

9/16/46
~~SECRET~~

FSRO-357

12 Sept. 1946

TO: The Director
VIA: Acting Chief, FSRO
FROM: Acting Chief, FEL
SUBJECT: Excerpts (relating to cryptanalysis and codes) from the interrogations of General ONODERA, General OMOUCHI and Colonel HIROSE.

1. Attached are the excerpts relating to cryptanalysis and codes made from the above interrogation reports which were recently submitted by Mr. Theodore Rousseau and explanatory memorandum.
2. These excerpts are for transmittal, at your discretion, to ASA.

DESENSITIZED
per DGI 70-17

WASH-OSS-OP-81

CS copy filed in []

NAZI WAR CRIMES DISCLOSURE ACT

- EXEMPTIONS Section 3(b)
(2)(A) Privacy
(2)(B) Methods/Sources
(2)(C) Foreign Relations

Declassified and Approved for Release
by the Central Intelligence Agency
Date: *2005*

ESR0357

~~SECRET~~

COUNTRY: Various

SUBJECT: Excerpts (relating to crypto-analysis and codes) from the Interrogations of General ONODERA, General ONOCHI and Colonel HEROSE

DATE OF INFORMATION: Dates of respective interrogations as given below

EVALUATION: Believed fairly reliable

1. The following excerpts bearing on Japanese and sundry European crypto-analysis, interception and code services during and shortly after the war have been made from the Report of the Interrogation of Major General Makoto ONODERA, Formerly Military Attache at the Japanese Legation in Stockholm, by an SSU interrogator. The interrogation was completed on 20 July 1946 at the Sugamo Prison, Tokyo.

2. The evaluation of ONODERA's information was that it was largely true but far from the entire truth with regard to any subject upon which the prisoner was interrogated.

(1) "..... Two ciphers were assigned to ONODERA's office. One was a general system for communication with Tokyo and all other Japanese military attache posts. The other was ONODERA's personal code which was a one-time pad for use with Tokyo Headquarters only.

"Before the arrival of Col. SATO and SHOUJE all coding was done by Mrs. ONODERA and YOKOI. Later all the assistants, both military and civilian, did their share, each being assigned hours for cipher duty.

"The personal one-time pad cipher was the most frequently used because of ONODERA's fear that the other might have been broken by the Swedes and the Germans, and because at the end of the war, the Stockholm military attache's office inherited the one-time pad system from many of the posts which had been closed down such as Paris-Vichy, Rome and Berlin.

"Sources were indicated in the text of the message either by initials such as K for KRAEMER, MA for MAASING, and P for 'Peter IZAKOV', or fully spelled out as 'Swedish General Staff', 'Finnish Military attache'.

~~SECRET~~

"On two occasions ONODERA was entrusted with foreign codes for communicating with agents. In January, 1945, MAASING (an Estonian working for Axis Intelligence and possibly British) gave him an Estonian code, complete with wave lengths and call signals, for liaison with the Baltic countries. Messages were to be received and sent through KALBUS (now with the STELLA POLARIS group in France) over the A/T set in the Finnish Legation (i.e. in Stockholm).

"When SUBIKOWSKY (a Polish Intelligence officer) left Stockholm in 1944 (i.e. for England), he gave ONODERA a Polish code for communications with Col. GARG in London. ONODERA says this was never used. Both foreign codes were destroyed in August 1945.

(2) "..... The contact with the Finns was the best method for ensuring the protection of his (ONODERA's) codes. The Japanese crypto-analytical station in Budapest also took a part in this, and HAYASHI on one occasion warned the (Japanese) Legation (in Stockholm) that one of its ciphers had been broken by the British. However, Subsequent tests initiated by Minister OKAMOTO tended to contradict his statement.

(3) "..... ONODERA never had a Japanese crypto-analyst working in his office. Although his predecessor MISHIMURA had initiated the work with HALLANAA in Stockholm, it was carried on during the war by HIROSE in Helsinki. After the Finnish surrender, ONODERA purchased some code material from the Finnish refugee group, but his contact was indirect through HALLANAA, PAIS or KALBUS. He also had indirect contact with HAYASHI's office through SAKURAI, but, generally speaking, he did not participate in this aspect of intelligence activity.

