"TOP SECRET U"

B-J-S-M-800

BRITISH JOINT STAFF MISSION

Offices of the Combined Chiefs of Staff

WASHINGTON

AM 164 25 August 1945

MEMORANDUM for Brigadier-General Carter W. Clarke
Brigadier-General W. Preston Corderman.

SUBJECT: Security of Allied Ciphers

I enclose herewith a further paper in this series dealing with Security of Allied Communications.

W. Tarley
Eric M. Jones,
Group Captain.

Encl: ULTRA/ZIP/SAC/J.8 of 17 August (Copy 8 for G-2, 9 to S.S.A.)

Jek A

55A

~~ULTRA~~ Copy No: 9

ULTRA/ZIP/SAC/J 8.
17/8/45.

~~TOP SECRET U.~~

SECURITY OF ALLIED COMMUNICATIONS.

Far Eastern Summary No. 8.

I. Intelligence derived from Cryptanalysis.

(i) British

Army Communications.

(ii) U.S.A.

Aircraft Movement Code.

(iii) CHINA.

(a) Attache Cyphers.

(b) Army Communications.

(c) Air Communications.

(iv) TURKEY.

Diplomatic Cypher.

(v) RUSSIA.

(a) Intelligence from HARBIN.

(b) Army Communications.

(c) Met Reports.

(vi) FRANCE.

(a) Diplomatic Cypher.

(b) Consular Cypher.

(c) Study of French Communications.

II. Enemy Sigint Organisation.

(a) Proposed German-Japanese Cooperation.

(b) Security of Japanese Naval Cypher.

(c) Japanese Crib Methods.

(d) Appreciation of Sigint Reports.

I. Intelligence derived from Cryptanalysis.

(i) British.

a) Army Communications.

Further information is now available about Japanese Army Sigint in the Burma area from the recent interrogation of an apparently reliable P.O.W.

19/DSI 26/4/45.

He stated that the Signal Intelligence Section, attached to Army H.Q., periodically broke Allied (non Chinese) codes. He remembered seeing a large TOPSEC file at H.Q. 33rd Army marked 'A' Intelligence, which contained results of cryptographic success; and Japanese staff officers discussed in an excited manner the fact that we had discovered the location of their H.Q. This fact was confirmed by heavy bomber attacks on their H.Q. P.O.W. stated that the Japanese invariably ascribed the leakage to activities of "Radio Spies", i.e. local agents equipped with wireless sets for transmitting information back to the Allies. Hence the whole Japanese staff was infested by "Spy fever" most of the time.

b) Extracts from Documents captured at MEIKTILA 12/3/45, giving A Intelligence of British dispositions and troop movements.

1) From 15th Army Intelligence Report (no date given).

SEATIC/ 141.

CHINDWIN River Area.

"No. 2 V UNIT advanced E from SATKAYA area, and reached TON-MAKENG-MAGYIBIN area.
In correlating "A" Intelligence, the 98 Bde. appears to be attached to 19 Division, and its organisation is as follows :-

22 and 24 Assam Rifles at H KO DAUNG.
28 Assam Rifles at MASEIN."

Extracts from 15th Army Intelligence Report 1st - 10th January.

2) A Intelligence.

The 19th Indian Division seems to be planning to attack the Command post at ONBAUK on the 10th January.

3) Organization of 19th Indian Division A Intelligence.

62 Brigade :
2 Royal Welsh Regt. (British Army).
3 " Rajput Regt. (Indian Army).
4 Bu 6 Gurkha Regt. (" ").

64 Brigade :
2 Royal Worcestershire Regt. (British Army).
5 Royal Baluch Regt. (Indian Army).
1 Bu 6 Gurkha Regt. (Indian Army).

98 Brigade :
2 Royal Berkshire Regt. (British Army).
4 Bu Gurkha Regt. (Indian Army).
1 Bu 8 Assam Rifles Regt. (Indian Army).

The source of this intelligence is not given, but it may possibly be from the result of reading British Army Cyphers or from Chinese sources.

See ZIP/SAC/J7 for P.O.W. report on reading of British Army Communications in Burma Area.

