Annex 15. David Sissons to Kenneth McKay, 9 November 2004

22 SAVIGE ST
CAMPBELL
A.C.T., 2612
<d.sissons@tpg.com.au>

9 November 2004

Mr K L McKay
[redacted]

Dear Ken,

Another request for help and guidance. Once again please pardon my importunity.

MR HIBI'S REQUEST

At the suggestion of the Military Attaché, Mr Hibi eventually approached me. I was able to give him some help, but unfortunately was not able to produce the items he sought—sound recordings of Japanese news broadcasts on the day of the Emperor's surrender announcement.

Mr Hibi was under the reasonable misapprehension that the monitoring of Japanese civil transmissions was one of the tasks allotted to our cryptographic organisations. In fact it was the task of the Short-Wave Division of the Department of External Affairs. Their monitors had an office somewhere in the city—in Temple Court, I think—with landlines to their receiving station at Ballan. Mr Graves and his successor Mr Whittall were part of that organisation. You may remember that their secretary, Mary Stewart, used to come over to our eyrie for afternoon tea. On the day of the Surrender she brought us a copy of the English translation of the Emperor's broadcast, which Whittall's organisation had monitored.

For Mr Hibi I was able to locate the hard-copy transcriptions of the broadcasts that were monitored. It was, however, the recording disks/cylinders that he required. Unfortunately, these appear to have been destroyed.

GEAM

Since I wrote to you in May I have devoted a good deal of time and effort to the History; but I have to report that, alas, I have made little progress. Please cast your eye over the updated version of *The Breaking of GEAM I* (**Enclosure A**) and you will see why. (That document, of course, is merely my thoughts to date and bears little resemblance to what will be the final text).

Essentially the thesis that emerges in *The Breaking of GEAM I* is that, according to his cables to TANTRUM:

(i) Trendall on August 9th had since August 5th sent London about thirteen keys (some of which we now know to be wrong) but had established no 'good' bigrams (although he had noted some frequently occurring short concatenations—of row length or less);

(ii) On August 10th he received the Hanoi to GEAM statistical list that gave him the bigrams for comma (UF) and the ten numerals;

(iii) He remembered that UF represented comma in LA also and analysed his accumulated GEAM traffic on the hypothesis that some other bigrams represented the same plaintext in both LA and GEAM. He was in luck; for this was the case for 48 out of the 60 kana syllables and for an additional 30 syllables and 4 punctuation marks.

(iv) Thus armed, he was able within twenty-four hours to establish, by anagramming, the correct column order and to establish the bigrams common to LA and GEAM and the values of another nine bigrams where GEAM and LA differed (including the bigrams for the very common syllables *wa* (UR), *no* (GO), *o* (BO) and *to* (FO).

Underlying my thesis are the following considerations:

(i) In all the examples of columnar transposition that I have seen—namely Sinkov, Friedman, ADFGX and FUJI (**Enclosure B**)—solution of the column order has depended on prior identification of 'good' bigrams and/or the presence of some short columns among the long (and in GEAM I there are no short columns).

(ii) GEAM's code is cunningly devised to prevent this—e.g. GI represents *ni* but IG represents *nin*; AC/CA which represent *kan* and ki respectively appear more frequently than GO/OG which represent *no* (the most common kana syllable) and *Begin English* respectively.

My problem is that my thesis is inconsistent with the account given by Eric in his *Report*:

> It merely remained to put these groups together on repeats. This part of the job did actually present a few stumbling-blocks, as the presence of a row-order was not at first suspected and we were unfortunate enough to have constructed all the repeats backwards. The code-breakers were therefore somewhat baffled when these texts were presented to them—although it was later found that the main difficulty was the fact that the early messages were encoded from an English text. The first guide to the real solution was given by the incomplete blocks in which an incomplete line of five letters appeared at the end of the line instead of at the beginning. Thus we saw that we had our keys backwards; this was remedied and then long repeats were found going from one line to another, the second line not necessarily being the next in order. From then on the breaking of the code and row order was a relatively simple matter and the complete code and cypher system were known within a fortnight.

