

Annex 3. David Sissons to Ian Smith, 3 August 1990

3 August 1990

Prof I.H.Smith

Dear Ian,

Please excuse me for troubling you in your well earned retirement.

Two of my colleagues in this Research School, Prof Desmond Ball and Dr David Horner, have for some time been toying with the idea of producing a book of collected articles on the history of signals intelligence in Australia. They wish to include an article on Australian interception and decryption of Japanese diplomatic traffic during World War II. They had hoped that Professor Trendall might have felt able either to write this or to tape his recollections. But unfortunately, when approached, Trendall felt that he had more urgent, academic tasks to complete. He was, however, prepared to be interviewed and speak freely, although he feared that his recollection of those years was not good -- particularly as he had deliberately in the immediate postwar period tried to purge his memory of such matters.

The interview took place in Melbourne a few weeks ago. Ball tells me that Trendall was in excellent form and gave him a full three hours. As a result Ball is convinced that the book should contain an article on the Diplomatic Section and has asked me to try and put one together! I have said that I shall see what I can do -- on the basis of the very fragmentary archival material that has survived, supplemented by the recollections of some of the people involved. I wonder, therefore, if I could trespass on your forbearance, and plumb your memory a little.

As you are probably aware, this subject has, since the Pearl Harbor Hearings in 1946 and, more particularly, since the fairly liberal declassification of official archives in the late 1970s, become considerably less sensitive than you and I were trained to believe it would always remain. I was quite surprised when Ball in 1978 drew my attention to the enclosed papers in Department of Defence file A816 43/302/18 which he had read at the Australian Archives (Enclosure A). I was even more surprised at the publication of

the Denniston memorandum (Enclosure B). Christopher Andrew came upon this in the Archives Centre at Churchill College and, after referring it to the 'D' Notice Committee (which made no objection), published it in the opening number of Intelligence and National Security in 1986.

Archival material regarding the Section is very meagre indeed. The present Head of our Defence Signals Directorate tells me that, after extensive searches, all that his staff have been able to find is a file of the translations of intercepted Japanese diplomatic telegrams that we sent to Washington during the year 1942 and a copy of our Special Intelligence Precise for the week ending 21 December 1942. The first is in the U.S. National Archives and was declassified in 1985; the second is in the MacArthur Memorial and was declassified in 1982. He was good enough to provide me with a copy of each; but I'm afraid that they are not wildly exciting. A bit more interesting has been the war diary of our friends at Mornington, 52 Aust Special Wireless Section, held at the War Memorial. Enclosure C contains examples of the kind of information that from time to time turns up there. Among the records of the Department of External Affairs, I have come upon the files of Hubert Graves's little Political Warfare outfit in M Block. From these it would appear that Graves joined the cryptographic Section in about February 1942 and by the end of the year had been joined there by Archer. In March 1943 External Affairs requested that he be released for Political Warfare work. Army agreed that this could be done when Graves's successor, Sawbridge, reached Australia. Sawbridge arrived at the end of July; but Graves was unable to leave his cryptographic work until September 'because the enemy has recently made changes in his procedure'. In March 1944 External Affairs asked if Sawbridge, too, could be transferred to Political Warfare work; but before this could be effected he was admitted to an Army Convalescent Home with some psychiatric complaint.

Ball has given me the notes of his interview with Trendall. Essentially the story that emerges from these is as follows: Early in 1940 Trendall, at Prof Room's request, joined Room, Lyons and Treweek who, under the auspices of Military Intelligence (Eastern Command), were in their spare time (mainly at week-ends) practising cryptographic theory and techniques. During 1941 they were given some old LA traffic to try their teeth on. This they cracked without much difficulty -- without any knowledge of the Japanese language. It came in repeating patterns. The clue was the repetitive end to the sentences: YEIZ YEIZ. Trendall was taken on strength at the very beginning of 1942 when he joined Cdr Nave's outfit in a block of flats near Albert Park. There they worked on both diplomatic and Service traffic; but most of it was diplomatic. After a few months (before, he thinks, any Americans joined them) he and the diplomatic side were transferred from Nave's organisation to Victoria Barracks where they came under Army (ADMI) control. There he remained until the latter half of 1944, when he returned to Sydney University. During the whole of his time at Victoria Barracks he has no recollection of any exchange of information with Washington: it was all with the British. It was while they were at Victoria Barracks, early in 1942, that they were joined by Arthur Cooper, who, together with his gibbon, Tertius, arrived by submarine from the Philippines.