(4) "..... Until 1939 the center of the Japanese intelligence activities against Russia was always in the Warsaw military attache's office. An arrangement existed whereby Japanese officers were periodically sent to Poland to study Russian codes with the Polish General Staff crypto-analytical section. ONODERA cites the following Japanese officers who were trained to this agreement:

- according
- "General HYAKUTAKE in the late 1920's
 - "General OKUBO in the late 1920's
 - "Colonel SAKAI (deceased) in the early 1930's
 - "Colonel KUDOO in the early 1930's
 - "Colonel SAKURAI from 1935 to 36
 - "Colonel FUKAI from 1935 to 36

"The origin of the Japanese system of analysis and compilation of material from the press and its successful use for intelligence purposes — which was practiced so extensively during the war — was also learned from the Poles. Col. KOWALEWSKI, an authority on this system who had visited Japan and was later Polish military attache in Portugal, was

their teacher. In exchange for instruction in these matters the Japanese undertook to supply the Poles with Russian code intercepts and other intelligence material obtained from the Far East.

(5) "Wishing to take every advantage of the possibilities of collaboration in 1940, Col. GANO sent a Polish intelligence mission to Japan to collaborate with the Japanese throughout the Far East. The only name which ONODERA remembers in this group is that of Lieutenant SKORA who he thinks was connected with crypto-analysis.

(6) "..... In studying the Russo-Finnish war and in conversations with the Finnish War Minister (in 1938, Col.) NISHIMURA discovered that perhaps the most important cause of the Finnish successes against the Russian armies had been the crypto-analytical services of Col. HALLAMAA. They had succeeded in breaking the codes used in Russian combat communications so rapidly that they would communicate Russian orders to Finnish unit commanders before they reached their destination in the Russian lines. NISHIMURA determined to acquire this valuable weapon for the Japanese services. He consulted with HALLAMAA and worked out an arrangement whereby a specially designated Japanese officer would be assigned to the Finnish crypto-analytical section for the purpose of learning their methods. The Japanese paid for this privilege with money of which the Finns were sorely in need as a result of the war, and with Russian cipher material — five digits — obtained in the Far East and forwarded by Tokyo.

"The appointment to NISHIMURA's office in 1940 of Col. HORIUCHI and a naval officer whose name ONODERA cannot recall, was the immediate result of this agreement. HORIUCHI who had had no previous training in such matter proved unequal to the task and was replaced by Col. Richi HIROSE, a trained specialist, in 1941.

(7) ".....In August of 1944 ONODERA heard from his Finnish friends that peace between their country and Russia was imminent. He immediately made contact with PAASONEN and HALLAMAA through WILLIAMS for the purpose of taking over the Japanese contacts with the Finnish Intelligence Service, which would naturally lapse as a result of the surrender. At the same time he cabled ONOCHI (then Japanese Military Attache in Finland) to make a proposal at his end. After some time the latter answered that although he had made every effort to arrange that both the crypto-analytical and espionage services be passed on, this had proven impossible. ONODERA says that he was unaware that the matter had been taken up personally in Stockholm and did not learn how successfully the collaboration was continued until much later in Japan.

"Meanwhile ONODERA says he undertook to do what he could to protect and help the Finnish services. He says that at that time more than one thousand Finnish intelligence operators — including a special service parachute battalion of 400 men — secretly came over the frontier into Sweden bringing with them their radio equipment and their archives.

SECRET

Page 4.

This undertaking was given the active support of the Swedish Army, and Major PETERSEN was assigned to carry out the details. The Finnish group continued its activities in Sweden setting up a crypto-analytical section near Stockholm and operating three or four monitoring stations in northern Sweden. They were in direct communication with the Finnish resistance movement. ONOERA says that in spite of what was done for them by the Swedes, they were in desperate need of money. They were not even able to apply for help to their traditional friends, the Americans. As a result, he undertook to do what he could to finance them and paid out about between 250,000 and 300,000 Kroner -- his entire funds including War Ministry money which he later had to replace. He had promised more and had received an additional 150,000 Kroner from Tokyo for this special purpose but the war ended before this could be done. He says that although the information which he received at the time was in no way commensurate with the amount expended, he considered it an excellent investment for the future from the Japanese point of view.