(ii) U.S.A.

a) Aircraft Movement Code. . . . Reported Change in A.M. Code.

SAIGON Southern Area Army to Tokyo on 16 June, 1945.

C 1066A. "The AM (Aircraft Movement) code which changed from a 3-figure to a 4-figure book on 1st April was still being used on 18th May."

C 1050 A,C,D,E-K,M. On 17th June 2nd Area Army reported recoveries in the basic book of the AM code, which changed on 5th June. A list followed giving 66 recoveries of a two letter substitution table for letters, numerals, abbreviations and various types of aircraft.

Some of the common abbreviations had alternative substitution :-

e.g. Dep. = AH, CI, CN, EC, XO, HM
ARR = DP, GC, HG, IN, LA, OF, XA.

Types of aircraft were identified thus :-

R 4D = DC
C 54 = [illegible]B
B 25 = PH etc.

These results were arrived at with apparently a 12 day time lag.

b) On 28 June Tokyo sent PINRANG the following signal :-

C 1058 A,B. "The average number of AM code messages intercepted daily is approximately 100 - Because of the small number of messages at present, it is difficult to do decrypting - Please report the results of your work, as they are obtained.
The next change in the basic book is to be on 5th July A Intelligence."

A list of some recoveries of a two letter substitution for numerals was given but the meaning of some of the abbreviations, BUNO, ETF, AAC, SEN had apparently not been clear.

c) On 1st July PINRANG replied to Tokyo :

C 1063 - D. "We are reading perfectly all AM code numbers, letters, types of aircraft, place names etc, in the basic book. . . . . .
In the original text :
ETF = estimated time of flying.
AACS = Army Air Communication Station (guides aircraft back to base).
SEN = SENTANI, an airfield in Hollandia.
BUNO is an abbreviation included in names of Navy transport planes, but the meaning is not yet clear. We are increasing our activities and re-examining our results."

iii) China.
a). Attache Cyphers.

Some further examples of D. Intelligence have recently become available (for previous reference see ZIP/SAC/J7).

1) D 4 Intelligence (i.e. Sydney).

Tokyo to MANILA on 13th December, 1944.

UBJ 15572. "American Army positions on LEYTE according to D4 Intelligence of 6th December - The 32nd Division is attacking our TAMA/GYOKU group. The 24th Division is replacing the forces around CAPOOCAN. The 1st Cavalry Division is at Western SAMAR Island (it is doubtful if this is the main force). The 96th Division is in Central LEYTE, it is attacking our units. The 7th Division is in the neighbourhood of PALAMAS."

2) D6 Intelligence (I.E. Washington).

Tokyo to NANYUETH of 4th January, 1945.

J 62545A. "Report of Chungking M.A. in Washington of 29 December. After the American forces have occupied part of the Philippines, it is possible that they will land on the South-East China coast, using the Philippines as a base. Recently American infantry school instructors have been studying landing operations in the sector near TAISHAN, CANTON, HONGKONG : ....

3) Another example of D.6 Intelligence is given in a Tokyo staff message to NANKING and SAIGON of 25 January.

UBJ 15580.
BLY 0910. "According to "A" Intelligence despatched from the Chungking M.A. in the United States on 9th January, the United States has requested that documents relating to the official language of the Chinese Army, and to various types of enemy strategies mentioned in intelligence and spy reports be sent so that preparations can be made for landing operations on the China coast."

4) D.4 Intelligence (i.e. Sydney).

Tokyo Broadcast of 11th June.

UBJ 18165.
BLY 1073. "WEDEMEYER's general H.Q. in China has been in close contact with the Chungking Attache in Sydney. The American forces have communicated to this Attache a request to investigate the military topography of the China coast - He has sent a Staff Liaison Officer to MANILA, but appears to be anxious to move the Attache's office up to MANILA."

The original Chinese message quoted above was decoded by GC&CS and issued as BJ 145722.

5) D.5 Intelligence (i.e. Melbourne).

J 75337A. 7th Area Army (Singapore) to SAIGON, 23rd June.