Eric's account is of unassailable authority—he was a very gifted and experienced cryptanalyst, he was present at the time, and in 1946 when he wrote the *Report* the comprehensive and well organised records of every message received and decrypted were still intact and at his disposal. The *Report* suggests that, before the first code group was known, Trendall had established column orders, in several keys, that were in each case correct except that they were in reverse. We know that this was not done by the usual method of anagramming on the basis of known 'good' bigrams. Perhaps the clue lies in the sentence: 'We were unfortunate enough to have constructed all the repeats backwards'. Perhaps these 'repeats' are the single-row concatenations enumerated in Trendall's August 10th cable? In the absence of any known bigrams did he attempt to anagram on the basis of these? But how can this be done unless the code values of these bigrams were known? Was this not doomed from the outset—as evidenced by the fact that in most of these repeats he got it wrong way about? But here I must be mistaken; for Trendall and Eric, of all people, were highly skilled and understood completely what they were doing.

The basic question, I suppose, is how is it that Trendall managed without identifying a single bigram, to produce solutions for a dozen keys in which he was fairly confident.

It appeared to me that in the absence of any identified bigrams the only technique available to Trendall was Friedman's 'Solution of Messages Containing the Same Long Plaintext Phrase'. I accordingly, as an exercise,

tried to apply this technique to a couple of GEAM messages that I concocted (**Enclosure C**). But as you can see, this proved to be a task beyond my ability.

It was foolish and presumptuous of me to imagine that, totally devoid of mathematical aptitude or cryptographic experience, I could reconstruct Trendall's solution.

I hate to impose on you yet again; but I'd be greatly indebted to you if you would cast your eye over what I have written and, with your experience with transpositions, perhaps put me back on the rails.

THE BIBULOUS SIG

Over the years, I've tried to find some documentation for the case of our bibulous Sig, who over a cup of tea in the Cathedral recreation hut palled up with a young rookie, explained the GEAM system to him and urged him to contact Col Little for a job in the outfit—which the rookie promptly did. It was Ian Smith who told me the story:

> His name was Cpl Budge, a heavily built man, with a fleshy pock-marked face, sallow complexion. He got sozzled one day (late 44 or early 45) in a city bar and began narrating to all and sundry details of our operation... He was arrested, never to be seen again... I saw him again in the early fifties on an Essendon tram (I.H.S. to D.C.S.S. 18/9/90)I

If he were court-martialled, his name would appear in the comprehensive alphabetical index to court-martials available at the Australian Archives. If the case was disposed of summarily by his CO (or if, instead, he was merely posted elsewhere) this would be noted in **Routine Orders Part II** of his unit. But to search these records I need to know the Sig's name. I think that Ian may have got it wrong. A couple of years ago the Department of Veterans Affairs published on the internet their roll of AMF personnel who served in World War II. I have worked through all the Budges in it and there are none in the Aust Corps of Sigs whose postings fit our chap. I remember, however, that one of the AWAS who operated our cipher machines was named Budge; and the Veterans Affairs roll confirms this (W45806, Sgt BUDGE Helen Lindsay, b. 5/8/23, 1 Aust Cipher Sect, disch. 13/3/46). The odds against two people with the rather uncommon name, Budge, serving in the same small unit must be fairly high. I wonder if Ian may have got the names mixed up. Do you happen to remember the chap's surname and Christian name?

ARTEMIS

I wonder how ARTEMIS came to be chosen as the Section's cable address. I doubt that Bletchley or Cable & Wireless Ltd dealt it out at random from some previously prepared list. It has nothing in common with the cable addresses of kindred organisations e.g. MOUSETRAP, TANTRUM, AMBITION, etc. Was it chosen by some wag in M.I. with a classical background who saw Trendall as the virgin huntress and the rest of you as his attendant nymphs? Or did Trendall himself choose it in some play on words obvious to any classicist but not to me? Trendall appears to have enjoyed jesting with cable addresses—Treweek told me that he once despatched the following signal to Kilindini (whose cable address was AMBITION): 'Your proposed solution indicates grievous lack of serendipity. Ambition should be made of sterner stuff'.

Once again, my apologies for burdening you with these requests.

Yours sincerely,

(D.C.S.Sissons)