

~~SECRET~~

REF ID: A4P48603

Tactical Index

B-751

EVIDENCE OF AXIS (AND POSSIBLY RUSSIAN) CRYPTANALYTIC ACTIVITY

Search has been made of all Code Instruction messages on file (German, Japanese, miscellaneous), and of SSA Bulletin and "D" messages insofar as these have been indexed (since January, 1943). Material found has been arranged by names of governments conducting the cryptanalytic studies, with sub-headings for countries on whose messages they are working.

GERMANY.

- Miscellaneous. 1. Portuguese Minister in Bucharest says Germans are rumored to have told Rumanian Government they are aware of certain of its intentions because they can decipher telegrams of diplomatic missions in Bucharest, containing this information. He doubts veracity of report but believes it wise to change Portuguese code anyway.

(SSA 99035 Bucharest-Lisbon 4.16.43)

2. Advisable that Col. TAHEI HAYASHI, Japanese Military Attache to Hungary, be detailed for cooperation between Germany and Japan in work of breaking foreign cipher.

(CI 984(SSA 68836) Berlin-Tokyo 12.23.42)

(CI 1026(SSA 74117) Berlin-Tokyo 12.23.42)

Japan.

1. From OSHIMA. Specialist attached to Military Attache's office has discovered Germans are reading some Japanese codes. This is evidenced by German admonishing of Japanese about lack of security, handling of important reports, etc. Codes being read are probably commercial or abbreviation codes.

(CI 516(SSA 35172) Berlin-Tokyo 5.7.42)

2. Re precautions for paraphrasing Japanese wires to offices in Germany and Italy so as not to give those countries clues to Japanese codes.

(CI 116(SSA 16312) Berlin-Tokyo 4.14.41)

~~SECRET~~

GERMANY. (Continued)Russia.

1. Secret military (5-digit) code captured by Germans from the Russians.

(CI 863(SSA 64596) Berlin-Tokyo 6.15.42)
(D 3324 Berlin-Tokyo 12.19.42)

2. From Budapest (possibly from HAYASHI), re sending Russian code to Japan. Wants instructions as to whether to continue cooperating with Germans on Russian codes.

(D 1286 Budapest-Tokyo 2.12.43)

3. Reported arrest by Bulgarian police of Bulgarian national in Sofia acting as Russian secret agent, who confessed to having code book and operating Russian espionage agency unconnected with Communist Party. Code used was letter conversion with key, and reading of it showed agency covered reports on political, military, economic and social questions, and had accurate report of mobilization strength of Bulgarian Army in 1943. Reading of code carried on jointly by Bulgarian police and German Army Secret Intelligence.

(D 2834 Bucharest-Tokyo 7.10.43)

United States.

1. Germans reading reports of American Legation in Sweden.

(SSA 66097 Helsinki-Tokyo 2.10.43)

2. Germany wants code messages sent by U.S. Military Attaches in Cairo and Kuibyshev to Washington to ascertain condition of British and American armies. Request aid of Japanese in intercepting same.

(CI 863(SSA 64596) Berlin-Tokyo 6.15.42)

3. To chief of Japanese Central Special Bureau. Have sent by trustworthy means three packages of American telegraphic reports. These have been sent to chief of General Affairs Department from Berlin,

GERMANY. (Continued)

United States.
(Continued)

and should be burned if anything unusual occurs. (This may imply Germans have had access to these messages, especially in view of No. 2 above.)

(D 3585 Helsinki-Tokyo 9.24.43)

JAPAN.

Miscellaneous.

- 1. Advisable that Col. TAHEI HAYASHI, after taking up his duties as Military Attache to Hungary, be detailed for cooperation between Japan and Germany in work of breaking foreign cipher.

(CI 984(SSA 68836) Berlin-Tokyo 12.23.42)
(CI 1026 (SSA 74117) Berlin-Tokyo 12.23.42)

- 2. Japan has broken Turkish ciphers and those of other small countries. These systems also described as "easy codes."