ONOERA received intelligence from the Finns in two ways. Through personal contacts and written reports. HALLAMAA and PAASONEN both visited him separately on two occasions. They brought him no particular item of information but came to discuss the progress of the war in general, the situation of the Finnish refugee group in Sweden and the development of their mutual collaboration. When they were both absent from Stockholm, PALE was their representative and carried out their instructions. He was HALLAMAA's most outstanding crypto-analyst and at the same time the guardian and archivist of the files and equipment which the refugee group had brought with them. Col. KOSKONEN also came with reports from Finland three or four times. He had been Finnish military attaché in Moscow and was, with SALOKSEPI, in charge of HALLAMAA's agents behind the Russian lines. At the end of 1945 both he and PALE returned to Finland where they were arrested by the Russians. When ONOERA last discussed this matter with other Finns, they were confident of obtaining their release and did not seem to fear that the secrets of the Finnish Intelligence Service would be compromised. KAIMUS, a Latvian radio engineer and crypto-analyst, considered second only to PALE, who had worked in Berlin before joining the HALLAMAA group, was also in touch with ONOERA and MAASING. For a while he collaborated with the Swedish crypto-analytical section. When ONOERA left Stockholm, he was studying in the engineering school and had broken off all contacts with the Finnish Intelligence Service and the Swedish Intelligence Service.

Written reports were delivered to ONOERA weekly, usually on Mondays, by WILLMAN or by Mrs. MAENINEN, an employee of the Finnish Legation. The information contained in these reports reached Stockholm in three different ways:

1. By radio. The Finns had a W/T set in their location which was in touch with Finland. (ONOERA believes that this was operated with the knowledge and tacit consent of the Swedes). In this case the reports were usually written up by WILLMAN.
- SECRET

SECRET

PALZ, or KORKKONEN in Stockholm.

"b. By the Finnish diplomatic courier.

"c. By clandestine frontier crossers. This method was used mostly in 1945. ONODERA believes that they were secretly assisted by the Swedes, (probably Major PETERSEN), but he knows no further details. He heard that SALOKORPI had returned to Finland by one of their lines during the winter of 1944. AHLIO who operated a smuggler's boat between Finland and Sweden sometimes also acted as a messenger.

"Over a period of about ten months (1944-45) the Finns supplied (ONODERA with) the following information:

"a. Weekly reports covering the situation on the eastern front and Russian troop movements. These were most complete, containing detailed identification of units and positions. However, ONODERA complains that they always came too late to be of any use.

"b. Weekly reports on German troop movements on the Eastern front. These ceased in April 1945.

"c. Three lots of codes. These were handed over in person by PALZ either in book form or microfilm.

Lot No. 1.

Supplied in November 1944, four Russian military codes:

- (i) Five symbol operational code complete with method use.
- (ii) Five symbol MKVD code complete with method.
- (iii) Four symbol tank combat communication code, incomplete, about twenty to twenty-five per-cent broken.
- (iv) Four symbol air force communications code, incomplete as (iii).

Lot No. 2.

Supplied in January or February 1945, one four symbol Russian military code, incomplete, about twenty-five per-cent broken.

Lot No. 3.

Supplied in March 1945. A group of seven codes of

SECRET

different European countries on undeveloped microfilm. CRODERA has supplied the list which follows below as the best he can remember.

NOTE: It ~~is~~ evidently corresponds with the list, known to be exact, obtained from the Stockholm German teleprinter intercepts -- #30165, 29 May, 1945. He denies ever having had a United States code and persists in his denial even when confronted with the contents of PANDOR telegram #392 of 4 March in 1945 to Berlin, in which he is quoted as having offered ~~one~~ to the Germans. He says that he repeatedly requested United States code material from the Finns, but received the answer that the Japanese already had the best available in Tokyo. (His contention is somewhat strengthened by the fact that no United States code is listed in the second more specific PANDOR telegram #427 of 15/17 March 1945.) He says that these codes were offered to the Germans because he had no facilities for developing such a large quantity of microfilm in Stockholm. However, the Germans delayed too long in giving him their answer and so the films were finally sent back by PALE to Finland -- occupied by the Russians at the time -- and secretly developed there. The results were sent to Tokyo in July 1945.