Cooper was still with them at Victoria Barracks when Trendall left in 1944. In the middle of 1943 the Japanese introduced 10101. This was a numerical code and used a grid in which particular squares were blacked out. The code consisted mainly of two-letter groups with some three and four letter groups. It was reciphered with random additives. Patterns would emerge only with sufficient depth of messages. For this, an enormous amount of traffic was needed. One prayed for 'repeats': a repeat often revealed the message. Sometimes one got a beautiful fit and could break a message in half-an-hour: sometimes one just had to slog it out. It was in Melbourne -- probably in 1943 -- that he devised the TRENCODE. The specifications were that it should be simple enough for use in the field but proof against being read by the enemy within a few hours or days. Before its adoption it was given to Treweek to test. Treweek managed to break it; but it took him a long time and he had to cheat a bit.

So much for the material that I have to go on -- supplemented by my own worm's-eye observation of the period April-September 1945. I'm afraid that I can't remember much beyond tons of very dull economic and shipping information in the telegrams that I translated (These were almost entirely GEAMs). In terms of the history of signals intelligence more interesting, perhaps, are my recollections of who were on the door-step when, as one of our lowly doormen, I answered the bell: Lt Col Sinkov (CB), Lt Col Sandford (CB), and Lt Col Treweek (FRUMEL).

I'd be much assisted by anything that you can remember about the Section and its activities. To start you off, I wonder if you could help me on the following points.

Am I right in thinking that you joined the Section before Trendall's departure? In my time, I had the impression that Cowley rather than Bond was in charge but that the day-to-day communications with Mornington, London (and Washington?) seemed to be in Bond's hands. It was Bond that did most of the chivvyng when Mornington missed particular stations; and only in the last resort would Cowley be brought into it and send them an acid signal over his own signature. It was Cowley, I think, and not Bond, that wrote the monthly *Precis*. What was the situation in Trendall's day? Which part of our suite of rooms did Trendall occupy (Enclosure D is my attempt to represent the seating plan in my day)? Did Trendall or Archer write the *Precis*? When Trendall left, which survivor (Archer, Bond, Barnes, McKay, yourself) assumed which of his functions?

A good deal has been written recently about how in Britain GC&CS (now GCHQ) recruited its future cryptographers from Oxbridge dons and the bright students that the latter recommended. You, Barnes, Bond and McKay are of that category. I presume that Treweek recruited Barnes, and that Trendall recruited Bond and McKay. But you, I think, are a Melbourne graduate; who was the talent scout in your case? What was Tony Eastway's function in the team? Did he have a similar background? I seem to remember a 'corps troops' (MG bn?) colour-patch on his hat.

I was surprised that Trendall had no recollection of close liaison and exchange of information with Washington. My impression was that, of the outwards and inwards signals that passed Bond's desk, Washington would account for as many as London. Am I

mistaken in this? Did we work with the British on one code and with the Americans on another? Was there any code for which we were, so to speak, the major player; or did we just play the minor role of covering those stations that for atmospheric or other technical reasons were more audible in Australia than elsewhere.

This brings me to a related point. I seem to remember Mornington regularly sending us machine-cipher traffic that we could not read. Why I remember this is that, during the few days between the bombing of Hiroshima and the Surrender, we, like the rest of the community, were very excited and eager to know what was happening. I can remember Bond pointing to a heap of traffic in his 'in' tray (messages to and from Sweden in machine-cipher, I think) and saying: 'The answer is in there'. Was one of our roles intercepting material for which we were not given the codes and bundling this off to those who could read them?

As I mentioned earlier, I was translating principally GEAMs. What were the other codes that the Section was working on? As well as 10101 that Trendall mentioned, I seem to remember the names, 'Bar', JBD, umiyukaba, 'Head of Mission Cipher' (in Japanese 'kanchō fugo'), and SOSOS (one of the ciphers that we could not yet read?). Could you describe any of these for me? Incidentally, I presume that, to avoid confusion, the Americans, the British and ourselves adopted a uniform nomenclature. The reason why I raise this is that, of the above names, only JBD bears any similarity to the system of nomenclature in use by the Americans at the time of Pearl Harbor. For example, the code in which the Foreign Ministry on 2 December instructed overseas missions to destroy their code-books was called by the Americans J19-K9 (J apparently stands for Japan, 19 identifies the code-book, and K9 identifies the transposition system) and by Nave and the British TU (its Japanese title).

