

~~TOP SECRET FROTH~~

TO BE KEPT UNDER LOCK AND KEY AND NOT TO BE REMOVED FROM THE
OFFICE UNLESS AUTHORIZED IN ACCORDANCE WITH REGULATIONS

MH *[Handwritten initials]*

Copy No.: 3
Ref. No.: MA/RDE/012
Date : 1st June 1954

REPORT ON VISIT TO
FEDERATION OF MALAYA POLICE, BY SIGNALS INTELLIGENCE
REPRESENTATIVE, APRIL 1954.

Contents

1. Reason for visit.
2. Description of visit.
3. Results.
4. Security.
5. Acknowledgement.

Appendix A. Draft brief for visit.

- B. Comments on questions raised in brief.
- C. System of crypt records suggested to
- D. List of requirements from
and of ways in which the Signal
Intelligence organization might
render assistance.

DISTRIBUTION

Controller of Joint Service Organizations	Copy No. 11
D.M.I., A.H.Q., A.M.F	" " 12
D.S.B.	" " 1 - 10
	13 - 18
G.C.O. SINGAPORE	19 - 22

INTERNAL DISTRIBUTION

DIR	COPY NOS. 1, 7 - 10
MA	2
MH	3
ATD	4
MP	5
NS	6

(21 pages)

~~TOP SECRET FROTH~~

MHC

>4

~~TOP SECRET FROTH~~

Page 2.

1. Reason for Visit.

This visit was arranged following discussions between GCO, D.of.I., Federation of MALAYA, H/SIFE and ISB concerning the exploitation of a large amount of MCP cypher material which was understood to be held at [redacted]

2. Description of Visit.

The first two working days (17 and 19 April) after my arrival in SINGAPORE were spent in GCO's office reading over his MCP file, discussing various points with him and preparing a draft brief (Appendix A, paras. 1-3) to serve as a basis for my enquiries.

On 20 April I flew to [redacted] where I was met by the retiring SLO, Federation of Malaya, Mr. [redacted]. Later in the morning I met his successor, Mr. [redacted] (who has now taken over) and D.of I., Federation of Malaya, [redacted] with whom I went over my draft brief. D. of I. emphasized the problems which could arise from interpretation of translations in the event of our intercepting and solving MCP material, especially if classified Top Secret Codeword. He said that [redacted] might not accept our translations without proof that we were as capable of interpreting them as they, with their long and detailed knowledge of MCP affairs. I therefore added the question of interpretation to my brief. (Appendix A, para. 4).

On the morning of 21 April I met Mr. [redacted] Head of [redacted] Federation of Malaya, and had a brief discussion with him. Due to a visit of inspection by the new [redacted] I was unable to go on to the [redacted] (the centre for, amongst other things, interrogations of SEPs and translations of captured documents by [redacted] that morning and so spent it in SLO's office reading up some general background on MCP activities. In the afternoon I accompanied Messrs. FLETCHER and MARTIN to the [redacted] and met [redacted] (who is now on long leave) and his 2 i/c Mr. [redacted] (who is in charge during absence).

In the course of this meeting it soon became clear that there was no mass of untranslated material either in cypher or in plaintext at the [redacted] O.C. [redacted] stated that the only times that any backlog accumulated were when a particularly large haul had been made which might take a little time to clear. O.C. [redacted] offered me all facilities in carrying out the other objects of my visit.

I worked at the [redacted] throughout the 22nd, 23rd, 24th, 25th, 27th and for the morning of 28th April. On 25th April I visited the [redacted] detachment at [redacted] with SLO. I met Capt Mitchell, S/Sgt Penton and the other members of the detachment. We discussed the results of Capt Mitchell's rescue the previous week and reviewed plans for sending out the two sub-dets for the MCP search operation between 4 and 8 May.

On the 22nd I was introduced to [redacted] cypher expert, "The General", and to their Chief Translator, Mr. [redacted]. (There are no European translators in the [redacted]. My comments on all questions raised in my [redacted]

~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~

Page 3.

brief based on my own observations and on discussions with
The General and Mr. [redacted] are contained in Appendix B.