List of codes:

- i Turkish military attache code, complete with method. CRODERA remembers the name as "GAKAI". Tokyo Headquarters were very pleased to receive this and complimented him officially. Included with it were three or four other Turkish codes, all incomplete, the names of which he cannot remember.
 - ii Two French (Vichy) diplomatic codes, incomplete.
 - iii Two Roumanian diplomatic (?) codes, incomplete.
 - iv One Vatican code, incomplete.
 - v One Yugoslav code, incomplete.
 - vi One Portuguese code, incomplete.
 - vii British government code, 1934, complete.
- "d. Information concerning the activities of the Finnish Resistance Movement. This amounted to about forty battalions under the secret orders of the Finnish Chief of Staff. Assault units were organized throughout the country. HALLAMAA and PAASCHEN directed the intelligence service which was organized on an elaborate scale with planes for liaison. CRODERA does not know that MELANDER was connected with the Finnish

Resistance Movement. He doubts it because MELANDER was pro-German and at that time the Finns had turned against their former Allies because of incidents such as the organization of sabotage against the Finnish army by CELLARTUS.

"In addition to what is listed above ONODERA says HALLAMAA promised him much more of the information contained in the (STELLA POLARIS) archives which had been brought to Sweden. However, none of these promises was fulfilled probably because the Swedes who were afraid that they might fall into the hands of some of the belligerents, kept to close a watch over them. ONODERA denies that he ever received from the Finns any results of intercepted radio dispatches of Allied or neutral diplomatic missions nor any operational intelligence concerning the western Allies. In addition to the payment which has been described, ONODERA gave the Finns information obtained from his other sources, in particular, operational reports on the Eastern Front compiled by the SS and forwarded to him by General KCHATSU.

"ONODERA has great admiration for the Finnish Intelligence Service which he believes to be the most successful organization of its kind operating against Russia. Its activity can be divided into two parts. The first, strictly the creation of HALLAMAA, is the monitoring and cryptanalytical section the center of which was formerly at SOLDAVALA near Lake LADOGA. When ONODERA left Sweden it was divided as follows:

- "a. A group of twenty operatives including HALLAMAA and PAASONEN who went to France at the end of 1945.
- "b. A smaller group made up of both Finns and Estonians who were transferred into the Swedish monitoring and cryptanalytical section. (ONODERA remembers the most outstanding of these as having a Polish sounding name).
- "c. The underground organization in Finland. This is composed of a crypto-analytical section, and a training center. It functions in connection with MAASING's organization in Sweden.

"The second is the subversive activities section, at the head of which was Capt. SALLIKORPI, a former consul in Leningrad who speaks fluent Russian. Col. KCEKKONEN was also connected with it. During the war recruiting, training, and dispatching of agents was handled by Major KRISTIAN. At that time the section had two organizations, one on the frontier near Lake Ladoga, the other inside Russia near Moscow. Its agents were equipped with W/T and communicated with SOLDAVALA. After the Finnish surrender the official organization was abolished. However, the peace terms were described by HALLAMAA and PAASONEN as 'not affecting their work', and

After a short period of confusion the old organization was revived as part of the Resistance Movement, with a training center for espionage and sabotage, and agents operating in Finland and Russia. ONODERA believes that their communications with Sweden are handled in part by MAASING's organization.

(3) "At the beginning of 1945 the Swedish crypto-analytical section succeeded in breaking ONODERA's general code. He was informed of this by PALL who repeatedly advised him only to use his one-time pad when sending information obtained from the Finns. The Swedish radio detection service was very active at the beginning of 1944. They discovered and closed down clandestine W/T posts operating in Hungarian and Roumanian Legations. ONODERA believes that the Finnish Legation set operated throughout the war with Swedish consent.