(D 1266 Helsinki-Tokyo 6.17.43)
(D 1084 Helsinki-Tokyo 6.17.43)

Chile.

- 1. From TANI to Ambassador YAMAGATA (Japanese Minister to Chile, then in Buenos Aires). Wish to make study of Chilean codes. Get in touch with person who supplies your "reliable reports" with view to obtaining code book, or part at least, or methods of revision (composition?), original code text of "reliable reports," official announcements, etc. Contact our ambassador in Argentina and reply through his office.

(SSA 49883 Tokyo-Buenos Aires 9.23.42.)

See that above telegram reaches YAMAGATA. As KOSEKI has already left, send some other suitable official to Chile.

(CI 615(SSA 49882) Tokyo-Buenos Aires 9.23.42)

JAPAN. (Continued)Finland.

1. Since February 1st of this year the code group "CH777" in opening part of Finnish defense unit messages has not been used on Finnish front.

(CI 1111 Helsinki-Tokyo 4.5.43)

2. Will send soon the Finnish place name code 490 via Berlin.

(D 3585 Helsinki-Tokyo 9.24.43)

France(Vichy).

1. Japanese precautions against letting the French authorities know that Japan can read French ciphers.

(CI 950(SSA 66627) Tokyo-Vichy 2.17.43)

Germany.

1. From Col. HAYASHI. I have been asked to investigate use of cipher machines by (?German?) War Department and Swedish War Department. As I have no facilities, for secret investigation, have been able to find out only a little. (Discussion of machines.) At present no countries are making much progress in (?solving?) cipher machines.

(CI 795 Berlin-Tokyo 1.29.42)

Great Britain.

1. As English and American diplomatic codes are difficult to read, advisable to work on easy codes such as those of Turkey and other small countries to gain intelligence on the Allies.

(D 1266 Helsinki-Tokyo 6.17.43)

(D 1084 Helsinki-Tokyo 6.17.43)

2. Great deal of British code material coming in now which we cannot read, so please investigate.

(CI 285 (SSA 25214) Tokyo-Peking 11.22.41)

JAPAN. (Continued)

Great Britain. 3. (Continued)

Clues have been obtained here re tele-graphic codes used at present by British Embassy for communication between Shang-hai, Chungking, Hongkong and London. Possibly they have already been decoded by the Northern Army.

(CI 284 Peking-Tsingtao 11.21.41)

- 4. (Following may refer to cryptanalysis.) Major WAGII, Hungarian Attache resident in Sweden, who has handled Axis intelli-gence in very masterful way, has been re-called to Hungary. We have depended on him heavily in prosecution of objectives against U.S. and Britain, and want him to continue here. Inform Hungarian General Staff.

(D 3557 Stockholm-Budapest 11.4.43)

LIBERIA
Portugal.

U.S. STATE DEPT CABLE STATES THEIR CODES COMPROMISED.

- 1. Japanese Foreign Office intercepting Portuguese messages with view to solving their codes.

(SSA 95191 Lisbon-Tokyo 8.26.43)

Russia.

- 1. Beginning May 21st instructions will be given through Major HORIUCHI re results of Finland's work on Russian Army's new 5-digit code. Finland has done no work on Russia's diplomatic code. Therefore, if you have any materials on it, send them by Capt. HIROSE.

(D 2225 Helsinki-Tokyo 5.17.41)

- 2. To Col. HAYASHI and Lt. Col. SAKURAI. The new 5-digit code sent in your previous wire being studied with key. Send indica-tors.

(CI 1003 Tokyo-Circular 12.24.41)

Code indicator sent.

(CI 1004 WER-? 12.31.41)

JAPAN. (Continued)

Russia.
(Continued)

3. Russian Army Code becoming increasingly difficult to break down.

(CI 985(SSA 68509) Helsinki-Tokyo 7.7.42)
4. We are sending you Russian Code 024B, addressed to head of General Affairs Section, from Military Attache in Hungary.