At O.C. [redacted] request I prepared and
explained to the General a system of keeping crypt records
based more or less on our own (Appendix C). I also left with
the Acting O/C a paper listing our present and future require-
ments, making some suggestions on the way in which we might
be able to help them and proposing that our channel of commun-
ication continue to be via SLO, Federation of Malaya (Appendix
D). It is particularly fortunate that the present SLO,
Mr. A.S. MARTIN has had considerable experience of Sigtint in
the past.

O.C. [redacted] also asked me for my comments on
their translation. I agreed to do this but explained that I
was not really qualified. Before leaving I informed the Acting
O.C. that the translations of the documents I had seen were
very good.

The afternoon of 28 April was spent at SLO's office
discussing the visit. On the morning of 29 April I saw the
D. of I., gave him an outline of my opinions on the various
points raised in my brief and thanked him for the assistance
and cooperation given by the Federation. After a rapid farewell
to Head of [redacted] I then flew back to Singapore.

In the afternoon of 29 April I wrote a signal to DSB
and [redacted] reviewing the results of my visit. On 30 April I
informed Messrs. [redacted]
of [redacted] of the main points arising from my visit. I also took
the opportunity of having a short discussion with two of
desk officers. Mr. [redacted]
and Mr. [redacted] on Sigtint matters
affecting their work. I was able to clear up some points and
noted others to be taken up on my return to DSB.

On Saturday morning, 1 May, I attended a meeting at
[redacted] to go over all arrangements made for the MCF search
operation, 1-3 May. Maj. A.A.M. Mason from Directorate of
Signals, AMF, also was present.

Remaining working time in Singapore, Saturday afternoon,
1 May, together with other odd earlier times was spent in
writing my report.

I left Singapore on the morning of 3 May.

3. Results of Visit.

Despite the misunderstanding over the amount of
uncollated material on hand I think the visit was well worth-
while for the following reasons:

~~TOP SECRET FROTH~~

Page 4.

- a) A good insight has been obtained into MCP cryptographic practices. This knowledge would be very valuable in the event of success in intercepting MCP material.
- b) It was possible to give a certain amount of assistance, advice and encouragement to the General.
- c) Present and future requirements and possible fields of mutual aid between both parties have been clarified; each has a better knowledge of the others problems and capabilities.
- d) I think that the establishment of personal contact has been of the utmost value in the present situation; without it I feel considerable doubt as to whether (a) and (c) could have been achieved.

4. Security.

The cover story which it was agreed by D. of I., Head of and SLO that I should adopt was that I was a code expert from Singapore, with some knowledge of codes and cyphers and that no mention of wireless be made unless it proved necessary. In fact this story proved quite satisfactory, no reference to wireless was made either to Mr. or the General, and I am sure that Signal security was not jeopardized in any way by the visit.

5. Acknowledgement.

I should like to express my appreciation of the help and cooperation I received from all the Federation and authorities concerned.

~~TOP SECRET FROTH~~

Page 5

Appendix 1

DRAFT BRIEF FOR VISIT

1. To find out what is known about MCP cryptography. To ascertain what types of cyphers have been broken and what methods are employed in breaking them. To obtain or render (within security limits) advice on methods of solution.
2. To arrange a channel for rapid exchange of cypher information and views on breaking MCP cyphers between [redacted] and the Sigint Organization (S.C.O.) and to define cryptographic information likely to be of assistance from Sigint point of view.
3. To examine uncollated material to find proportion and type of unsolved cypher. To determine whether there is a requirement for further detailed Sigint examination, if so, to make suggestions concerning further processing.
4. To investigate bearing of local expertise on interpretation of translations.

~~TOP SECRET FROTH~~

~~TOP SECRET~~ ~~FROTH~~

Page 6.

Appendix B.