(9) ".....ONODERA says that he had never heard of official collaboration between the Hungarian and Japanese General Staffs on a basis similar to that which has been described in the case of Poland, Estonia, and Finland. Limited cooperation did exist between Col. SAKURAI, who directed a small crypto-analytical section, Col. HAYASHI in the military attache's office, and a group of Hungarian civilian and military code experts....."

4. The following excerpts bearing on Japanese and sundry European crypto-analysis, interception and code services during and shortly after the war have been made from the Report of the Interrogation of Major General HIROSE ONOUCHI, formerly Military Attache at the Japanese Legation in Helsinki, Finland, by a GBU interrogator. The interrogation was completed on 20 July 1946, at Sugamo Prison, Tokyo.

5. The evaluation of ONOUCHI's information was that it was largely true.

(1) ".....Collaboration on crypto-analysis with the Finnish General Staff was (on) a highly secret order received from the Central Special Intelligence Bureau of the Imperial General Staff, and coincided with the arrival of Lt. Colonel HIROSE Eiichi. The Minister himself was not advised of the nature of HIROSE's mission, and all subsequent details were handled only by HIROSE.

ONOUCHI says that he received no special directives from Tokyo Headquarters because he had only one code, the additive of which was considered weak. Special orders were therefore sent more frequently to offices such as Berlin, Rome, and Stockholm which had numerous codes and were considered more secure.

(2) ".....The work was carried out on an exchange basis. The Finns gave the Japanese instruction in crypto-analysis and access to all types of intelligence on Russia, and the Japanese gave money (through payments made to the Finnish military attache in Tokyo) and Russian intelligence and intercept material (5 depot) obtained in Asia. ONOUCHI says

that this part of their contribution was small.

"In 1939 and 1940 as a result of the threat to highly secret activities in Finland the centre of espionage and sabotage collaboration between Finns and Japanese was moved to NISHIMURA's office in Stockholm. At the end of the Russo-Finnish war it was again moved back to Helsinki. At this time the Poles were also collaborating with the Finns and the Japanese, and it was in this connection that IRANOW (alias RUBIKOWSKI) went to Riga.

(3) ".....Collaboration in these matters began with negotiations between NISHIMURA and HALLAMAA in Stockholm in July 1940. As a result of these Major HORIUCHI was assigned to HALLAMAA's office. He arrived in Finland in the Autumn of 1940 and began work with the Finnish Crypto-analysis section. At that time ONOUCHI had no connection with the work at all. HORIUCHI was recalled to Tokyo in the spring of 1941. He was succeeded by Lt. Colonel HIROSE Eiichi who arrived in Helsinki 22 June 1941. ONOUCHI says that he had HIROSE appointed to diplomatic status as an assistant military attache to facilitate his movements. He received his orders direct from the Central Intelligence Section in Tokyo and worked almost exclusively on matters related to crypto-analysis until 1944.

"...Of the people connected with this work ONOUCHI came into contact with HALLAMAA, the chief of the section, and PASKO, the director of the station at Soldavala. He also knew PALS, one of the most outstanding crypto-analysts, BOGOWABLENSKI and VIGNMAA, both of whom were HALLAMAA's assistants. Lt. Col. LAUTKARI, an electrical engineer attached to the section, frequently visited the Japanese military attache's office early in 1941 in connection with the purchase of a N/T set which was sent to Japan.

(4) "ONOUCHI's first contact with the Poles was when he was stationed with the Special Agency in Harbin. There the Poles had a crypto-analysis and document study center under the Consul KWATKOWSKI. He was assisted by one or two Polish officers who had been sent from Warsaw and who worked under cover as civilian members of the Consulate staff. One of these was a document analysis specialist whose name ONOUCHI remembers as resembling 'RIPUTSKI'. He says that this was almost surely a cover name. (NOTE: It is quite possible that this may have been ECHALESKI who is reported to have been in the Far East at about this time.)

"ONOUCHI remembers the name PANLOWICZ in connection with this group. General YAMAMOTO and Col. SUZUKI cooperated with them and they trained Japanese officers who were specially sent from Tokyo. ISHIZUKI Sakne and NEMURA Saburo were among the latter.