"A Intelligence from the Melbourne Attache of 19th June. Report of landings at BRUNEI Bay. On the 10th, Units attached to the Australian Army 9th Division, landed east of BROOKETON."

The text of the original message from the Chinese Naval Attache, Melbourne, has been decoded by GC&CS and circulated as BJ 146428.

6) On 30th June the 7th Area Army (SINGAPORE) sent the following report to DALAT containing extracts from a signal sent by the Naval Attache MELBOURNE on 27th June, which was issued by G.C.C.S. as BJ 146872.

JEQ 1754
GRO 7664

"A Intelligence Report.

War situation of BORNEO area sent on the 27th by MELBOURNE Observation Unit.

Enemy positions N.E. of DJOEWATA oil-fields in the TARAKAN sector have been recaptured. Following this enemy resistance in this area ceased.

In the BRUNEI Bay sector, Australian troops captured SERIA on the 22nd. The enemy razed and burnt 21 oil-fields in this area. On the 20th, one detachment of Australian troops succeeded in landing at LUTONG and moving four miles South, reached "PAJUTTO".

In the LIMBANG sector, column heads of Australian troops have moved towards UKONG following the LIMBANG River. - However, as yet, they have not encountered the enemy. In the WESTON Sector, patrol troops of the Australian Army reached GADONG and NAPARAN on the 21st. They did not encounter the enemy.

On the 19th, the Australian Army landed at MEMPAKUL S.E. of LABUAN Island. - However, as yet no resistance has been encountered. Column heads have reached KARUKAN, 16 miles N.E. and KOTA KLIAS, 8 miles S.E.".

It will be seen that the time lag in the signals quoted vary between three to sixteen days.

7) Work at RANGOON on NEW DELHI-CHUNGKING Link.

Although the later signals giving D Intelligence are promulgated by the 7th Area Army at SINGAPORE it is clear from the following messages that the Special Intelligence Branch at RANGOON in the early part of 1945 was to some extent responsible for the interception, decoding and collation of this type of Intelligence from the NEW DELHI-CHUNGKING link.

a) Southern Army, SAIGON to RANGOON of 10th January, 1945.

UBJ
18129

"We would like interception of signals sent on the NEW DELHI-CHUNGKING link to be carried out, and you are requested to make arrangements. We are now applying to the Central Special Intelligence Bureau for code books".

b) Rangoon Air to Tokyo Air on 23rd January.

UBJ 16284.
BLY 0949.

"Please reply at once in connection with the following matters relating to the collation of intelligence reports from the Chungking people in India, which is to be effected by this Branch in the near future.
Do the remainder of your 1944 monthly Intelligence reports have a low or high priority ? Are the text books from SAIGON to be used for these messages ?
Please advise Southern Army Chief of General Staff whether or not interception can be carried out on a low priority ? "

ZIP/JES/
7059.

c) On 29th January, Rangoon informed SAIGON that the code used by the Chungking Military Attaches abroad passed on a high speed international link between BOMBAY and CHENGTU.

6) Army Communications.
The following signal is of interest having been promulgated by the Japanese with a time lag of eleven days.

J 53287A.

1) The 33rd Army at LASHIO to KI on 1st December, 1944, quoted "A" Intelligence :
"From LU, 93 Division C.O. to Commander CHOKAN WEI dated 20 November. Vacancies of personnel in this Army are as follows : Normal strength 6815 officers and men, including 93 officers."

J 55091
A-F H-J.

2) On 14th December, Nanking signalled to Tokyo the text of a message sent on the 12th (two day time lag) by the C-in-C 5th Group Army (Chinese) to the 2nd Reserve Commander in which the C-in-C quoted "a CHIANG KAI SHEK wire of 9th December."
This signal gave in some detail the Chinese order of battle, and appointments of various personnel, including proposals for despatching liaison officers to the various HQs to increase the close co-operation with the Allied Armies.

3) On the 5th January Tokyo sent a signal to CANTON, SINGAPORE, MANILA, BANGKOK and RANGOON, with these instructions :
"This information is "A" Intelligence, please handle it carefully."

UBJ 19601.
Extract.