COMMENTS ON QUESTIONS RAISED IN BRIEF

1. MCP Cryptography.

- a) All MCP cyphers seen so far in ground source material have been interspersed with character plain text and all have been solved by the General.
- b) Details of systems will be found in Appendix C. A specimen key only is given in each case. In some cases many keys have been solved.
- c) Judging from both captured and solved cypher materials, the systems used within the Northern Bureau have been much more sophisticated than those in use in the Centre and South; this is somewhat surprising for instance in the case of a state in which MCP influence is considerable. Apparently there is one person or group of persons in Northern Bureau who has some ideas on cryptography. There is no obvious evidence of either internal coordination or external influence.
- d) Various other points of interest -
 - (i) Dummy letters are frequently used
 - (ii) Letter figure substitutions are usually based on key words, character figure substitutions on key phrases.
 - (iii) The arrangement of characters is used for the vocabulary in 3 captured codes (Z-2, Z-3 and AD). The most recent book captured (Z-1) has its vocabulary arranged in radical order.
 - (iv) In most captured books, page numbers and row/column coordinates have not been printed but filled in by hand and appeared in most cases to be human random. Space is provided for three sets of these, presumably enabling each user (up to three) to use a different set.

2. Method of Solution.

Since all MCP ciphers to date have been interspersed with character plain text, the General's procedure has been as follows:

- a) Solve the letter figure substitution used, if any, with the aid of any dates or figures encyphered in the text.
- b) Then, making use of the plain text, prapse in recoveries.
- c) Try to fit these characters to known dictionaries or code books.

~~TOP SECRET~~ ~~FROTH~~

~~TOP SECRET FROTH~~

Page 7.

This seemed to me perfectly satisfactory under these conditions and there was little assistance I could give him.

However, I did examine his recoveries in AD, many of which were ambiguous. Much of the ambiguity was in fact only due to the characters concerned being place names which could be recovered either as the first character of the name in the vocabulary section or as a whole name in the place name section. I spoke to the General about it and stressed the need for a clear distinction to be made between "certain" and "probable" values. He fully appreciated this and has undertaken to go through the book again checking each value.

I gave the General some hints, using made up examples, on the use of frequency counts in solving simple recyphers of CTC (single group additive; letter figure substitution) and in getting an initial break into code material. The most likely need for their application of course would be if the whole of a document or all of a number of documents were encyphered. The General considers (and I am inclined to agree with him, that this possibility is somewhat remote due to the amount of work involved in encyphering.

One can be reasonably confident that Sigint would be able to cope with any cyphers used on the lines of those either captured or solved to date and would not require assistance; and conversely that the General is at present in no need of expert Sigint assistance.

3. Interpretation.

I investigated the need for local expertise in interpreting translations in two ways, firstly by asking Mr. [redacted] and the General for an outline of the main points involved, and secondly by working through the text and translation of a typical document. The factors which Mr. [redacted] considered to have most bearing on interpretation were :

- a) Knowledge of Communist terms and jargon (*)
- b) Knowledge of character abbreviations used by MCP (*)
- c) Knowledge of organization of MCP
- d) General knowledge of MCP history - events, conferences, anniversaries, personalities.
- e) Experience.

(*) Copies of lists of these compiled by [redacted] have been given to DSB.

~~TOP SECRET FROTH~~

~~TOP SECRET FROTH~~

Page 8.

My opinions on this subject are:

- a) In all translation work a good background knowledge of the subject is essential.
- b) Points (a)-(d) above refer to exactly the sort of background information and collateral collected by reporting branches for the benefit of Sigint translation.
- c) [redacted] and in particular Mr. [redacted] and the General are in possession of very complete knowledge of the MCP, much of which is not on paper. If security regulations permitted it is clear that it would be most advantageous for the Sigint translator to work on Sigint material alongside [redacted] Chief Translator, so as to get the benefit of this experience.
- d) If however security regulations preclude this, it should certainly be possible for an experienced Sigint translator to cope with intercepted MCP traffic provided adequate collateral is available. It is worth noting in this connection that when dealing with telegraphic texts as opposed to documents the Siginter would have the advantage of being on his home ground.
- e) I would like to suggest that a service of collateral (e.g. periodic summaries, collated reports etc) be laid on forthwith as an insurance against future developments.

~~TOP SECRET FROTH~~