(CI 715 RVZ-? 11.18.42)
5. Japanese in Berlin have received the 5-digit code which the German Army captured from the Russians. Plan to send copy to Agent SAKURAI.

(CI 863(SSA 64596) Berlin-Tokyo 6.15.42)

Have read secret ~~secret~~ Russian military code book captured by Germans.

(D 3324 Berlin-Tokyo 12.19.42)
6. To Col. HAYASHI and Major HIROSE. We have begun study of Russian diplomatic and commercial codes and have obtained results. Let us know how you are getting on. Messages mostly from Moscow and Foreign Office in Kuibyshev, also from embassies and consulates in Japan and Manchukuo.

(CI 896 Tokyo-Berlin & Helsinki 10.6.42)
7. Re Russian Army Code--Finland judges system same as described in your wire, and has stopped studying it. Since Japan has had success deciphering those messages, desire reference collection be sent over here.

(CI 821(SSA 64597--corrected trans.) Helsinki-Tokyo 10.19.42)
(CI 900(SSA 64597) Helsinki-Tokyo 10.19.42)
8. We cannot decide whether a letter or machine code is being used between Russian High Command and armies in the field. Refer secretly to SAKURAI.

(CI 849 Berlin-Tokyo 10.21.42)

JAPAN. (Continued)Russia.
(Continued)

9. From HIROSE. Results of Russian Army Code investigation. Finns have recovered approximately 1000 words. British are reported directing Russian codes.
- (CI 882(SSA 64147) Helsinki-Circular 1.11.43)
- Answer to above. To Major HIROSE. Japan reading about 4000 values.
- (CI 883 Tokyo-Circular 1.17.43)
10. Suggest conferring of Japanese decoration on Major YRJO PALKO, Headquarters Chief of the Scientific Intelligence (or Chemical Espionage) Bureau of the Finnish Army, in charge of decrypting Russian Army codes. Since 1940 he has furnished Japan with much material on these codes from the Finnish War Department, and has contributed to reading of 5-digit and 4-digit Army and Navy codes. Has always accompanied Major HIROSE on visits to the front line and assisted him in scientific espionage.
- (D 2381 Helsinki-Tokyo 12.20.42)
(D 2729 Helsinki-Tokyo 5.26.42)
(SSA 73410 Helsinki-Tokyo 12.1.42)
11. Re sending Russian Code 054A to Japan. (Message possibly from HAYASHI, Military Attache in Budapest.) Am studying movements of Agent SAKURAI. Want instructions on whether to continue cooperation with Germans on Russian codes.
- (D 1286 Budapest-Tokyo 2.12.43)
12. We have begun to read Russian Foreign Diplomatic Code used for communication with Moscow and Vladivostok by consuls in Seoul and Dairen. Report study of 1-letter and 2-digit mixed codes. Secret intelligence reports on conditions in Japan constitute bulk of traffic.
- (D 1835, Tokyo-Circular 4.6.43)

JAPAN. (Continued)

Russian.
(Continued)

13. (Incomplete message, apparently account of Japanese intelligence office in Helsinki--begins with discussion of Col. HAYASHI's interest in chemical secret intelligence and procurement of local dye-stuffs.) --Missing--2 persons connected with transmission materials. 3 persons connected with U.S. matters, 1 with Turkish. Chief of Central Division of Russian Affairs. Head of decoding work, 3 persons working on Red Army 5-digit code; 2 persons working on Guards Code, 4-digit and 3-digit codes; 4 persons connected with Navy Code; 2 persons working on intelligence code.

(D 2730 Helsinki-Tokyo 7.12.43)

14. Want to have HIROSE and HAKATA make official trip to front-line cryptanalytic offices, therefore send appropriate report on Russian code situation.

