Annex 4. Ian Smith to David Sissons, 8 August 1990

Excuse handwriting, I cannot type, & no longer have access to typists.

8 August 1990

Dear David,

Your letter of 3/8 came to hand to-day. Please do not apologise for intruding on my retirement, on the contrary I have spent a pleasant few hours trying to remember one of the happy periods of my life.

I fear you will have a difficult task, if the records of that diplomatic section have been destroyed. I have a clear memory of participating in the composition of an archive sometime in the spring or early summer of 1945. Eric Barnes was in charge of this operation, I think, and it was well done. Description of the codes and the work done, &, I think, the files containing each weekly report put together by the head translator. Alas! it is no good weeping over burnt paper.

If you do take on this task, I should think that Ron Bond and Eric Barnes would be good sources, in some ways better than Trendall, since they were there till September 1945 (Ron Bond is retired from Scotch College some 3-4 years now, and lives at 30 Hortense Street, Burwood, Victoria, -- we have remained in touch over the years, tho' we do not often speak of the Vic Barracks room & its work -- conditioned by the tabus of 1945?). Eric Barnes finished his career at the University of Adelaide, but I have not seen him for about 10 years (he was at a conference in Hobart) -- he was then fascinated by his war work & used to give talks on cryptography, -- he was also familiar with modern cryptography (it sounded diabolically sophisticated -- I gather it is in great demand for computer security).

Tony Eastway retired from CSR early (in his early fifties), -- he spent a few years in the peacetime successor of the section, but his wife grew fed up with Melbourne & he went to CSR in Sydney. His address is 15 Ruby Street, Mosman, NSW -- he keeps in contact with my mother & we write at Xmas, but I have not seen him since the early 70's.

Ken Mackay must have retired from ANU, but I have lost touch.

Jac James (now, alas, Cyril James, as he was baptised) is retired in UK, at a fiendishly long address, Rosebery House, Elenby Road, Ashton-under-Hill, Evesham, Worcs, WR11 6SW. He sends a news circular at Xmas, mainly about his four children, who seem to be

all "trendoid" -- not seen since 1972, when we passed thru' London and played "battleships" again in memory of old times. He may have memories of the actual material that was handled.

I arrived in the unit in May 1944 (via Central Bureau, where I spent a miserable month after basic infantry training). Trendall presided when I arrived, sitting in the corner where RB sat later. His absences became more & more frequent and he returned to Sydney some time in the spring of 1944, perhaps as late as November. I have memories of him taking us each Thursday to the Society Restaurant for lunch for quite some time after my arrival. I stayed on until November 1946, I think, intending at one stage to seek a position in the postwar section, which began crystallizing with people who had been in Central Bureau and who must have begun arriving by October or November 1945. I have memories of playing endless games of bridge & chess during this interim period. When I got a p/g CRTS scholarship, I abandoned any idea of staying on & have no regrets, the more so as it quickly ceased to be a game for amateurs.

Tho' I worked on an equal footing with Eric Barnes (of course I had nothing like his creative talents), I did not really see what happened in the actual administering of the department. We were under Col.Little (ADMI) in my time and RB used to take his orders (I have a feeling Trendall kept a paternal eye on what went on -- I can remember him telling me I was to be promoted corporal, which would have been on a fleeting visit to Melbourne after his departure). I have a feeling that nothing very dramatic or crucial came out in the decoded material during my time, but I was so fascinated by the game of cryptography that I really took no interest in the end result, -- it could have been a treatise on Zen philosophy for all I cared. As long as the messages used new sections of the cipher book, I was happy. The ciphers that we worked out were transmitted to UK & much more rarely we received material, often of poor quality, from them (UK) -- I cannot remember clearly whether our material was transmitted to Washington but I think so. The weekly reports went to Blamey, and (once again, I think, but am not sure) also to McArthur. I have vague memories of spies being identified in Kabul & New Delhi.

A postscript on the personnel: Arthur Cooper (a character -- Trendall's memory deceives him on the dates of Cooper's presence -- I never knew him) had left before I arrived (he returned to work in the postwar section in the 50's but I never met him). There was also John Davies, who left for Central Bureau before my arrival, -- he became Prof of French at New England & then Adelaide, now retired, living somewhere in Adelaide, -- he would have memories of 1943 & early 1944.

