(---) were omitted for the purpose of camouflage since those letters only appeared in Russian Morse traffic and thus call signs employing those Morse characters would be recognized

immediately as being Russian. Similarly 0 was not used since the Russian operator always used the abbreviated form (-) which would have confused it with the letter T.[1-173, p. 21]

[*The Russian Secret Police (NKVD) worked in conjunction with the Russian Armed Forces. The functions of the NKVD frontier troops as follows:
a. Arrest of Army deserters.
b. Prevention of infiltration by enemy groups into rear areas.
c. Location and arrest of enemy agents dropped in rear areas.
d. Evacuation of civilians from battle zones.
e. Supervision of railroad traffic; guarding of railroad lines, traffic routes, bridges and Industrial plants; close search of forests and villages for deserters and enemy agents.]

The call signs were taken from a call sign book consisting of 26 pages, each page containing 35 x 35 or 1,225 items (the 26 letters of the roman alphabet plus the digits 1-9). The last element of the unenciphered station call sign indicated the page of the book (the 26 pages corresponding to the 26 letters of the roman alphabet); "the first element of the call sign indicated the horizontal row of the designated page; and the second element indicated the vertical column. Call signs beginning With "SHCH (Q)" or "Z" were not used as these might be confused with the procedure signals of the International Q or Z code. One call sign block was kept for long periods of time, apparently for a year in most cases. It was assumed by the Germans that units of the Army, Air Force and the Secret Police (NKVD) all took their call signs from one block, for by this means the simultaneous appearance of the same call sign at different places was most easily avoided. Units which appeared in regimental nets down used call signs of the general form "BBB" in which "B" represented any letter of the Russian alphabet. These call signs were formed from the cover name allotted to the units. If, for instance, a unit was allotted the cover name "SVJEZDA" for a certain time, it would use the call signs SVE, SZA, SED, etc., in its radio traffic. No changes might he made in the sequence of the letters. Call signs were chosen so that no confusion was possible. These call signs were changed at intervals of one day to a week, and occasionally were changed at the same time a new cryptographic system was placed in effect. However, there were exceptions to the above use of call signs. From time to time it was observed by the German operators and traffic analysts that some radio stations appeared whose call signs varied from each other only by the addition of a numeral. If these stations belonged to a division or higher echelon, then they were all in the same unit, but if the call signs appeared in a small unit the stations belonged to individual aircraft, tanks, etc. in communication with a ground station, leading tank, etc.[I-173, p.21]

The call signs of a few of the higher Secret Police (NKVD) units, and of the nets of the "Artillery Reserve of the Supreme Command" were, in some cases, made up of four elements. These were not taken from call sign blocks nor formed from cover names. In all internal state traffic of the people's Commissariat international call signs were used.[I-173, p.21]

i. Cover Names.
Cover names (simple in nature) were used frequently by the Russian military forces to cover or camouflage the identity of units, locations, proper names, airfields, etc., and could be found in various positions in messages. Examples of cover names which were common were ROSA and RUBIN.[IF-187, p. 50]

The German Signal Intelligence Regiment 353, which was on the Russian Northern front, reported it was easy to solve the simple code cover name system used by all the air units in that sector. Each air division had a code name which changed three times a month. Regiments used the basic divisional code name plus a figure suffix, the lowest regimental number having the lowest suffix. Aircraft had a basic code name according to type to which would be added the regimental suffix, and either a number or the pilot's name to indicate the individual aircraft. Ground control stations with the armies in the field also had a basic code name with figure suffixes for subsidiary stations.[I-163]

j. Proper Names.
The use of proper names often led to the identity of particular Russian traffic. Statements of the capture of German prisoners, communiqués, and press reports often served to confirm identifications which the Germans had previously made. Air base depots and airfield battalions used the names of unit commanders in the clear as a signature to messages or put the names in the actual message content in plain language.[IF-187, p. 51]

k. Preambles.
Messages of the Anti-Aircraft Defense (Protivovsduschnaya oborona--PV0) units could be recognized from their preambles alone. Three 2-dlgit cover numbers and the abbreviation "VZD" (air—vozduch) were used in the preamble. At other times a 3-digit cover number followed by the abbreviation "MU" with "IJ" at the end of the message was to be found. The text of these messages usually contained 5-digit groups interspersed with 6-digit PVO grid references.[IF-187, p. 51]

l. Message Number Sequences.
Russian messages were numbered consecutively and these numbers could often be used to identify traffic. The message number was usually the last group in a message.

6. Methods and Results of German Traffic Analysis.
The analysis of Russian Army Air Force traffic will be treated at the same time since the organizations of both were so closely tied together. The main purpose for the existence of the Russian Air Armies in the military command w. for the support which they could give to the ground forces.[IF-187, p. 9]

The German traffic analysts worked hand in hand with the intercept operators on Russian traffic. The tasks of the traffic analysis section on the Southern Russian front were to record the radio characteristics of Individual Air Armies, to identify the various radio nets and their inter-relationships, and to identify call signs and reconstruct call sign lists.[IF-187, p. 41]

The successes on the Southern front and the information gained from sources other than cryptanalysis may be summed up as follows:

a. Knowledge of the Russian air situation.
b. Knowledge of the organization and order of battle of Russian Air Armies.
c. Knowledge of the strength of Russian units including types and armament of aircraft.
d. Knowledge of the location and occupation of airfields.
e. Knowledge of the movements and concentrations of Russian air and ground units.
f. Knowledge of operational intentions.
g. Knowledge of the amount and type of air transport.
h. Knowledge of the supply situation.
i. Knowledge of probable targets.