(D 2883 Helsinki-Tokyo 8.26.43)

15. To Chief of Central Special Bureau. Although Finnish authorities have succeeded in reading several messages of the 4-digit Naval Code, this work has been discontinued for the present so we have nothing to report.

(D 3585 Helsinki-Tokyo 9.24.43)

16. HA Intelligence. Re investigation of Turkish telegrams (presumably Russian messages), according to Secretary USHIBA who is passing through here at present, as result of check on materials being intercepted and read by Finnish Army, it seems reliable that they coincide in the main with what is being done by our Military Attache's office in Helsinki.

*(CI 1327(SSA 103470) Ankara-Tokyo 11.25.43)

JAPAN. (Continued)

Russia.
(Continued)

Additional messages mentioning Russian army, navy and civil codes are:

- 17. D 3161 Tokyo-Bucharest 7.15.43.
- 18. D 2905 Bucharest-Tokyo 8.2.43, 8.5.43.
- 19. D 2036 Hsinking-Helsinki 3.8.43.
- 20. D 2744 RVZ-? 1.23.42.
- 21. CI 1098 Tokyo-Helsinki 5.20.43.

SPAIN -

Sweden.

- 1. See above under Germany, p.4. Col. HAYASHI has been asked to investigate use of cipher machines by Swedish War Department. He will send a Swedish machine to Japan.

(CI 795 Berlin-Tokyo 1.29.42)

2. *see special folder "FOREIGN CRYPTANALYSIS"*

Turkey.

- 1. Japan has broken Turkish ciphers and her "easy codes." These very valuable for intelligence on Allies which is difficult to obtain from British and American diplomatic codes.

(D 1266 Helsinki-Tokyo 6.17.43)

(D 1084 Helsinki-Tokyo 6.17.43)

- 2. Incomplete message--apparently describing staff of Japanese intelligence office in Helsinki. One person working on Turkish materials, others on American and Russian.

(D 2730 Helsinki-Tokyo 7.12.43)

- 3. Possibly HA Intelligence above under Russia No. 16, p.8. "Turkish telegrams" may be Turkish messages being intercepted and read by the Finnish Army and the Japanese, or may be Russian messages routed through Turkey.

(CI 1327(SSA 103470) Ankara-Tokyo 11.25.43)

United States.

- 1. Three persons working on American matters (apparently in Japanese intelligence office in Helsinki).

(D 2730 Helsinki-Tokyo 7.12.43)

JAPAN. (Continued)

United States. 2. American and British diplomatic codes are difficult to read, making Turkish and other easy codes better source of information on Allies.
(Continued)

(D 1266 Helsinki-Tokyo 6.17.43)
(D 1084 Helsinki-Tokyo 7.16.43)

3. Major YRJO PALKO of Finnish Army Scientific Intelligence Bureau, is cooperating with Japanese in Helsinki in study of American diplomatic code.

(D 2381 Helsinki-Tokyo 12.20.42)
(D 2729 Helsinki-Tokyo 5.26.42)
(SSA 72410 Helsinki-Tokyo 12.1.42)

4. To Chief of Central Special Bureau. I have sent by trustworthy means 3 packages of American telegraphic reports. These have been sent to Chief of General Affairs Department from Berlin, and should be burned in event of any suspicious circumstance.

(D 3585 Helsinki-Tokyo 9.24.43)

5. (Possible reference to cryptanalysis.) Major WAGII, Hungarian Attache resident in Sweden, has been recalled. We want him retained here because we have depended heavily on him in prosecution of objectives against America and Britain.

(D 3557 Stockholm-Budapest 11.4.43)

BULGARIARussia.

1. See above under Russia No. 3, p.2, re joint reading by Bulgarian police and German Army Secret Intelligence of code used by Russian secret agent arrested in Sofia.

(D 2834 Bucharest-Tokyo 7.10.43)

FINLAND.

Russia.

- 1. Japanese report on results of Finland's work on Russian Army's new 5-digit code. Finland has done no work on Russian diplomatic code.