"The United States Army in response to a request by CHIANG KAI SHEK on 9th December, formally despatched liaison officials. They are assigned to Army and Air General H.Q. and will handle liaison affairs. One officer has also been sent to the 4th War Zone, and to each emergency H.Q. under each district. He is to act as an instructor in peacetime, and a liaison officer in wartime.

4) A Tokyo Broadcast of 10th May gave an "A" Intelligence report for 7th May.

UBJ 14738.
BLY 0838.

"Traffic suggests that the 1st Army, newly organised at Chungking may have been dissolved at KUNMING - The C.O. of this Army, SUN LT-JEN, in response to an invitation from the Americans, is going to inspect the European Front."

5) Japanese aware of British Intentions from Chinese Sources.

SEATIC/141. Extract from a document captured at MEIKTILA 12/3/45. Burma Area Army Intelligence Report 20-31 December 1944. A Intelligence. "To LEE. O.C. New 22 Division (Chinese) from LUI, O.C. New 6 Army 21st December 1944.

The British 14th Army will command the 4th and 33rd Corps and will take positions for advance into middle reaches of the Chindwin. MEZA River will be the sector boundary between them and 36 Corps.

33 Corps will command 5th Indian Division, 11th E. African Division and 60th Division. Their role is to cross the CHINDWIN to the East, attack TANTABIN, and garrison SHWEBO.

The H.Q. of the British 36 Div (36 Indian Div ?) is at KANNI. The Division has taken up positions for the attack on MONGMIT."

c) Air Communications.

1) Signals read with delay.
5th Air Army, HANKOW to Tokyo of 21st August, 1944. (7 day time lag).

UBJ 9038. "According to an "A" Intelligence Report, the American representatives convened at the SINO-American Army Transport H.Q. at SINTSING on the 14th August and made the following decisions. Following the increase in the amount of various commodities transported by air to the aerodromes in the environs of CHENGTU, 50 trucks are to be allotted as follows to those aerodromes ....."

2) The Japanese 13th Air Division at Canton sent on 21 June the following signal to LIUCHOW.

J 76016.B. "The Chungking 1st and 2nd Air Armies (? YING YUAM and SINFENG) have moved to CHANGCHOW .... 26 May ..... A Intelligence."
This message appears to have been read with a time lag of 5 weeks.

Low grade Air Communications.

On 27th January, 1945, Tokyo passed the following signal to Rangoon concerning Chinese Air cyphers.

UBJ 12383. "Many low security codes are used for air communications. The systems such as the following are used by the Chungking Air Force and deal with patients entering the hospital, and commodities, but they contain little intelligence: SHIMMITSU. This is in process of solution. HIJO, COS, ITSUMITSU. These have been solved."

JES/7059. On 29th January, Rangoon informed SAIGON that there were many low grade codes used by the Chinese Aviation Commission in India. These dealt with supplies to CHIANG KAI SHEK and were of little intelligence value.

(iv) TURKEY.

Diplomatic Cypher.

The Military Attache BERLIN sent to TOKYO on 21st March the text of a signal despatched by the Turkish Ambassador in CHUNGKING to his Government in the beginning of February -

JMA/ 11606

"Internal situation in China. YENAN did not agree to the incopporation of the Communist Army in the Peoples Army, and negotiations with the Communist Party were broken off on 22nd December. The American Ambassador HURLEY went to the actual place (? YENAN) to pass on instructions from WASHINGTON, and had discussions with the Communist Party but failed to gain any objective, and reported to the American Government that YENAN had been acting in a way which made reconciliation difficult. - The Government informed the Ambassador that no other policy was open to America but to support CHUNGKING."

This signal was read with about 5 - 6 week time lag.

It was known from messages passing between HELSINKI and TOKYO during 1944 that the Finns and Japanese exchanged information on the reading of Turkish Diplomatic Cyphers.

It is possible that the code involved is Cypher 25 (SAKARYA) which until recently was the only book used at CHUNGKING.

(v) RUSSIA.

a) Intelligence from HARBIN. Possibly through physical means.

BRUTP 12814

On 17th April, 1945, the R.N.O. at HARBIN sent the following report on Russian Intelligence to TOKYO.