Interrogation of members of the German Army Kona No. 1 (Kommandeur der Nachrichten Aufklaerung 1) brought to light some important facts concerning German successes in analyzing intercepted Russian traffic.[IF-186, p. 149] Kona 1 was engaged in the interception, analysis and evaluation of the Russian Army, Air, and Secret Police (NKVD) traffic on the southern half of the Russian front from June 1941 until May 1945. The Germans were able to obtain, as a result of this work, an accurate picture of the Russian order of battle. They were able to take oftentimes, to predict the time and location of impending Russian offensives in sufficient time to be able to take advantage of such information. These results were achieved more by the close interrogation of all available sources of information (traffic analysis, evaluation, prisoner of war interrogation, captured documents, etc.) than by reading of enciphered or encoded traffic. However, there was considerable of the Russian low and medium grade traffic read. In the German Command organization there existed considerable rivalry between the cryptanalytic and traffic analysis personnel on the relative merits of their respective units. This fact appears to have created definite disturbances as to which of the two units was the most valuable source of intelligence to the German High Command. It seems, from the overall picture presented by the interrogation of German personnel of the two units, that to the German Signal Intelligence the respective value of traffic analysis and of cryptanalysis was about three to one. This is due to two factors:

a. The general unreadabillty of Russian high grade traffic because of the extensive use of one-time pad systems.

b. The large amount of information that could be extracted from the generally low standard of Russian radio and cipher security, especially in respect to the use of call signs and radio frequencies and indicators.[I-196, p.1]

Russian security, from a cryptanalytic angle, was based almost entirely on the use of one-time pad systems for high level traffic and the use of a large number of code books and enciphering tables for medium and low level traffic.[I-19b, p.1]

The main source of information to the traffic analyst came from the Russian use of call signs and indicator groups and from stereotyped direction-finding reports. On the basis of this information the German traffic analysts established a detailed and accurate order of battle of the Russian forces operating on the entire Eastern front. In addition they also gained information concerning Russian operational movements and intentions.[I-19b, p. 19] ft

The Russians had a habit of using the surnames of officers and pilots, for code and cover names. This was especially so in the Air Force. This type of information was considered very valuable by the Germans.

Quite often the Information provided by the German Signal Intelligence units to the various German combat units went unheeded. For example, in the fall of 1941, when the Germans were attempting to effect a junction with the Finns at Tichvin, certain radio characteristics appeared in intercepted Russian traffic which had been noticed two weeks previously in traffic emanating from Siberia. This fact was evaluated by the German Signal Intelligence as an indication that Russian troops had been transferred in this short interval from Siberia to the sector north of Tichvln. The German Command maintained that such a thing was impossible, and therefore did not take any evasive action. Consequently, the Russians attacked in great force and won a decided victory. The junction with the Finns never took place. The railroad between Leningrad and Moscow was liberated by the Russians and the Germans were forced to take up positions on the Volchov front leaving the "hedgehog" redoubt at Demyansk to its fate. .[IF-186, p. 16]

A clarification of the working organization of the Russian Air Force is advisable before considering the weak points in their transmission security. The Air Forces were an integral part of the Russian Army. Their operations were confined primarily to the tactical air support of ground operations. During operations actual command was by the ground force commanders, with the air commanders acting in an advisory capacity and having sole responsibility for the successful execution of missions. The structure of the Soviet Air organization emphasizes it as an instrument of the Army. Of some 12,000 Russian aircraft identified by the German Luftwaffe Signal Intelligence during the war (not counting long-range bombers which were in a separate organization) almost 10,000, or more than 8056, were fighters and fighter bombers. The remainder were bombers and operated mainly against front-line targets. At the end of the war there were 11 Russian Air Armies operating on the Eastern front. These were, from south to north, the 17th, 5th, 8th, 2nd, 6th, 16th, 4th, 1st, 3rd, 15th, and 7th Air Army. One Air Army was assigned to each Army Group to which It was operationally subordinate, and was then subdivided into Corps, Divisions, Regiments, and Escadrilles. Each Air Army had two to eight Corps, according to the importance of its work. At first these corps were mixed fighter, fighter-bomber, and bomber units. During the war, however, there was a tendency to change these mixed units into uniform corps, and by the end of the war there was only one mixed corps left on the East front: the VI Corps. Each corps was made up of two to three divisions; each division of two or three regiments; and each regiment of three escadrilles. Reconnaissance and artillery observation aircraft, as well as transport units, were sometimes organized into escadrilles, but usually they were regiments and were directly subordinate to the Air Army. Each Air Army also had one reconnaissance and one artillery observation regiment. In areas where preparations for a concentrated attack were being carried out the Air Armies were often reinforced by one or more of these regiments. By noting such reinforcements the Germans could recognize, at times, the intentions and probable plans of the Russians. IF-187, p. 9]

<table>
<tr><th>GERMAN</th><th>AMERICAN</th><th>BRITISH</th><th>RUSSIAN</th></tr>
<tr><td>Staffel 9-12 planes</td><td>Flight 8-12 planes</td><td>Flight 8-12 planes</td><td>Escadrille 8-10 planes</td></tr>
<tr><td>Gruppe (3 Staffeln)
27-30 planes</td><td>Squadron 20-30 planes</td><td>Squadron 20-30 planes</td><td>Regiment about 30 planes</td></tr>
<tr><td>Geschwader (3 Gruppen)
80-90 planes</td><td>Group 70-90 planes</td><td>Wing 70-90 planes</td><td rowspan="2">Division (2 or 3 Regiments, usually 3) 60-150 planes</td></tr>
<tr><td>Fliefu-Jaffu 1 (2 Geschwader)
about 160 planes</td><td>Wing 210-360 planes</td><td rowspan="3">Group (number of planes depend on mission)</td></tr>
<tr><td>FPlieger-Division About 320 planes</td><td rowspan="2">Command (2 or more wings) 700-1,500 planes</td><td rowspan="2">Corps (2 or 3 Divisions)
120- 450 planes</td></tr>
<tr><td>Plieger Korps (2 or 3 Divisions). About 600-900 planes</td></tr>
<tr><td>Luftflotte</td><td>Air Force</td><td>Command or Tactical Air Force</td><td>Air Army</td></tr>
</table>

Figure 5. COMPARATIVE STRENGTH OF GERMAN AND ALLIED FORCES [IF-187, P 9a]

Lt. Werner RASCH, of the 353rd German Air Force Signal Intelligence Regiment in the East, gives the following account of the development and achievements of the Russian Long Range Bomber Forces (ADD—Aviatsiya Dalnego Dyestviya).

"Soon after the outbreak of the Russian-German war, practically all of the Russian Long Range Bomber Force was destroyed, either by German attacks on Russian airfields, or in combat with German fighters. What was left of it was withdrawn from action. Marshall GOLOVANOV, chief of ADD, reorganized his forces with the intention of using them in night operations only, owing to the threat presented by the strong German flak defense. The first successful operations following the reorganization took place in the battle of Stalingrad (September 1942 - February 1943). From then on, ADD operations played an important part in all Russian offensives. The training for night operations was of long duration; at the end of the war each bomber regiment had crews which were still in a training status.