Recruitment, -- the connection was Sydney University, but also Sydney high schools. Like Tony Eastway, I was put in contact with Trendall by a brilliant Classics master at North Sydney Boys' High School (my family moved to Melb, so I studied at Melb), -- Tony & I were exact contemporaries, Ken Mackay a year ahead. Ron Bond would have known Trendall as an u/g at Sydney, but would have put him in touch with Eric Barnes & John Davies (they were all at Canterbury High together & Treweek, I think, had

taught Classics there before the war & before getting a post at Sydney University

Trendall's recollections of the cipher 10101 are blurred. When I came in May 1944 I was assigned to this cipher working under Eric Barnes. The code-book consisted of 4-figure groups, representing kana syllables, but also common words or phrases, also things like 6378...8014 which enclosed kana transcriptions of English phrases (eagerly welcomed; for one could guess the transcribed phrase -- I remember "heiseibingudebaisu" -- face-saving device). "No" was 8416, "wa" 8559, "to" 2758", -- if only I could remember the details of my present life as vividly! The message was encoded, then enciphered using the cipher-book, with the second 5-figure group (the first was 10101) indicating the beginning in the cipher-book. Your assumptions given on p.5 about the decipherment method are correct for normal ciphers of this kind, -- a large number of messages are usually needed to build up the "depth", but we were helped by the old-fashioned spirit of the Foreign Office in Japan. The full 10000 4-figure groups were not used in the code-book, the first figure being restricted to 2,4,6,8, the second to 1,2,3,4,5, the third figure to 1,3,5,7,9, the fourth alone being unrestricted, except that 0 was not used. The basic pattern in the code even-anything-odd-anything meant that whenever the same cipher numbers were used, the number groups of messages would have a common pattern and it was very easy to line up messages using the same passage, once you had catalogued the even-odd patterns of the messages.

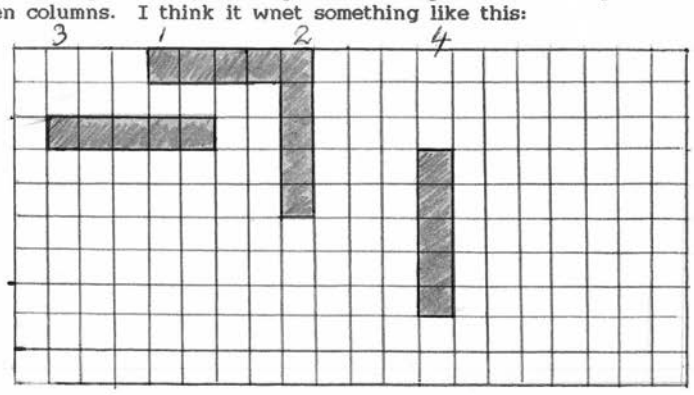
When I arrived the code-book was fairly well-known & the main task was deciphering the messages, when they had built up to a certain "depth". In some cases with the help of Jac James, one could work on a "depth" of two, particularly when the code-groups overlapped by two, or when the subject-matter was routine.

By early 1945, or perhaps before, Eric Barnes had discovered the secret of the indicator. This was the second 5-figure group. The third group (first of the actual message) was subtracted from this & the result was the cipher-book reference in clear, page reference, column, line. I cannot remember how he hit on this, but he had brilliant intuitions. From then on the messages were read using the same method as the Japanese cipher clerks (JBD, by the way, was the reference for 10101).

There had been another 4-figure code, NE, I think, was the name, in use until just before I came; but it fell into disuse and the other main code in my time (apart from GEAM, which was easily read & and left to Paul Grange & McKenzie to decipher mechanically) was called BA (from the two initial letters of its indicator; JBC was its reference). Ron B & Tony Eastway used to work on BA, and when 10101 was easily read, Eric used to turn his mind to BA, -- I, too, but with very middling success.

BA was a transposition cipher, with a grid, I think, 20 across (but maybe 25), and about 10 or 15 deep. The code consisted of bigrams, with a smaller number of trigrams. The message was encoded, then written across the grid, then read by columns in a

random order indicated by the group BA... at the beginning. Further there were groups of blanks in fives, horizontal alternating vertical, their position being determined by the first ten columns. I think it wnet something like this:



This cipher was broken before I arrived, I think, because a message had been badly enciphered, was repeated using the same indicator & so the same grid with the same blanks. This gave a break into the nature of the grid.

Your SOSOS was in fact 50505, -- it was thought to be a one-time pad cipher (i.e. the pages of figures were used only once), as it was never broken -- the traffic in it was very small. I remember learning after the war, probably late in 1945 that it was in fact a one-time pad cipher. No doubt they were terrified of using up their pads, hence the small traffic & the general use of the vulnerable 10101 & BA in 1944 & 1945.

Until this point I have been following my own thought train. I turn now to your letter & its questions (if I have not already answered them above).

