ODC Liaison 3 August 1951

MEMORANDUM FOR USCIB SECURITY COMMITTEE:

SUBJECT: Information Relevant to Soviet COMINT

1. Attached herewith as inclosure #1 is a copy of a paper prepared some time ago in this office and reproduced at the present time for your information since it has a bearing on the subject stated above.

2. Attached as inclosure #2 is an extract from a Russian Army Operational Order, available only in German translation, which indicates further Russian use of COMINT.

3. Inclosures 1 and 2 relate to the "draft" memo previously submitted to the Chairman of the Security Committee on the general subject of Soviet sophistication in communications intelligence and communications Security as relevant to the proposed change of the BRUSA Appendix "B" to provide for a Category D.

Thomas A. Miller

THOMAS A. MILLER
USAFSS Member,
Security Committee

2 Incls
1. ODCLO# 25-19
2. ODCLO# 25-20



Cy 4 of 20 cys
Pg 1 of 1 pgs

## Russian Knowledge of German Cryptographic Practice (1943)

A German translation of a captured Russian intelligence manual designed "for higher staffs" and dated 1943 indicates that as of that date Russian intelligence held a surprisingly detailed knowledge of German Army signal communications with regard to their organization, equipment, and cryptographic media. The report also states that the German Army Chief Signal Officer supplied German Army Intelligence with a daily report on intercept results.

The brochure, available in German translation as GHDS Document H3/382, becomes of interest as another item indicative of Russian appreciation of the elements of communications security. "TICOM" information, summarized in the GCHQ discussion of "The Russian 'Y' Service" (L 91/G-38) indicated that it was the belief of a British liaison mission to Moscow early in the war that the Russians were "well on the way" to the solution of Enigma traffic if they had not indeed already solved it. The present manual, while not giving any indication of such Russian cryptanalytic activity, does indicate that the Russians were thoroughly familiar with the distribution and use of Enigma cipher machines in the German Army at approximately this date. In addition, the "TICOM" Team which investigated a German factory which had produced Enigma machines discovered that a Russian inspection of the factory had preceded their visit and that the Russian investigators, who were Russian Army officers, significantly showed greater interest in models of the German Naval Enigma than in models of the German Army Enigma which were equally available. (The implication is that as Russian Army "experts" the investigators were already quite

familiar with the German Army machine but the German Navy version, which differed in some features from the German Army model, was new to them).

Evaluation of the statements made in the manual is perhaps subjective and should not be attempted without consideration of the context in which they appear. The difficulties of dealing with a German translation from the Russian must be mentioned, for example, there is no indication of its dissemination other than that to be inferred from the reference in the German translation of the title to "for higher staffs" and there is no indication of the Russian classification. On the basis of this statement, however, it may be assumed that the manual was intended for the use of staff intelligence officers - whether such staffs were at the Front or Army level or may have included Division is unclear.

Making allowance for the linguistic difficulties of an English translation from a German translation from the Russian (where the Russian text discussed German organization) the "tone" of the references to signal communications compare in phraseology and reference to salient points for communications security to other recently available Russian material which has led ASA to comment on apparent Russian "sophistication" in communications intelligence and communications security. This "tone of reference" to German communications may be compared with the language and terminology used in the "Lectures on Cryptographic Security (SUV)" recently translated from Source 267 by CSAW (NI-4-TIC[illegible]). The ASA translation of the 1944 "Manual for the Processing of Radio Intelligence Materials" may also be cited in this connection with particular attention to chapters i and ii of that translation which concern Russian traffic analysis [illegible] communications

Consistent with the limitation of discussion in the "Manual for Processing Radio Intelligence Materials" to the communications of foreign armies the present manual, prepared for Red Army intelligence officers, limits its discussion to the organization of the German Army ("Oberkommando des Heeres" - the German translation of the title uses "Wehrmacht" - "armed forces" - but the subject matter is limited to the German Army"). Examination of the complete manual leaves the impression that the German Army organization was thoroughly familiar to Russian Army intelligence. In the case of German Army Intelligence on the Eastern Front (I-c Ost), for example, the manual gives a breakdown of the various sections showing their numerical designation, their responsibilities, their sources of information, and the intelligence produced. The following translation of selected pages gives the gist of the information contained in the manual.

GYDS, H3/382
Oberkommando des Heeres
Generalstab des Heeres
Abt Fremde Heere Ost (III-C)

"Translation of Russian Captured Document Number 1: Orientation Manual on the German Armed Forces for Higher Staffs", issued by the Chief Intelligence Directorate of the Red Army; Moscow 1943.

Organizations of OKH/GenStab and Fremde Heere Ost, charts and explanation, pp. 27-28.

"The Signal Communications Section (Nachrichten Abteilung, Chef Heeres Nachrichtenwesen) provides the signal communications between command and operational staffs and places at their disposal current enemy intelligence reports as well as a daily report on intercept results (Abhörgebnisse). This section is responsible for the recruiting, training, and assignment of signal troops

and keeps the Waffenamt advised of requirements for the development of technical equipment. The section prepares new cryptographic regulations, administrates the cryptographic service, and controls enciphering and deciphering work". p.30.

The strength and equipment of a Corps signal complement is given in tabular form with the statement that each Corps has 22 Enigma cipher machines. p. 63.

The radio company of an Army's signal troop complement includes 24 Enigma cipher machines. p.65.

A tabular listing of the various types of signal equipment with its specifications used in the German Army is presented on p.77.

Under "Troop Command, Organization of Signal Communications", the following discussion of "Enciphered Command Communications" appears:

"The question of enciphering command communications is given very great importance in the German Army. The army is equipped with cipher machines which are used for radio traffic from division staff upwards. Such a cipher machine has over 1 million possible enciphering combinations.

"In addition to the cipher machines the Germans use a "Hand Cryptographic System". They have a simple troop cipher used by division, regiment, and battalion. In addition there is a difficult ("Schwierigen") cipher with a double encipherment that is used by division and corps, often by Army.

"The Troop cipher, which is prepared in a basic principle, is distributed in thousands of modifications.

"In addition, there are thousands of various signal tables,

covernames, and symbols.

"As a rule for an individual large operation each formation has its own key table, covername listing, radic signal table, etc.

"The Germans use various methods for map encipherment:

1. Use of the standard map grid.

2. Division of a large map square ("Quadrat") into four parts; middle square (traneze), each middle square in four parts - small squares; and each small square in nine parts. Finally each map point on the map is designated by a five digit number.

3. Cover names are provided for the important orientation points.

4. "Stosslinien" method ". p. 107.