"The achievements of the ADD units were not very impressive. Crews were not trained for carrying out night attacks in close formation. In the latter days of the war 60 aircraft of a division need approximately one hour to assemble and take off, and even this was accomplished only under the most favorable navigational and meteorological conditions. In planning an attack, each division was allotted 20 minutes over the target; in that time it was intended that all aircraft of one division should have completed their mission and moved out to make room for the next division. Unless targets on the front itself were being raided, the front line was usually crossed before dark. This permitted the take-off to be made during daylight, and the first aircraft to take off were held in an assembly area in order that a close-flying formation be formed. Formations equipped with radio-telephone communications were again brought into close order by the leading aircraft of the regiments before going into the bomb run. Each regiment had several Pathfinder aircraft, which were flown by the most experienced crews, since the success of the mission depended upon their efforts. In addition to their flares, they usually carried a 1,000 pound bomb."[IF-187, p. 30]

7. Point-to-Point Nets.

These point-to-point nets of the Long Range Bomber Forces (ADD) alone were a sufficient basis on which the Germans could build up an accurate picture of the ADD organization. When the 18th Russian Air Army was reorganized the Germans immediately recognized such steps from traffic on these nets. The most profitable traffic in these nets, from an intelligence standpoint, came from units which were widely separated in the field as this necessitated the use of radio facilities for communication. In instances where the units were close together very little signal intelligence could be gained since there was slight need for radio transmissions.

From the intercept and analysis of traffic on these point-to-point nets, movements of the Russian Air Army units, locations and occupations of airfields, numbers of operational and unoperational aircraft, and locations of supply dumps could be determined. Traffic intercepted on these nets also gave the Germans considerable information regarding intended operations and offensives. One outstanding success along this line occurred when a Russian order to bomber units was intercepted by the Germans. The message ordered an attack on Shavli, Lithuania, where an entire German Panzer Army was immobilized due to a lack of sufficient fuel. The German Signal Intelligence Service reported the information to the Luftflotte which provided fighters to meet the Russian Long Range Bombers while German JU 52's dropped gasoline supplies to the encircled Panzer Army and enabled it to escape.[IF-187, p. 36]

8. Call Signs and Frequencies.

Three-character call signs were used in t radio nets between the Air Army and Its Corps. They were changed once during the day and once at night, at which time the frequencies also were changed. Call signs were based on an arbitrary combination of letters and digits and were selected from a call sign list that changed monthly. The Germans were unable to determine whether any definite system was employed for the choosing of the call signs. They did notice, however, that during the course of a month a call sign used by a given radio station might be repeated without the succession of call signs which had followed at the time of the previous occurrence. Traffic between corps and divisions took place with a periodic change of call signs, but on fixed frequencies. This fact aided the intercept tasks of the German Signal Intelligence. Frequencies used were in the 2,500-5,000kilocycle band: i.e., the normal Russian military frequency band. The call sign systems and the time of change differed from corps to corps as there was no over-all unification in their communication systems, and this fact was a great aid to the German Signal Intelligence in identifying the various units. Each radio link had two different frequencies for use during the day and two different frequencies for use at night. The night frequencies lay in the 3,400-4,500 kilocycle band; the day frequencies between the 5,000-8,000 kilocycle band. As the seasons of the year advanced the day frequencies gradually moved up to a maximum of 10,000 kilocycles.[IF l87, p. 37]

9. Analysis of Characteristic Messages.

a. Address and Signature Groups.— Five-figure messages of the Russian Long Range Bomber units could not be decrypted by the German Signal Intelligence Service but they were able to extract a great deal of important information from the analysis of data found in the message numbers and delivery groups. In these messages the signature group was next to the last one before the message number group. This signature group was constant and served to identify the headquarters of the originator, each headquarters having a 3-digit designation. Two zeros inserted in front of the 3-digit signature designation completed the 5-figure group. Since no other Russian 5-figure traffic contained similar groups, this signature was the most essential characteristic for the identification of the traffic of the Long Range Bombers. The traffic was further identified by two address groups contained in the preamble of the messages. These address groups were likewise 3-digit groups, repeated periodically, one of them designating the unit and the other the section. In front of the address group appeared the symbol "ADR" (address). In front of the signature group appeared the symbol "SIG".[54IF l87, p. 38]

b. Pre-arranged Message Forms.— A very valuable source of intelligence was found in the pre-arranged message forms which all the Long Range Bomber units were required to send in to their commands. These messages contained data on regimental reports of locations, strength, and aircraft serviceability. One type of these pre-arranged message forms was "Form 1": a dally report sent by division to corps, containing regimental strengths in personnel and aircraft. The text of the messages consisted of unenciphered numbers proceeded by a 2-digit null, resulting in a four or five digit group. The ' following is an example of such a message.

**"12238 1350 1436 2332 2430 2502 2629 2728
2801 2903 3002 3101."**

After removing the first two nulls of each group the message can be interpreted as follows: (12)238 indicates the designation of the regiment whose strength is being reported: i.e., the 238th Regiment. The second group (13)50 contains data on personnel strength—the details of which were never definitely determined by the Germans. The last nine groups (2332 through 3101) refer to aircraft strength and must be read in units of three groups. After again removing the two nulls of each group, the first gives total number of planes; the second group the number of serviceable planes; and the third group the number of unserviceable planes. In this case (23)32, (24)30, (25)02 indicates there is 32 planes total; 30 serviceable, and 02 planes unserviceable. The second unit of three groups, (i.e., groups 2629, 2728, & 2801) indicate the total number of aircraft on an airfield, and the number of serviceable and unserviceable planes. In this case there are a total of 29 planes, of which 28 are serviceable and 1 unserviceable. The last three groups (i.e., 2903, 3002, and 3101) refer to regimental aircraft which had landed at other airfields. In this case, a total of 3 planes, of which 2 are serviceable and 1 unserviceable.

**Another pre-arranged message form, known as "Form 4," was sent every fifth day by division to corps, and by corps to Air Army. Here again the text of the message consisted of numbers in the clear slightly camouflaged by a two-digit null in front of each group. An example is as follows:
"22250 3246 4214 42685 5229 6203 7240 .... 1219"**

By again removing the two nulls of each group the messages gives the following information:

(22)250 (32)46 (42)14 (42)685 (52)29 (62)03 (72)40 (12)19.

Message being reported by the 250th Regiment; located at 46, a grid system of coordinates not too difficult to solve (this system, changed monthly); 14 aircraft type; 685 serviceable aircraft; 29 aircraft unserviceable; 03 and 40 give details of personnel strength which the Germans never could, fully understand. The last group "19" indicates the number of crews ready for operations.