I can remember very few messages that contained information that was either patently important, or dramatic. Only one of the telegrams that I translated fell into the former category. This was a report from a spy passing on that at the Yalta Conference Stalin had agreed to enter the war against Japan within three months of the defeat of Germany. This does not sound like a GEAM -- perhaps while Jac James was convalescing from his concussion I was translating some of the more high-grade material. I remember Jac's glorious translation of the Minister at Kabul's account of when the Afghans made him pull up the floor-boards revealing the small arsenal that he was amassing ~~up~~ (Which code would that have been?). I can remember one GEAM that contained information about the movement of POW to Japan by sea that would have interested our Chiefs-of-Staff. I remember one telegram that gave the name and address of a Japanese spy in India (Which code would that have been?) and Miss Shearer's telling me that there had been a similar telegram some months earlier about a spy named 'Bengal Tiger'. Eric Barnes told me of the sinking of a German submarine en route to Japan because the Japanese codes were being read; but I received the impression that it was not our Section that had decrypted the signal in question. Ken McKay told me that we had picked up information about the movements of the German submarine U-862 and its depredations in Bass Strait in December 1944 (Which code would that have been?). Are there any

particularly significant or dramatic telegrams that you can remember?

Were there any particular triumphs in the field of cryptography that the Section had to its credit? Eric Barnes told me of some long battle that Trendall and Archer (or was it Graves) had with a system of bigrams, at the end of which one announced victory to the other in a letter commencing: 'Myves Gradear', or words to that effect. This sounds a little like a GEAM.

Lastly, could you please have mercy on me and explain to this mere translator the implications of what, I understand, is one of the most basic of the axioms underlying the craft -- that one can begin to read a message sent in a reciphered code (for which one has neither the reciphering tables nor the key to the 'indicator' that tells the recipient which page of the additives to use) only when one has access to another message in which the same stretch of reciphering tables is used and several of the same code-groups appear over the same additives in both messages. For example, taking a four-figure code, one needs something like the following:

Message 1	Code-groups	4416	2089	1526	9734	5771
	+Additives	9046	7127	8168	3072	8643
	=Signal	3452	9106	9684	2706	3314
Message 2	Code-groups	7298	1492	1526	9090	5771
	+Additives	9046	7127	8168	3072	8643
	=Signal	6234	8519	9684	2062	3314

In other words, it is by observing the same figures 9684 and 3314 separated by the same distance that the ball is set rolling. This seems logical enough. What I want to know is how on earth you managed to do this time and time again in practice. So far as I can remember, you had no punch-cards, computers, or adding-machines to assist you. Surely you didn't just go through hundreds of past signals at random until such a similarity appeared. What was your system of filing past messages? Perhaps a ritual that we indulged in from time to time is part of the explanation. All hands were called to the pumps and, like some card game, Bond dealt each of us a hand. He then started to read aloud a series of numbers which we each tried to follow in the document before us. Frequently this would get out of hand -- one would find oneself lost and shout out 'I'm off the rails'. Whereupon, Bond and Barnes would become furious. What was this all about?

How did the Japanese construct the 'indicators' and how did anyone ever manage to break them?

It seems to me completely inappropriate that I, the most junior and a very transitory member of the Section, should be asked to undertake this article. If anyone else with the time and the inclination wishes to do it, I'd be only too happy to make way. About three years ago the present Head of the Defence Signals Directorate approached me and put out feelers as to whether I should be interested in writing an in-house history of the Directorate since 1939. Someone in khaki produced such a volume

about ten years ago; but apparently they are not satisfied with it. I didn't rise to the bait --for a number of reasons. First, I had more urgent things to do. Secondly, the archival back-up that they offered appeared very amateur and haphazard. Although they were well acquainted with F.H.Hinsley's volumes on signals intelligence in the European theatre (British Intelligence in the Second World War: Its Influence on Strategy and Operations, London, HMSO, 4 vols, 1979-88), they seemed unable to appreciate the extent of his reliance on extensive, well organised records and well trained registry staff. In Australia the care of our signals intelligence records appears to have been entrusted either to sleuths or quartermaster-sergeants who made great bonfires of intercepts, registers and all in the late 1940s. Hinsley is of the opinion that most of the material that we sent to London by bag or signal would have survived. But our DSD didn't seem to be thinking in terms of sending the historian on visits to London and Washington. But a more important factor was that, as one who had, during the passage of the Australian Archives Bill, said a good deal in professional journals and in testimony before Parliamentary committees about 'open access', I didn't feel that I could participate in the writing of a secret in-house history. They eventually signed a contract with Peter Hastings (who served in Central Bureau during the War) to do the job for \$100,000; but he threw in the towel after a few months. He found that my fears about lack of expert archival back-up were all too well founded.

I do apologise for burdening you with a letter of such length. Any help that you may be able to give me will, I assure you, be very greatly appreciated.

With very best wishes,

Yours sincerely,

D.C.S.Sissons

Encl: 4