"From PETROPAVLOVSK to VLADIVOSTOK. A report from the (Russian) Naval Attache in America.

7th April. In reply to Senior Officers (Air Forces) of the fleet in the large scale air assault on OGASAWARA, COMINCH considers that at the present stage of the OKINAWA operations the fleet cannot be sent, and, furthermore, that air forces do in fact possess sufficient strength for the initial attack.
9th April. COMINCH is leaving only light cruisers and aircraft carriers in forward areas, and has recalled 3rd Fleet and both Task Forces. The position is now such that he has no alternative but to await preparation of a new airfield on OKINAWA.
13th April. COMINCH has just reported his reasons for stopping the advance of 3rd Fleet, (5 blanks) the appearance of a powerful fleet in the EAST CHINA SEA. That is to say, he is having battleships of 3rd Fleet remain in OKINAWA vicinity, and having cruisers accompanied by aircraft carriers advance into the above area.

From the Russian Legation in Australia to the Foreign Ministry.

8th April. 5th and 6th Squadrons are continuing to send aircraft which are to make OKINAWA their base. Reserve aircraft from SAIPAN are being sent as replacements to Task Force 58 and it is urged that the remaining ships of Task Force 3, which has been temporarily disbanded, should be incorporated in Task Force 58. (? 6) crack auxiliary carriers were to have arrived at SAIPAN within the week, but these are now to sail direct to reinforce Task Force 58.
9th April. BRITISH 4th Fleet is now steadily moving up from the sea area off SAKISHIMA to the OKINAWA area. There are signs in fact the British Chief of Staff has ordered the dispatch to the OKINAWA area of a further 2 battleships, 2 cruisers, 5 destroyers and 2 aircraft carriers to relieve damaged warships".

b) Army Communications.

J.59635

In a signal of 31st October, 1944, from KAMISHIKUKA to TOKYO. A Intelligence was quoted giving the gist of the orders for the defence system of the Border Garrison Unit of PETROPAVLOVSK Harbour and movements of U.S. and Japanese aircraft.

This signal is very incomplete and its only interest lies in the fact it is one of the few examples of Russian 'A' Intelligence.

c) Met. Reports in plain text.

J.63392
JM/CRYPT/
69/16

The Japanese 800 Met. Unit at HSINKING informed PEKING on 2nd February, 1945, that since 1st February all U.S.S.R. stations had suspended broadcasts of weather reports (? in cipher) and were now broadcasting in plain text.

(vi) FRANCE.

a) Diplomatic Cypher.

Some examples of the exploitation of French Diplomatic traffic by the Japanese have recently been seen.

1) Burma Area Army MAYMYO to RANGOON on 31st December, 1944, quotes "Special A Intelligence of 10th December. In connection with the RUSSO-FRENCH Neutral Assistance pact, SOVIET RUSSIA demands HAIPHONG as a base in the Far East".

The above signal was promulgated with a three weeks time lag.

UBJ
14992
BLY
0849

2) On 20th January, 1945, TOKYO sent a signal to CANTON, SAIGON, NANKING giving the text of a message sent by the French Ambassador in China on 18th January.

"According to 'A' Intelligence, the French Ambassador resident in China gains the impression that the Japanese authorities feel uneasy about the future situation and are preparing to take extra-ordinary measures against the French Indo-China Governor General. It will be necessary from his point of view, as the French Ambassador to China, to devise some corresponding plan immediately. Please report on any symtoms you may observe of this. We are also making enquiries as to the present position of the Japanese Army in French Indo-China".

UBJ 15775. 3) A further example is given in a signal of 25 January 1945 from Tokyo to SAIGON and CANTON, quoted as A Intelligence of 22nd January from the governor general of French Indo China, who planned to grant a special pardon for four Chinese criminals.

b) Consular Cyphers.

UBJ 13673. On 13th September, 1944, the following signal was sent from SAIGON to TOKYO - giving the "contents of the intercept " of a message, from an unidentified call-sign EZQ8 to FYW2 (LYONS wireless station).