The two types of pre-arranged message forms given above were the two main sources of Information for the German Signal Intelligence in gaining information of the organization, order of battle, location, and aircraft strength of the Russian Long Range Bomber Forces.[IF-187, p. 38]

c. Operations Reports.— Reports of results of operations were also sent by Corps to Air Army by pre-arranged message forms. These messages contained details as to the number of aircraft taking part in an attack, the target, time and altitude over the target, weight of bombs dropped according to type, results observed by flying personnel, details of German defenses, details of Russian losses, and observations of weather conditions. Quite often messages from corps to division containing operational orders were also intercepted. These messages contained details as to the target, the time of attack, and the altitude of attack, and often afforded ample time for German counter-measures to be effected. The division also reported to corps the number of aircraft to participate in the attack, as well as the time of take-off. This information provided the Germans with a valuable and reliable basis for route-tracking.[IF-18, p. 40]

d. Airfield Serviceability Reports.— Corps were required to make daily reports on the serviceability of airfields being used by their regiments and divisions. Airfields locations were given by using a 6-dlgit grid reference system. The serviceability was indicated by constant 4-figure groups designating "serviceable," "partially serviceable," and "unserviceable." These reports afforded the German Air Force Signal Intelligence a good picture of Russian airfield serviceability and of any changes in location which might have taken place.

e. Orders for Use of Navigational Aids.--The headquarters of the Air Army transmitted messages to subordinate commands ordering the use of navigational aids for a particular day, and indicating the type of aid to be used. When these messages were intercepted it could be taken as a definite indication of a forthcoming operation. If no messages were intercepted it could be interpreted that no attack was to be anticipated during that day or that night.[IF-187, p. 40]

f. Weather Messages.—Weather messages were of great assistance to the German Signal Intelligence Service in identifying the geographical origin of other traffic intercepted on the same radio nets. These weather messages often mentioned in the clear the names and locations of Russian meteorological, stations. Thus probable location of the radio station could be made.

The Russian weather messages could be recognized easily by the German Signal Intelligence Service because of message preamble characteristics, by random use of the letter "X" within the text, and by the absence of message number and delivery groups. In the early part of the war the Russians transmitted weather messages in the clear quite frequently. Later in the war all the messages were enciphered.

A large number of Russian weather messages were intercepted by the Germans. The contents of these messages, when decrypted, served two purposes. One purpose was to brief the German air crews on the weather conditions in Russia; the other purpose was to obtain advance warning of impending Russian operations. If a "winds aloft" message was intercepted by the Germans in the middle of the day, it could be taken as an indication of an impending air operation by the Russian corps transmitting the message.[IF-187, p. 41]

10. Air to Ground Traffic.

The assignment of call signs and frequencies used In air-to-ground radio traffic of the Long Range Bomber forces was performed individually by the corps signal officers and did not follow any uniform procedure throughout the entire Air Army. It was therefore a rather simple task, because of this lack of uniformity, for the German Signal Intelligence Service to identify the various individual corps by their call signs and frequencies. Each regiment, as well as each aircraft, was allotted two different frequencies: one for transmitting and one for receiving. The aircraft of each regiment were divided into two groups, I each group transmitting on its own frequency. The frequencies of the ground stations, in general, lay between 2,500 and 3,000 kilocycles, while the frequencies of the aircraft] were between 3,000 and 3,700 kilocycles. The aircraft of the IV Guards Corps of the 18th Air Army, whose units were equipped with American B-25 planes, and therefore had American radio sets, used frequencies between 1,800 and 2,500 kilo-cycles. Call signs on these air-to-ground nets remained in use for several months; the various call signs being repeated at irregular intervals of 5, 6, or 7 days. The regimental ground stations used 2-or 3-letter call signs, while aircraft used 1-or 2-letter call signs with numerical suffixes. These suffixes referred to the pilot rather than to the aircraft, and were allocated by either the commanding regiment or commanding division. When the suffixes were allocated by the commanding regiment the numbers of the suffixes ran from 1 to 32; when allocated by the commanding division they ran from 1 to 100. The German Signal intelligence Service could identify regiments after a short period of time because they also used special CQ call signs.[IF-187, p. 41]

a. Tuning and Take-off Traffic.—When the Russian bombers were assembling for the take-off on a mission the aircraft usually engaged in tuning traffic while still on the ground, and at the completion of tuning the traffic was usually terminated with a "QSA 4" or "QSA 5" procedure signal indicating what the signal strength of the radio set in the aircraft was. The tuning traffic furthermore was transmitted by one of the frequencies allotted for this purpose and was easily intercepted by the Germans. Thus, the beginning of an operation could be recognized immediately, because the end of the tuning traffic indicated that the take-off was to begin. In those divisions which had aircraft equipped with radio-telephone sets the noise of the engines being warmed up could be heard by the German operators, and this also served as an additional source of early warning. In the radio-telephone traffic, instead of using the complete call sign, only the numerical suffix was used.[IF-187, p 42]

b. Direction-finding Traffic.—The navigational training of the Long Range Bomber Force crews was so poor that "QDM" and "QDR" [QDM requests magnetic course to steer with no wind. QDR requests magnetic bearing in relation to station.] bearings constantly had to be given by the ground stations while the planes were enroute to the target. This fact aided the German Signal Intelligence Service in their route-tracking of the Russian Air Force because the Russians, instead of flying feint courses as did the Americans and British, usually flew a direct course to the target. Therefore, these direction-finding fixes sent by the ground stations could be taken as the actual course of the bombers and permitted the Germans to make a reasonably accurate target prediction. The direction-finding traffic between aircraft and ground stations did not possess any special characteristics as the bearings were given in the clear with little attempt at camouflage. The ground stations of the IV Guards Corps of the 18th Air Army used two nulls before a three-digit group indicating course bearings; e.g., 00252 indicating a course of 252 degrees. The I Guard Corps used the

abbreviation "TRS" before giving bearings on the outward flight, and "OPM" before giving bearings on the return flight. Other corps transmitted the letter "W" three times before giving the course bearing oh the outward flight and the letter "A" three times before giving the bearing on the return flight. These characteristics served to identify the type of traffic and unit.[IF-187, p. 43]

c. Tactical Traffic.—Over a long period of time German monitoring of bomber tactical traffic during approach flights resulted in the identification of the greater part of this type of traffic. The procedure signals used for this traffic differed with individual corps. In most cases the traffic consisted of 2 or 3-digit groups, sometimes enciphered and sometimes unenciphered. The III and IV Guards Corps were very free in their use of tactical traffic, their aircraft often reporting such data as take-offs, flight over the initial point (IPM), flight over the front, execution of mission, and observations over the targets. In such traffic the time was always given and this aided the German Signal Intelligence in its route-tracking. The ground stations also often transmitted data concerning the target or time of attack In cases where plans had to be changed after the planes had taken off. This data was very valuable to the Germans in determine the most favorable time to put their night fighters in the air for defense.[IF-187, p 44]