(5) ".....OHOUCHI says that there was close collaboration between the Hungarians and the Japanese in Budapest. The Hungarian General Staff gave official permission for a Japanese military radio station to be set up in the Japanese Military Attache's office, and Hungarians were assigned to the crypto-analysis office which Colonel SAKURAI directed there.

(6) ".....OHOUCHI has submitted the following list of names, chosen from among those of friends and colleagues whom he considers best qualified of Russian intelligence, and whom he believes to be absolutely reliable. (They include the following):.....

".....
"Crypto-analysis and codes experts:

"HAYASHI Tabei (expert on Chinese codes).
"HIROSE Eiichi
"SAKURAI, Shinta
"OSUO, Shunjiro."

5. The following excerpts bearing on Japanese and sundry European crypto-analysis, interception and code services during and shortly after the war have been made from the Report of the Interrogation of Colonel Eiichi HIROSE, former Assistant Military Attache in the Japanese Legation in Helsinki, Finland, by a SSU interrogator. The interrogation was completed on 20 July 1945 at Sugamo Prison, Tokyo.

6. The evaluation of HIROSE's information was that it was largely true but not the entire truth with regard to the subjects about which the prisoner was questioned.

(1) ".....The purpose of HIROSE's mission to Finland was to cooperate with the crypto-analysis section of the Finnish General Staff. It was considered as highly secret and personal. Not even the Japanese Minister to Finland was aware that he was anything more than an Assistant Military Attache. For administrative purposes he was attached to the Japanese War Ministry, but his directives were communicated to him in person from the Central Special Intelligence Section. Except for questions of office routine, he was entirely independent of Col. OHOUCHI, the Military Attache.

"In July 1943 as assistant was unexpectedly assigned to him from BUDAPEST. This was HAGATA Kozamson, a civilian graduate of the Foreign Office Language School who had been working under Col. SAKURAI. He was trained in the Russian language but did not speak it. HIROSE says that he was not able to be of much assistance in crypto-analysis because of inexperience resulting from his long period of inactivity in Budapest.

(2) ".....Immediately after his arrival in Finland, HIROSE was taken to Grankura, a naval monitoring and crypto-analysis station located about 40 kilometers west of Helsinki. It was commanded by Captain POKARINEN with a staff of about 100. This station concentrated on interception and deciphering of Russian messages in the Baltic area, in particular those emanating from the principal Russian naval base.

"At the beginning of July, HIROSE was taken to the Finnish General Staff Headquarters at Mikkeli. There he met Col. HALLAMAA who took him on to the Army Crypto-Analysis centre at Savonlinna. He was put into contact with the Finnish officers who were to direct and assist him in his study of Russian codes. They were:

"Lieutenant (later Captain) PALI, the best of the Finnish crypto-analysts, who worked on the codes of all nations. Unfortunately he spoke no Russian.

"Captain PARKO, crypto-analyst.

"SOGOWABLENSKI, a white Russian who had taken Finnish nationality.

HIROSE is not sure who was in command of the centre which came under the authority of HALLAMAA in Mikkeli. The staff was similar in size to that of Grankura.

"In December 1941 the Grankura and the Savonlinna stations were amalgamated as to personnel and equipment and transferred to Soldavala on the shore of Lake Ladoga. Captain PARKO was put in command of the new centre and PALI was the chief of the crypto-analysis services. POKARINEN was in charge of a communications section. HIROSE says that the total staff was about 500 men, including 200 signal operators. This included a number of Russian refugees whose knowledge of the language HIROSE says was a great help to the Finns.

"The intercept material used in these stations was obtained by the Finns from their own monitoring facilities, from the Germans, and from mobile units attached to Soldavala and operating throughout north eastern Finland. From time to time Tokyo sent HIROSE material obtained in the Far East.

"HIROSE states that to his knowledge the Finns used no machines to facilitate their crypto-analytic work and that all the processes involved were done by hand. He believes that they did buy a few

Page 12.

of the Swedish code machines, but he never saw them in use in this connection. He himself purchased one in 1942 and sent it to Berlin for forwarding to Tokyo by sub-marine.