(D 2225 Helsinki-Tokyo 5.17.41)

- 2. Finland agrees with Japan's description of Russian Army Code and has stopped studying it. Since Japan has succeeded in deciphering some messages, desire reference collection be sent over here (Finland will presumably consult this).

(CI 821 (SSA 64597--corrected trans.) Helsinki-Tokyo 10.19.42)

(CI 900 (SSA 64597) Helsinki-Tokyo 10.19.42)

- 3. Finns have recovered approximately 1000 words of Russian Army Code.

(CI 882(SSA 64147) Helsinki-Circular 1.11.43)

- 4. Suggest conferring of Japanese decoration on Major YRJO PALKO, Headquarters Chief of the Scientific Intelligence (or Chemical Espionage) Bureau of the Finnish Army. Since 1940 he has furnished Japan with much material on the decrypting of Russian codes, of which he has charge. He has contributed to reading of 5-digit and 4-digit Army and Navy codes, has always accompanied Major HIROSE on visits to the front line and assisted him in scientific espionage.

(D 2381 Helsinki-Tokyo 12.20.42)

(D 2729 Helsinki-Tokyo 5.26.42)

(SSA 72410 Helsinki-Tokyo 12.1.42)

- 5. Japanese cryptanalytic specialists HIROSE and HAKATA to make official trip to Finnish front-line cryptanalytic offices, in connection with Russian code.

(D 2883 Helsinki-Tokyo 8.26.43)

FINLAND. (Continued)

Russia.
(Continued)

- 6. Finnish authorities have succeeded in reading several messages of the Russian 4-digit Naval Code, but work has been discontinued for present.

(D 3585 Helsinki-Tokyo 9.24.43)

- 7. Japanese HA Intelligence. Re investigation of Turkish telegrams (?Russian?), it seems from check on materials being intercepted and read by Finnish Army that they coincide with work being done in Japanese Military Attache's office in Helsinki.

(CI 1327(SSA 103470) Ankara-Tokyo 11.25.43)

Turkey.

- 1. See message directly above. These may be Turkish rather than Russian messages being intercepted and read by Finnish Army.

(CI 1327(SSA 103470) Ankara-Tokyo 11.25.43)

United States.

- 1. Major YRJO PALKO of Finnish Army Scientific Intelligence (or Chemical Espionage) Bureau is cooperating with Japanese in Helsinki in study of American diplomatic code.

(D 2381 Helsinki-Tokyo 12.20.42)

(D 2729 Helsinki-Tokyo 5.26.42)

(SSA 72410 Helsinki-Tokyo 12.1.42)

HUNGARY

Great Britain.
United States.

- 1. (Possible reference to cryptanalysis). Japanese in Stockholm have depended heavily on assistance of Major WAGII, Hungarian Attache in Sweden, whose recall to Hungary they are protesting. He has handled Axis intelligence in a very masterful way, and aided in prosecution of objectives against Britain and America.

(D 3557 Stockholm-Budapest 11.4.43)

RUSSIA.Germany.

Following messages on collapse of German scheme for insurrection in India indicate Russians are in possession of decoded messages from traffic between Berlin and Kabul and the Central Committee in India. Whether this information was obtained by the Russians themselves or whether it was furnished to them by the British is not clear.

1. Alleged Soviet Col. MICHAILOV informed RASMUSS (German Commercial Attache in Kabul) that whole German traffic with R.K. (BHAGAT RAM) and the Central Committee was known to the Russians. He produced decoded recent "Tiger" code messages.

(SSA 102195 Kabul-Berlin 10.25.43)

2. Re above message. Evident from material produced that the Russians know the following schluesselverfahren: Books 1 and 2, "Lotos" and "Reis" with the kennwort "Nod" and "Signal Code." They do not know the "Tiger-Burg" circuit or the "Tiger-Burg" code.

(SSA 101027 Kabul-Berlin 10.28.43)