11. Russian Air Service Command Traffic.

The largest unit of the Air Service Command was the District Air Base Depot (Rayon Aviazionnogo Bazirovaniya—RAB) and, in the case of the Naval Air Force, the Naval Air Base Depot (Morskaya Aviabasa—MAB). As a rule each Russian Air Army had three to five of these RAB's. In order to use to the fullest extent the intelligence which could be gained from an analysis of the daily reports sent by the airfield battalions to their District Air Base Depots it was necessary for the Germans to draw up as complete a Russian Air Service Command order of battle as possible. The reports contained details on number of serviceable and unserviceable aircraft in the tactical units. From such an order of battle the German Signal Intelligence Service of the Air Force was able to correlate Russian airfields and tactical units, and to predict movements of tactical units on the basis of air- fields under construction. The locations of the airfields could be readily determined from the contents of the radio traffic between battalions and RAB's, and from direction- finding of the sending stations. Reports on the building of new airfields were of special value to the Germans since these reports often revealed enemy intentions and permitted the Germans to prepare defensive action against intended Russian offensives. Bo offensive ever commenced without strong air support, which necessarily meant that airfields had to toe located as near the active front as possible. The Russian Standard operating Procedure called for aviation in direct support of the ground forces to be located at bases not more than 40 kilometers (24 miles) behind the front. On some occasions the air bases were so near the front that Russian planes on the ground were hit by German artillery. The number and location of airfields under construction was a very good indication of the time in which an offensive could be expected.[IF-187, p. 21]

Radio traffic involving movements of airfield battalions was also monitored closely by the Germans. From this monitoring they could obtain clues as to the direction in which the tactical units would later move. AS an example, the reconquest of the Crimea by the Russians in the spring of 1944 liberated two Air Armies for further assignment. The German Command was naturally very much interested in where these units would go. In a few days the German Air Force Signal Intelligence Service had the answer; one airfield battalion had received an order to board a troop train in Simferopol. After the train departed the airfield battalion transmitted a message by radio to its District Air Base Depot at each stop along the way until it reached Gomel. It was obvious that the battalion would be followed by tactical units, if not by the whole Air Army. This assumption was confirmed a short time later when the entire 4th Russian Air Army moved from the Crimea to the Central front. The operational area of the second liberated Air Army—the 8th Air Army—was likewise quickly determined. A message from an airfield battalion was intercepted and read toy the German Signal Intelligence Service. The message stated: "The headquarters for the 8th Air Army in Tarnopol are ready." In a very short time this Air Army moved from the Crimea to this new sector.[IF-187, p. 23]

a. Supply Traffic.—Valuable intelligence was obtained by the German Signal Intelligence from the interception of radio traffic which gave details on supplies of fuel, ammunition and other materials. Details of railway movements of supplies were transmitted by the District Air Base Depots to their subordinate airfield battalions. These messages contained information on the destination, number of railway cars being used, amount and type of supplies, and the scheduled time of arrival. When the trains arrived at their destination a message announcing their arrival was sent to the airfield battalions, AS a result of the exploitation of this type of traffic the Germans were able to bomb successfully the stations soon after trainloads of fuel and ammunition had arrived. In the Southern sector a Service Command point-to-point

radio net reported arrivals of replacement aircraft for the 17th, 5th, and 8th Air Armies. These replacement planes were ferried from the factories to the airfields. Tactical units down to regiment level receipted for these planes and supplies, and from interception of these strength reports the Germans were able to estimate the production and distribution rate of Russian planes. Current fuel and ammunition supplies at airfields were reported on pre-arranged-message forms transmitted by the air-field battalions. These messages, since fuel and ammunition supplies were always increased prior to an offensive, afforded the Germans a sound basis for predicting impending Russian offensives.[IF-187, p. 24]

b. Miscellaneous Air Service Command Traffic. —-The Russian Air Service Command reported by radio on the achievements in salvaging German aircraft which had been shot down or which had been forced to land. These reports afforded the Germans with a source of information concerning their missing crews, and in many cases it was possible for the Germans to inform families that the crew members were alive and were Russian prisoners of var. Reports of interrogations of captured German military personnel were also often transmitted and intercepted by the Germans. In some bases as a result of the information contained in these reports, the German Command carried out court martial proceedings in absentia where the intercepted information carried sufficient proof that the German prisoners of war had revealed information of a secret nature. An Air Service Command of the 8th Russian Air Army on the southern front reported routes to be flown by aircraft in large-scale ground attacks, giving the time at which the attack would take place. For such attacks the Russian Air Army usually ordered the placing of smoke markers in the frontal area on the day before the attack would take place. These smoke markers were used by the Russian planes as an orientation point, and not only indicated the proposed direction to be flown, but also corresponded to the direction the ground force would advance. After a study of these smoke signals the German Air Force Signal Intelligence learned that the signals were lit thirty minutes to an hour before the actual time of attack. Thus, when it was learned that smoke signals had been set out the German Signal Intelligence could usually inform the Air and Ground forces some twenty-four hours in advance of plans for a Russian offensive. [IF-187, p. 25]

12. Russian Air Raid Warning Service.

The Russian Air Raid Warning Service was monitored regularly by the Germans. From this source the following information was available:

a. Reports of German aircraft over Russian territory and their positions.

b. Reports of Russian and American aircraft over Russian territory.
In the case of flight made entirely over Russian territory the time of departure and airfield destination was included. In the case of flights which crossed the front into German territory the time of arrival at the front would be given. When observation of German aircraft was reported by the Russians it was possible for the German Signal Intelligence Service to warn the planes that the Russians knew their positions and to recommend a change of course or other evasive action. Reports on American aircraft often revealed information about the "shuttle" or "triangular" flights of the 8th and 15th U. S. Air Forces.[IF-187, p. 26]

13. German Monitoring and Analysis of Russian Naval Traffic.

The Russian Navy had its own Air Force which performed the following duties:

a. Protection of Russian Naval units and their bases.
b. Support of Naval operations.
c. Combat of enemy naval forces.

