

~~TOP SECRET CANOE~~REPORT ON VISIT BY MR. [REDACTED]16th, 17th and 18th February, 1953EO 3.3(h)(2)
PL 86-36/50 USC 3605

I

GENERAL

I arrived at Paris at 6 p.m. on February 16th and had dinner with Colonel [REDACTED] the same evening. Over dinner we had some informal discussion of a wide range of [REDACTED] topics. Next morning I went to the HQ of the STR where I discussed the Vietminh problems, and on the same afternoon I was invited to meet a research cryptanalyst and discuss [REDACTED]. On February 18th I had a farewell luncheon with Colonel [REDACTED] and returned to his office in the afternoon for a brief discussion on security and dissemination.

2. [REDACTED] arrived on the morning of February 17th and had discussions on the equipment problem on the 17th and 18th February with [REDACTED] head of the intercept and [REDACTED] who is concerned with interception. At these meetings [REDACTED] was able to obtain precise information about [REDACTED] requirements, and the results of his visit are given in an appendix to this report.

3. [REDACTED] and I left for [REDACTED] together on the night of February 18th, arriving home the following morning.

II

VIETMINH

4. A sample of about six weeks [REDACTED] material was dispatched to [REDACTED] a week before I left. Unfortunately this material did not reach the [REDACTED] until Friday, February 13th, and they had not had time fully to examine what amounted to some 4,500 texts.

5. The sample referred to above was sterilised by removal of all [REDACTED] numbers. This rather laborious task was undertaken in order to comply strictly with the rules laid down in Appendix P to [REDACTED] Agreement.

6. A simplified Texta with ad hoc notation had been sent with the sample; this included only call signs and frequencies used on each link for which traffic was present in the sample.

7. The [REDACTED] representatives for the discussion on the morning of February 17th were [REDACTED] head of the Crypt and Reporting department or [REDACTED].

8. At the beginning of the meeting I handed [REDACTED] a list using the same ad hoc notation referred to in para. 6 above and giving a brief description of the location and functions of each link so far as was known to [REDACTED]. [REDACTED] compared this with a similar list prepared by his own staff after examination of the traffic. Except for the fact that some of our links were quite unknown to the [REDACTED], the general picture strongly suggested that our effort and theirs was already largely complementary. They have far more interception but it is tied down to day to day operational requirements and they have little or no leisure for search and development, on which our relatively small party at [REDACTED] can make a valuable contribution.

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

9. I explained to [] the system whereby all [] on Vietnam and other Far Eastern problems was concentrated at [] and mentioned also that when working on Vietnam we tended to concentrate on longer term problems (politico-economic situation and external relations) rather than the day to day conduct of the war.

10. M. Mouratoff said that he would take a copy of the complete French Vietnam interception data, superimpose on it the information about British interception obtained from study of the sample of material supplied by us and send the results to us with comments showing where we were duplicating, where our effort was of value to them and where they would like if possible to have more help. In reply to a question from me he said that STR were willing to supply DSB with French raw material as required.

11. There is a good deal of detail sorting and registration to be done before the [] can produce the annotated Texts referred to above, and we may expect to have to wait a week or two before the next move comes from them.

12. [] would like us meanwhile to continue to supply [] raw material on Vietnam, as sent in the sample.

(a) They consider that for the time being at least it should come to [] not to the sub-centre in []

(b) The intelligence value of our [] is largely long term and the sub-centre would in any case not be able to use it for their short term work unless very special arrangements could be made for quick delivery.

13. The subject of exchange of crypt recoveries was not discussed.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

III

EO 3.3(h)(2)

14. On the afternoon of February 17th I was invited by [] to meet some of his crypt experts who had been working on [] material supplied by []

15. [] showed me a number of [] and others, solved by his department. These fairly naturally corresponded to the similar work done at [] No evidence was given of similar success on military problems.

16. He then sent for [] (the research officer of [] whom I met last year - see para. 36 of DGC/2253) and the latter showed me some of the [] work on []

IV

OTHER TOPICS REFERRED TO IN CONVERSATION WITH []

17. [] are developing electronic high speed machinery,

(a) for production of random one time key,

and (b) for cryptanalysis.

18. [] is convinced that the future of cryptanalysis lies in use of [], if only on account of the vast bulk of material that would need to be processed.

- 2 -

~~TOP SECRET CANOE~~

19. [] mentioned the monitoring of an Allied exercise by [] and expressed his concern at the lack of security in allied communications. The [] intend to carry out a larger scale monitoring of an exercise this summer and have promised to give us a detailed report.