HIROSE says that there was a total of four mobile units working out of Soldavala. They operated close to the Russian frontier and sent back results obtained to their headquarters by means of V/T sets fitted with a secret apparatus which is inserted between the ordinary transmitter and the power line. This apparatus changes the form of out-going waves (Morse Code) and a similar attachment in the receiving station transports the waves again into their regular form. The organization of each unit was as follows:

- "Total strength 40 men.
- "One automobile for officers.
- "4 busses, all equipped with living quarters
 - one for crypto-analysis
 - two for monitoring
 - one for direction finders and liaison.
- "2 trucks for supplies, etc.

HIROSE knows no further details nor did he meet the commanders of any of these units. He says they were considered most effective in obtaining intercept material. He explains his own ignorance by saying that the Japanese were not interested in such units, which were not used in Manchuria at the time.

During this period HIROSE spent his time working in Soldavala for short periods after which he returned to Helsinki and wrote reports for the Tokyo Headquarters. He had no other duties in the Military Attache's office.

At the beginning of 1944, this close cooperation with the Finns was broken off, and HIROSE was no longer authorized to go to Soldavala. He was told that this was the result of an order by HANNEKHEIM which applied to all foreigners. He is not sure of the reason for it, but he believes it may have been because the Japanese were not supplying sufficient material to the Finns. The development of the war at that stage may also have been a contributing cause since contacts between the Finns and the Russians for a separate peace had already begun.

After the break collaboration was continued through written communications. HIROSE received technical intercept material from the KWANTUNG Army by dispatch through the Military Attache's office in Berlin. He translated this into Russian and forwarded it to HALLAMAA about once a month. The Finnish replies and answers to problems were prepared by PAIS and signed by HALLAMAA.

SECRET

"HEROSE and the Firms concentrated on Russian military operational and NKVD codes. As regards the former, they were successful in breaking infantry, tank, and Air Force combat communication ciphers. They failed to break the Navy "red" five digit code because its call signs and keys were changed daily from the very beginning of the war -- a system which was later adopted by the Army.

"The NKVD four numeral codes presented no difficulties. They varied according to the regional divisions of the USSR with special types for Moscow, Leningrad, and the eastern Siberia, and the NKVD frontier guards. The individual codes differed through changes in the additive tables. The best results obtained with these came from material intercepted by the Japanese between Kachatka and Vladivostock.

"HEROSE describes the development of Finnish crypto-analysis during the war as follows: He says that at the beginning of the invasion of Russia by the Germans in June 1941, various weak points in the Russian Army codes were exposed by the German surprise attack. The Firms easily deciphered the Russian codes and when they entered the war in July they had already accumulated considerable information on the disposition and strength of the Russian armed forces which faced them. The vital five digit code used by the Russians in the summer of 1941 was easily deciphered due to the systematic arrangement of digits and the use of a set additive table.

"At the end of 1941 the front was temporarily stabilized and the Russians tried to correct the weaknesses in their cryptographic systems. During the intervening period prior to the distribution of the new cipher, they tried to strengthen it by using a double additive on each message. They began at that time a system of revising their codes at two to six month intervals. They also controlled the use of additive tables, dividing them into three categories, one-time pads, rotating, and general, thus making it difficult to decipher messages unless a large number were accumulated. They used a two to four digit code of increasing complexity, often changing both the key and the cipher.

"In 1942 in spite of these difficulties the Finnish crypto-analysts managed to keep up with the changes in the Russian codes. The major portion of the messages which they deciphered were related to the German sector of the front rather than their own. This was due to the fact that operations on the latter had almost ceased, whereas the former continued to be very active. The following conditions are described by HEROSE as being responsible for the Finnish success:

SECRET

- a. Intercepted material from the German front.
- b. Simultaneous use of old and new ciphers during a period when ciphers were being changed.
- c. Mistakes of enciphering (fixed habits and non-adherence to regulations).
- d. Special characteristics of long messages.
- e. Special characteristics of short messages.

"During the spring of 1943 the volume of Russian traffic greatly decreased, and there was an over-all intensification of precautionary measures as a result of which it became impossible to decipher operational messages. The only success encountered was with four digit codes. In 1944 difficulties increased. The Russians employed even stricter security measures, instituted a large number of communication regulations and greatly restricted the use of N/T so that the Finns found it no longer possible to break their cyphers by intercepting operational traffic.