The German Air Force Signal Intelligence Service in the East monitored the air traffic of the Russian Naval Air Forces which were in a position to operate against the Germans. Those units monitored included the Black Sea Fleet Air Arm; the Baltic Fleet Air Arm, and the Arctic Fleet Air Arm. The amount of intelligence which the Germans were able to extract from this naval air traffic was due primarily to having solved the call sign encipherment table used by the Russian Naval units. This table was foolishly kept in use for more than a year with the result that it was completely reconstructed by SIS." Not only the air units but also the naval units with which they operated could be identified by their call signs. Messages at the time of the take-off which were transmitted by the Naval Air regiments and reconnaissance patrol reports could be read by the Germans in sufficient time to warn their convoys and submarines. [IF-187, p. 16]

Captain Wedim HEROLD, officer in charge of Ln. Regiment 111/353 of the Signal Intelligence Agency of the Air Force High Command, gives the following information on traffic analysis performed by the Germans on Russian Naval traffic.

"The Navy in the Southern Sector had the Black Sea Fleet of the Soviet Union as its monitoring area. As the Black Sea Fleet's code was unbroken results could only be achieved by traffic and direction-finding evaluation. The navy was especially interested in the monitoring of Black Sea seaplane forces. The planes were monitored and the results passed to the German navy. The forces consisted of bomber, torpedo, fighter, and sea rescue units. Bases and strength were currently known.
'The signal code of the reconnaissance aircraft ft could be read. The guiding of our own fighters by the listening service onto the reconnaissance aircraft on operations often brought us victories. The navy was especially interested in reconnaissance reports about our own ship movements, particularly for positions and courses of our own convoys, as after a report by the reconnaissance aircraft, attacks by aircraft or submarines could usually be reckoned with. The calling up of fighter protection, timely warning and changing of course often foiled the enemy's existing intentions of attack.[I-130, p 15]

14. Advanced Warning Reports and Route-tracking.
Advanced warning reports and route-tracking were often possible from the results of traffic analysis. The German Air Force Signal Intelligence Agency had more success than the German Army Signal Intelligence had against the Russians. One source of information from which the German Air Force Signal Intelligence were able to make use in giving timely warnings to the German Air Force came from the traffic of Russian Specialist Air Force Liaison officers who acted in an intermediary capacity between Army and Air Force for Army cooperation, close support, and tactical reconnaissance. These officers were known as "Flivos" (Fliegerverbindungsoffizier). The Flivos consistently transmitted messages which contained the starting time and course of the Russian Air units to which they were assigned. From the interception of these messages and the exploitation of the information derived therefrom, the German Air Force was able to destroy a large number of Russian planes. Assumptions of impending ground force operations could also be made noting an increase in local attacks or thrusts in the areas in which the Flivos were located. The Germans also had success in locating points of armored concentrations since orders asking for special air support would be transmitted by the Flivos. These requests for support originated at Army and Motorized Corps headquarters and came up on a point-to-point net between the Air Armies and their subordinate corps and independent divisions. As the cryptographic systems in which these messages were sent were being read by the German Signal Intelligence the German High Command was kept informed currently of those targets for which air support was requested. By the time operational instructions had been sent by the Russians to an Air Division by an Air Corps the German troops had ample time to take effective countermeasures. Thus these Flivos messages afforded the Germans an excellent means of making tactical evaluations of immediate value, especially when the reports contained Russian observations of German strong and weak points of defense. The reasons given by the German Signal Intelligence as to the usefulness of this traffic were:

(a) because of the close cooperation between the Russian Air and Ground Forces, a heavy ground attack could be expected whenever strong air support was requested;

(b) the Flivos reported their locations in these reports, thereby revealing the position of Russian Array and Corps headquarters at which the Flivos were located; and

(c) from ground situation reports transmitted by the Flivos several times a day, an accurate picture of the frontal sector of each Russian Army unit could be constructed.[I-17; 1-163, IF-186; IF-187]
The German Air Force Signal Intelligence Agency furthermore claimed that from information obtained from the Flivos traffic the German High Command had full knowledge of the concentration of troops at Stalingrad. This information came when five entire Air Divisions moved into that area. The Germans had learned that whenever traffic revealed Flivos of five Air Divisions were present in any area it could be expected that the Armies of those divisions would appear there in a short time. The Germans furthermore claim they had information from the same source as to the plans of the Russians for the last drive upon Berlin, but were unable to do anything about the matter because of the serious condition in which their Armed Forces found themselves.[I-17]

a. Route-tracking Data Available from Messages.— When the German Signal Intelligence Service intercepted operation orders it was an easy task to track the course flown by Long Range Bomber Force formations. The

only problems remaining were to identify the units participating in the formation, as several corps were quite often used in one raid, and to make necessary corrections if any new time was reported after the take-off of the predicted time of arrival over the targets. The 18 th Air Army traffic of this type served to piece together the intelligence already derived from air-to-ground traffic, which at that stage was usually meaningless. The Russian Air Defense organizations also frequently transmitted notification of impending missions which gave data regarding the course to be flown over Russian territory. These messages, which were directed to the Russian Anti-air-craft Units, contained the number and type] of planes as well as the location of the point of attack.[IF-187, p 44]

b. Weather Reconnaissance.—In instances where the Germans did not intercept operational orders there still existed a possibility for predicting Russian bomber raids from information derived from the Interception of weather reconnaissance reports. These reports were usually carried out in the target area prior to an attack. From an analysis of these messages the Germans could usually predict whether or not a raid was soon to take place, as a raid generally occurred only if the ceiling over the target area was at least 3,000 meters and there was no more than 6 to 10# of cloud cover. Route tracking of the weather reconnaissance planes was aided because of the fact that they transmitted messages every 5 to 10 minutes, sometimes even reporting their position, and thus making direction-finding by the Germans unnecessary.[IF-187, P 45]

c. Flash Reports.—Tactical intelligence resulting from the interception of Russian Long Range Bomber Forces (ADD) traffic was immediately enciphered and forwarded by wire to visual observational posts, to the Air Force, to the so-called "light division" for special missions in the German Army (Jagddivision), to the Anti-air-craft units, and to the Central Reporting Center for Defense of the Reich (Meldekopf). As a result of early warning through these flash reports German defensive preparations against an anticipated Russian night raid often took place during the morning proceeding the raid. As soon as the take-off of a bomber formation was established, a wire line from the Signal Intelligence Service evaluation company to fighter and Anti-air-craft unit headquarters was kept open, and all subsequent information currently reported to the stations. Another direct wire line was maintained to the nearest German Signal Intelligence Service radar intercept station. This station was kept informed of the course and altitude of the Russian bomber formation so that when radio silence was - begun the radar station could take over the route-tracking.[IF-187, p. 47]