20. [] showed me a new [] produced this year and kindly undertook to send me a copy. So far as I could judge from quick perusal of this book it is a well arranged work introducing basic mathematical principles at a relatively elementary stage just as [] do in their training courses.

21. Finally, before taking leave of [] I raised with him the whole question of security of dissemination.

(a) He said that in [] no intelligence report based on interception goes outside the intelligence compound on [] except only [] telegrams which go to the Foreign Ministry.

(b) In [] reports were issued from the sub-centre with two different security gradings distinguished by different coloured paper.

(c) As regards dissemination in [] he said that

(i) Military reports went to specified officers on the General Staff who were forbidden to give them further distribution.

(ii) Reports on politico-economic-administrative matters went to similarly specified officers in the Security Police.

[] kindly undertook to prepare a brief statement on [] Sigint security methods and send it to me.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

~~TOP SECRET CANOE~~

Appendix 'A'

REPORT BY [] ON HIS VISIT TO []

17/2/53 - 18/2/53

EO 3.3(h)(2)

PL 86-36/50 USC 3605

In connection with technical matters arising from the visit of AD1, I was present at a meeting held in Paris on February 17th. In company with AD1, I was introduced to:

[] Director

2. A technical discussion followed between myself and [] (who's responsibilities include the radio equipment of the []

[] This discussion was concerned equipment requirements for the prosecution of the war against

3. [] asked for three things:-

- (a) Spaced loop D/F equipment (1.5 - 12 Mc/s acceptable)
- (b) Mobile 'single' loop equipment (1.5 - 15 Mc/s acceptable)
- (c) HF receivers; to good, but not necessarily field, tropical standards; not so hermetically sealed as to preclude maintenance in the field. Frequency coverage 1.5 to at least 20 Mc/s.

4. I told [] -

- (a) That delivery of the Marconi DFG29 spaced loop equipment, which he was aware of, was at least eighteen months and that there was no other equipment known to me with earlier delivery.
- (b) That no HF loop equipment was immediately available; either, as far as I know, commercially or from Government sources. That we, ourselves, were about to adapt an existing receiver; possibly the [] (a commercial write up on which I left with him) by the development of a simple screened loop system. That we would add his requirement of 18 sets to the production run and do our best to meet the target date of first deliveries in six months time. That these sets would be tropicalised, as far as possible, and would be complete with any auxiliary equipment (such as converters for battery operation) and a pack of spares (preferably 'life-time').

I undertook to send details of the equipment, as soon as it had reached the design stage. I said I thought the cost of the complete equipment, with spares backing, would be in the region of []

- (c) That we would do our best to start the supply, within a month, of 60 HF receivers of a general purpose tropicalised pattern. (I did not commit myself to a specific type but indicated it would probably be a standard Army one). That the cost with spares backing would be about [] per kit.

~~TOP SECRET CANOE~~

~~TOP SECRET CANOE~~

Appendix "A"

(d) That the above agreements were made on the assumption that a satisfactory arrangement for the formal transfer of the equipment would be made shortly.

5. As [] inquired about prices, I judged that he, as controller of the equipment concerned, had assumed that they might have to face up to payment.

6. The discussion was extremely cordial and I had the impression that, though the [] were bitterly disappointed we could not assist them by the supply of spaced loop equipment, nevertheless they were very grateful for the aid we were able to offer, particularly the eighteen mobile D/F equipments.

7. [] told me that his interests were fully represented on the [], so that there is apparently a satisfactory coordination of their scientific effort. The subject of miniaturisation came up and he stated that he was not aware of any special progress in that field, resulting in the production of very small receivers of the pocket type, etc.

EO 3.3(h)(2)
PL 86-36/50 USC 3605

EO 3.3(h)(2)

~~TOP SECRET CANOE~~

Important

Introductory -
 P. 2 - TP 5 (v)
 - 6
 3. - TP 9
 10
 4. - P 12
 13
 15
 5 - P 16
 19
 8 - P 30
 9 - P 31
 10 - P 32 (v)
 33
 11 - P 36
 37
 38
 39
 12 - P 39 Contd
 40

Appendix A
 P. 1 - TP 1
 2
 3
 4
 5
Annex. 2
 P. 4 - TP 8
 5 - TP 9
Annex. 3
 P. 1 - all
 4 - TP 8
Annex. 4
 P. 1 - P 3
Annex. 5
 P. 1 - P 1, 2, 3
Annex. 6
 P. 1 - P 1, 2
Annex. 7
 P. 1 - TP 1, 2
 3 - TP 3