"ET VS VEILLONS COMME D'HABITUDE FYW2 - STOPPONS ET VS VEILLONS COMME D'HABITUDE - VCI STU L.S.25. NIL STOPPONS ET VS VEILLONS COMME D'HABITUDE."

c) Study of French Communications.

J 64545. In a signal of 26th January, the Southern Army Special Intelligence Staff at SAIGON asked TAIHOKU (TAIWAN) to send to SAIGON with priority status a French linguist, 2nd Lieut. UMEHARA, "since special intelligence against France has already been started."

Berlin is asked for information about French Cyphers.

POP/JMA/537. TOKYO to JMA BERLIN, 22nd March 1945.

"With reference to your telegram, please let us know the set up and chief code groups of the French cyphers mentioned. The others are being read here also."

II. Enemy Sigint Organisation.

a) Proposed German-Japanese Co-operation.

Japanese MA BERLIN to Summer TOKYO dated 7th April, 1945.

JMA 11623. "After further enquiry into the question of Japanese-German co-operation on scientific intelligence, (i.e. study of cryptography), the German Army has abandoned its earlier plan of sending a considerable quantity of men and materials, recruiting personnel on the spot, and forming an independent German organisation, and is sending instead a small number of leading specialists and some equipment desired by the Japanese. It has put forward a proposal for collaboration between specialists of all kinds in TOKYO on the same lines as Japanese-German collaboration in BERLIN. Owing to present conditions of transport, I have signified our agreement at this end."

Major OPITZ, a German Army Sigint Officer recently captured in Germany, was to have been in charge of this party - (ZIP/SAC/J7).

b) Security of Japanese Naval Cypher.
Japanese Naval Attache BERNE to TOKYO, 8th June :

SJA/1967. "Since the collapse of Germany, all kinds of secret information without exception came into enemy hands, it is presumed that secret information exchanged between the Germans and Japanese is in enemy possession. Details of the Japanese Navy's request that German submarines should operate in Far Eastern waters, and particulars of the negotiations, have been disclosed to the British by Hitler's Secretary, and technical data supplied to Japan, relative to Radar, rocket aircraft and new types of submarine have all been passed to the enemy (a good deal to the British).

It is believed, however, that our Naval cyphers constitute the only case in which there has so far been absolutely nothing handed over to the Germans."

c) Crib methods employed for Cypher breaking.

JMA/11484. On 7th April, the Japanese M.A. BERLIN reported to TOKYO the desire of the Germans to establish communications in the Far East. He stated that the subject of these communications would be information about the enemy, and would naturally be sent in cypher. By permitting this communication, it would be possible to obtain material for reading German cyphers.

d) Appreciation of Sigint Reports from 2nd Area Army (PINRANG).

UBJ 7778. 1) On 8th March, 1945, 7th Area Army SINGAPORE informed PINRANG of the "inestimable value" of the Sigint reports issued by 2nd Area Army, and asked that information should be passed to 3rd Special Air Signals Unit (PALEMBANG), as material for appreciation of plans for the American Navy and Air Force's advance into the South China Sea.

2) CANTON to PINRANG. 29th April.

J. 52112. "The various types of Intelligence collected by your groups are the only source of intelligence on the Philippine area to guide air operations by the 13th Air Division in the South China area. We have been putting this intelligence to good use."

G.C.C.S. (S.A.C.)
17th August, 1945.

Distribution :-

External
1. D.D. 'Y', War Office.
2. Wing Commander E.C.G. Badcock, Sigs 5, Air Ministry.
3. Commander W.G.S. Tighe, R.N., D.S.D.10., Admiralty.
4. D. of I., India.
5. D. of I., S.E.A.C.
6. W.E.C., New Delhi.
7-9. Colonel H.M. O'Connor (3 copies and for G.2 and S.S.A.).
10-11. Section V Representative (2 copies and for Section V)
12. H.M.S. Anderson, Colombo.

Internal
13. The Director
14. D.D.4
15. D.D.(C.S.A.)
16. D.D.(M.W.) and for Mr. Parkin
17. D.D.(N.S.) for N.S.V.
18. D.D.(A.S.)
19. D.D.(3)
20. I.E.
21-22. File (2 copies)