15. Intercept of Russian Radar.

Radar intercept on the Russian Eastern Front by the German Signal Intelligence Service brought only insignificent results since the Russians made little use of radar equipment. Very few details of Russian radar equipment are available. On several occasions, however, in traffic intercepted on point-to-point nets some mention of three types of equipments was found. These mentioned "RUS-I", "RUS-2" (Radio Ulavlivatel Samoletov), and "MRO" (Melki Radio Ulavlivatel). Several Russian prisoners of war stated to German interrogators that Intruder regiments of the Long Range Bomber Forces (ADD) used radar against German night fighters. However, the Germans never found any trace of any airborne radar equipment in the Russian planes which crashed or which were shot down. It was concluded by the German Signal Intelligence Service that the Russian prisoners only made the statements because of suggestions made by the interrogators rather than from any knowledge of such equipment because they knew the Germans and the Allies were using radar to a great extent and were only wishing their own forces were doing the same.[IF-187, p. 45] In the summer of 1941 the Germans did establish, from intercepted radio-telephone traffic, that the Russians were experimenting with ground radar to be used in their defense zones. Three or four German radar Intercept teams were placed along the Eastern front and equipped with direction finders. Intelligence obtained from these teams Indicated that the Russians were making very little progress in the field of radar, and that their equipment was inferior to that of the Germans, British, and Americans. In the fall of 1944 the German Signal Intelligence further determined that on the Central Russian front, apart from several small radar sets apparently being used for anti-air-craft control, there was only one large installation which was near Warsaw. Further Interception of Russian radio-telephone traffic later again indicated there were several other radar installations within the air defense zone, but the locations could never be established by German dlrection-finders.[IF-187, p. 45]

16. Russian Radio Counter-measures.

Very little information in reference to Russian use of radio counter-measures is to be found in TICOM materials. The Russians had a term (CYB) which denoted all types of varied camouflaged communications procedures, derived after 1942 by the Signals Officers for use at the front. The Russians apparently did not assume that their CYB-procedures would give 100% security. The procedures remained valid for indefinite

periods, being, changed either on the judgment of the Signals Officer who issued them, or when there was a suspicion of compromise. In general, the CYB-procedures of the Russian Air Forces remained in use longer than those of the Army, 9in.ce the Air Force procedures were employed behind the lines and were less exposed to physical compromise. [I-116, p. 3]

17. German Use of Captured Russian Material.

The German Signal Intelligence Service salvaged a large amount of material from Russian planes which were shot or forced to crash. However, the Germans did not gain much outstanding information from this material because they were already in possession of most of the important facts and information concerning Russian equipment. They were able to gain considerable information from the Standard Operating Instructions salvaged from planes. This included data on Russian codes, call signs, radio frequencies, maps, and grid-square enciphering: systems.[IF-187, p 71]

Chapter 3.
SUMMARY OP GERMAN SUCCESSES IN TRAFFIC ANALYSIS OF RUSSIAN COMMUNICATIONS

1. The Russians depended on the use of One-time Pad cryptographic systems for security of their high level traffic and on code books and enciphering tables for their medium and low level traffic. The One-time Pads were not read by the Germans, but the medium and low level systems were read to a great extent.

2. The main source of information the German Traffic Analysts had came from exploitation of the Russian use of call signs, radio frequencies, message indicator groups, and direction-finding reports.

3. Another source of information came from the intelligence gained from reading pre-arranged message forms. The Russians used these forms extensively for reports. The Germans had little difficulty In reading such traffic.

4. There was very close cooperation between the German Intercept operators and traffic analysts in the field. Integration of available information, such as traffic analysis results, evaluation of data, cryptanalysis, prisoner of war interrogations, captured documents, and other types of intelligence was carried out with excellent efficiency.

5. The Russian call sign systems were not as secure as the Russians believed. Given sufficient call sign, traffic and day-to-day continuity the German Signal Intelligence Service was able to reconstruct the systems.

6. Some of the outstanding successes of German Traffic Analysis were:
a. A knowledge of the Russian Air Force order of battle and of battle situation.
b. A knowledge of the organization and order of battle of some Russian Army units.
c. A knowledge of strength, types, and armament of aircraft,
d. A knowledge of the location and occupation of airfields.
e. A knowledge of the movements and concentrations of Air and Ground Force units.
f. A knowledge of operational intentions.
g. A knowledge of the amount and type of air transport.
h. A knowledge of the Russian supply situation.
i. A knowledge of probable targets.

TAB A [Abbreviations and Vocabulary]

- **ADD (Aviatsiya Dalnego Dyestviya).—Russian Long Range Bomber.**
- **ADR. Russian symbol for "address" appearing in front of the address group in military messages.**
- **Air.—Vozduch (Russian), abbreviated VZD.**
- **Air Army. Russian equivalent to American Air Force, and British Command.**
- **Air Liaison Officer.—German translations Fliegerverbindungsoffizier, (FLIVO).**
- **Antiaircraft Defense.—Protivovosduschnaya oborona (PVO).**
- **Avitsiya Dalnego Dyestviya (ADD).--Russian Long Range Bomber Forces.**
- **Corps (Air Force). 120-450 Russian planes (2 or 3 Divisions), partly equivalent to an American Wing.**
- **CYB. A Russian term denoting all types of varied camouflaged communications procedure.**