The relationship between Cowley (of whom I have no memory) or his predecessor, Archer (whom I remember vividly because he had piles and was always scratching his arse), and RB I cannot know for sure. I suspect that technically RB was in charge under Little, but that Cowley was deferred to, Archer likewise. Biggs I remember with distaste, my first experience of an arrogant Pom (he married Kiwi Boot-Polish, a Miss Ramsey, and was prominent in Japan-Aust cultural relations at one stage). The Nips had interned him & mistreated him despite his diplomatic status, -- I cannot find it in my heart to blame them.

In my time Archer wrote the précis, but Trendall was consulted. Cowley would have taken over. The military bods simply decrypted or translated (Jac James, Pitman, yourself).

I have a feeling Trendall is wrong in saying no information went to Washington, -- on the other hand, having slept on this sentence (it is now 9/8) perhaps he was right. Certainly all our solutions went to UK, -- little came in return, either because they despised colonials or , more likely, they weren't very bright. Jap.

diplomatic ciphers would have been low down the pecking order in Bletchley.

I believe we simply worked on all traffic that was available to us, mainly thru' Mornington, but also in either late 1944 or early 1945, on traffic from an Indian station (quite a lot of 10101 stuff missed by Mornington).

To what extent our section was responsible for actual breakthroughs I am not sure. At some stage (before Smith) someone must have noticed the even-odd pattern in 10101 messages using the same passage of the cipher-book (the occurrence of the same code-group with the same cipher-group would have given sufficient "depth" of messages to see this), but who was it -- London, Washington, Eric Barnes? -- I do not know. Did Melbourne break BA thru' the unwise repeat? I think so but cannot swear it. Eric Barnes certainly solved the 10101 indicator problem. I have a memory that Trendall made a crucial contribution to the solutiion of a transposition code called "Fuji" which they used round the time of Pearl Harbour, but the details have gone.

The Jac James Kabul message would have been in BA, from memory the favoured code of the Kabul man. All non-GEAM messages would have been either 10101 or BA in your time.

I have no vivid memories of the decoded material.

In my day the number ciphers were indexed by the pattern of 1st & 3rd figures in the group (for 10101; NE had another pattern, alas! forgotten) The indexes were made out by hand & the method was considerably simplified by Eric Barnes (no time for details). The original discovery of similar groups would have been done by hand-made indexes (oh dear departed days!) It was believed UK had punch-cards & vast technological resources badly used!

I have no memory of the Bond number ritual & and your inadequate attempts to obey the master.

I suspect that you are fitter than anyone to undertake a history of what went on in the Jap. Dip. ciphers section. I fear, however, you are gravely handicapped by the disappearance of the archive, which would have given you a basic canvas on which to embroider. Lacking that, you are really obliged to rely on your own memories (remarkable, in my view, -- I am particularly impressed by the accurate reconstruction of the physical premises & the positions of the dramatis personae) and those of the other participants. All this will be pretty messy stuff. I cannot help feeling that Trendall -- top of your p.3 -- has mixed up 101001 and BA (the latter, often, by the way, needed only one message to be solved, -- the letters of common bigrams were matched & with luck the columns of the original grid were put together like a jigsaw puzzle -- one needed to know the trick with the horizontal & vertical blanks to do this successfully) and that some of the 3-hour interview will need cross-checking. Likewise with my outpouring. I would like to think that you will take on the task, but it would certainly need a visit to UK where some material from Melbourne may survive.

Your remarks about the destruction of our intelligence archives perhaps explains something that puzzled me 3-4 years ago. A volume appeared on the sinking of HMAS Sydney, written, I think, by the son of an officer who went down with her. He postulated the presence of a Jap sub to explain Sydney's failure to cope with the German raider. I found this odd, because at some time in 1945, probably before VE-Day, Eric B & I were asked to decipher a coded narrative written by the captain of the "Kormoran"(?) in a small notebook, confiscated from him in Tatura (I can see it now, -- the brand was VANA, common at the time, for notebooks and exercise books). It was a simple Vigenere substitution & gave an account in German of the battle, which I translated, --"Sydney" was deceived & came too close, -- the first shells mortally crippled her, -- it was very clear proof in my view that "Kormoran" alone was responsible. This material must have disappeared, too.

I must stop. I have written in haste, but with some consideration. We leave for 3 weeks on Magnetic Island this coming Sunday & I was anxious to let you have something before we left. We shall be back 5 September. I shall be curious to know if you go ahead with the project, but would not be surprised if you didn't. Sad that the record of all that labour is lost.

I pray that you have had a happy career and are far removed from the follies of Dawkins & his cowboys. They drove me out a year early. One day there will be a massacre of economics graduates, -- get out of Canberra before that happens.

With all best wishes,

Yours

Ian Smith

Sorry for the scrawl, --but it is better than silence.