"The other departments of HALLAMAA's service worked on codes other than Russian. HERGSE knows that they were successful in breaking United States, British and Danish diplomatic codes. On instructions from Tokyo he had frequently asked for results obtained with the former. These had been refused until the autumn of 1943 just before the time when he was no longer authorized to go to Soldavala. Then he was given a diplomatic strip-type cipher which he describes as consisting of fifteen horizontal lines of thirty letters each and designated, he believes, as "A-1". He says that the American system was broken due to mistakes in enciphering made in the Vichy Embassy during 1941. The same code was found to be in use by the American missions in Berne and Chungking. The last messages which he saw were dated December 1942. He adds that the Finns were sometimes helped in their attempts to break new American ciphers by the fact that the new system was used for communications between European stations, while the same messages were sent in the old system between London, and Washington.

(3) ".....Before HINOKI left Japan in 1941 the Central Special Intelligence Section of the Japanese General Staff had planned to set up a central crypto-analysis station in Berlin where material would be studied and exchanged with Germany and her allies. Two civilian experts, TAKAHASHI, who had been with the Kwantung Army, and SEKIBOTO, were preparing to organize this but they were prevented from leaving by the outbreak of the Russo-German war. As a result of this matters relating to crypto-analysis and monitoring were handled in Berlin by Col. NISHI, who was occasionally assisted by SAKURAI from Budapest.

The only organized Japanese crypto-analysis section was located in the office of the Military Attache in Budapest. This was directed by Col. SAKURAI Nobuta who was assisted by Hungarian officers assigned by the General Staff. The material which they studied was obtained from the Hungarians and perhaps -- HIROSE is not sure -- from the Germans. When KUPOSS visited Budapest in 1943 SAKURAI complained to him that he was greatly handicapped because he received no material from Tokyo, and so HIROSE arranged to send him copies of what he got in Helsinki. He says that SAKURAI's group obtained almost no results with Russian codes and sent a negligible number of reports to Tokyo. The Hungarian crypto-analysts were considered poor by the Finns and SAKURAI never obtained complete cooperation from them.

"The staff of SAKURAI's section was composed of the following:

- HAGATA - Kozsamon, civilian, he was transferred to Helsinki in July 1943.
- INABA - Civilian attached to the Army General Staff. Radio technician.
- YOSHIKAWA - Civilian, formerly attached to the German Section of Department II of the General Staff. In charge of financial and administrative matters.
- Col. HIRIUCHI - Had been attached to the office in 1940 after leaving his post as Military Attache in Holland. However, he was not a trained crypto-analyst and disagreed on matters of policy with SAKURAI so that he was transferred to Stockholm.

"At the end of the war as the Russians threatened to occupy Hungary it was planned to set up a crypto-analysis office in the Japanese Legation in Bern. SAKURAI was accredited as assistant Military Attache to Switzerland, but the course of events prevented the plan from being fulfilled.

"HIROSE denies that there were any other Japanese crypto-analysis offices in Europe. He has never heard of one being connected with the Encharast mission, and adds that to the best of his knowledge neither the Navy nor the Foreign Office maintained similar services.

"After returning to Japan, HIROSE's only contact with the European aspect of his specialty was as follows. In 1945 ONODERA informed the General Staff that the Finns had obtained a Russian five digit code book (whether by capture or crypto-analysis, HIROSE does not know). The matter was turned over to HIROSE, who instructed ONODERA that SAKURAI should go to Stockholm to receive the book and wire the useful portions to Tokyo from Berlin. SAKURAI did so, and the messages were transmitted to HIROSE who passed them on to the Central Special Intelligence Section. However, the war ended before all the material obtained from the Finns could be forwarded to Tokyo.

Page 15.

*.....HIROSE has been cooperative under interrogation. He has completed and confirmed the evidence given by ONODERA and completed and confirmed evidence given by ONOUCHI concerning Finnish cryptanalytic activity. However, he certainly has considerably more technical knowledge and it is recommended that he be interrogated by a qualified expert.