- **District Air Base.—Rayon Aviazionnago Bazirovaniya (RAB). Largest unit of the Russian Air Service Command.**
- **Division (Air Force) 60-150 Russian planes, unit classed between an American Group and Wing.**
- **Escadrille. A flight of Russian planes, usually containing 8-10 planes.**
- **Fliefu-Jafu. About 160 German planes (2 Geschwader), equivalent to American Wing.**
- **Flieger-Division. About 320 German planes, classed between an American Wing and Command.**
- **Flieger Korps. About 600-900 German planes (2 or 3 Divisions) partially equivalent to an American Command.**
- **Flivo (Fliegerverbindungsofflzier) .—German for Air Liaison Officer.**
- **Fliegerverbindungsofflzier (Flivo).—German for Air Liaison Officer.**
- **Geschwader. 70-90 German planes (3 Gruppen), equivalent to American Group, and British Wing.**
- **Golovanov, Marshall. Russian commander of the Long Range Bomber Forces.**
- **Grubler, Corp. A member Of Gruppe VI, of the Signal Intelligence Agency of the Army High Command (OKH/Gen d . NA).**
- **Gruppe. 27-30 German planes (3 Staffeln), equivalent to US and British squadron.**
- **Heimann, Corporal William, A member of Kona 1, of the Signal Intelligence Agency of the Army High Command (OKH/Gen. d. NA).**
- **Hempel, Sgt. Werner. A member of Gruppe VI, of the Signal Intelligence Agency of the Army High Command {OKH/Gen. d. Na). He was a Baudot Intercept technician.**
- **Herold, Captain Wadim. Officer in charge of Ln. Regiment Hi/353 of the Signal Intelligence Agency of the Air Force High Command (OKL/LN) in the East.**
- **Heudorf, Corp. A member of Naa 8 (radio intelligence battalion) of the 3rd Panzer Army.**
- **I-17. ''Extracts of SHAEF Interrogation of the following German communications personnel: Maj. Gen. Boner, Col. Grube, Lt. Col. Mettig, Maj. Rottler." A TICOM publication.**
- **I-19. (b) "30 reports written by Kona 1 personnel." (f) "Report on traffic analysis of Russian wireless traffic." A TICOM publication.**
- **I-70. "Paper on the German Sigint Service by Lt. Col. Friedrich." A TICOM publication.**
- **I-75. "Interrogation reports on German field Sigint personnel carried out at Buffer. Lt. August Schroeder, Lt. Starke, Corp. Heudorf, Capt. Holetzko."**
- **I-116. "Report on the interrogation of Lt, Alex Dettmann of OKH '(Gen. d. NA)."**
- **I-130. "Homework of Hauptmann Herold, O.C., Ln. Rgt. III/353. A TICOM publication.**
- **I-163. "Report on interrogation of Hptm. Scheidl, Ltn. Sann, and Ltn. Smolin, all of I/LN. Rgt. 353 (East), on German Sigint activity against Russian Air Forces." A TICOM publication.**
- **I-168. -"Report-by the Karrenberg party on miscellaneous Russian W/T." A TICOM publication.**
- **I-173. "Report by the Karrenberg party on Russian W/T." /k TICOM publication.**
- **IF-187. Vol. XII, Seabourne Report. "Technical Operations in the-East, Luftwaffe SIS."**
- **lF-186. Vol. XI, Seabourne Report. "History of Operations in the East, Luftwaffe SIS."**
- **IPM. Abbreviation for flight over initial point (Russian Air Force).**
- **Jagddivision.—German "light" division.**
- **JU 52. German Junkers, transport plane.**
- **Junkers 52. German transport plane.**
- **Karrenberg, Sgt. Erich. A member of Gruppe VI, Signal Intelligence Agency of the Army High Command (OKH/Gen. d. NA). Worked on Russian Baudot traffic.**
- **Kona (Kommandeur der Nachrichten Aufklaerung) (Commander for Signal Intelligence). A Kona was the Signal Intelligence component in the German Army organization.**
- **"Light" division.—German translation, Jagddivlsion.**
- **Long Range Bomber Force.—Aviatsiya Dalnego Dyestviya, (ADD).**
- **Luftflotte. German equivalent to American Air Force and British Command.**
- **MAB (Morskaya Aviabasa).—Russian words for Naval Air Base Depot) largest unit of the Russian Naval Air Force.**
- **MAP. Call sign formed from the Russian cover name, MAPKA.**
- **MAPKA. Russian cover name.**
- **Meldekopf.—German word for "reporting center".**
- **Melki Radio Ulavlivatel. A type of Russian radar.**
- **Mishka. Russian radio operator's name as given in an example of a Russian radio message.**
- **Morskaya Aviabasa (MAB).--Russian words for "Naval Air Base Depot.' Largest unit in the Russian Naval Air Force.**
- **MRU (Melki Radio Ulavlivatel).—A type of Russian Radar.**

- **Narodni Kommissariat Vnutrinikh Del (NKVD).—Peoples' Commissariat for Internal Affairs.**
- **Naval Air Base Depot.—Morskaya Aviabasa, (MAB). Largest unit in the Russian Naval Air Force.**
- **NKRF.—Peoples' Commissariat for River Shipping.**
- **NKVD (Narodni Kommissariat Vnutrinikh Del).--Peoples' Commissariat for Internal Affairs. A Russian Secret Police organization.**
- **OPM. An abbreviation used by the Russian I Guards Corps before giving bearings on the return flight.**
- **Partisan nets. Radio nets used by the Russian Partisans, a guerilla organization.**
- **Peoples' Commissariat for Internal Affairs.—Narodni Kommissariat Vnutrinikh Del (NKVD). A Russian Secret Police organization.**
- **Peoples' Commissariat for River Shipping.—NKRF**
- **Protivovosduschnaya oborona (PVO).—Antiaircraft Defense (Russian).**
- **PVO, (Protlvovosduschnaya oborona).—Antiaircraft Defense (Russian).**
- **QDM.-Q-signal meaning a request for magnetic course to steer with no wind.**
- **QDR.- Q-signal requesting magnetic bearing in relation to station.**
- **QSA.--Q-signal meaning "What is the strength of my signal (1 to 5)?"**
- **RAB (Rayon Aviazionnogo Basirovaniya) The largest unit of the Russian Air Service Command.**
- **Radio Ulavlivatel Samoletov (RUS).—A type of Russian radar.**
- **Rasch. Lt. Werner. A member of 353rd German Air Force Signal Intelligence Regiment in the East.**
- **Rayon Aviazionnogo Basirovaniya (RAB). District Air Base. Largest unit in the Russian Air Service Command.**
- **Regiment (Russian Air Force). About 30 planes, equivalent to US and British squadron, German Gruppe.**
- **Reporting center.—Meldekopf (German).**
- **RUS (Radio Ulavlivatel Samoletov) .—A type of Russian radar.**
- **Schmitz, Sgt. A member of Gruppe VI, Signal Intelligence Agency of the Army High Command (OKH/Gen. d. NA).**
- **Staffel. A flight of German planes, usually containing 9-12 planes.**
- **Suschowk, Sgt. Dietrich. A member of Gruppe VI, Signal Intelligence Agency of the Army High Command (OKH/Gen. d. NA).**
- **TPR 43.--A Russian Call Sign Book.**
- **TRS.—An abbreviation used by the Russian I Guards Corps before giving bearings on an outward flight.**
- **Uffz. (Unteroffizier).—In general, non-commissioned officer; as a specific title, corporal.**
- **Vozduch (VZD).—Russian word for "air."**
- **VZD (vozduch).—Russian word for "air."**