SYDNEY UNIVERSITY, T.G. ROOM AND CODEBREAKING IN WW II

Peter Donovan (School of Mathematics, UNSW) and John Mack (School of

Mathematics and Statistics, University of Sydney)

[This is substantially the contents of a two-part article published in the *Gazette of the Australian Mathematical Society,* 2002.]

Introduction.

Thomas Gerald Room (1902-1986), FRS and FAA, was Professor of Mathematics at the University of Sydney from 1935 to 1968, succeeding H. S. Carslaw. He was one of the founders of the Australian Mathematical Society and one of its early Presidents, as well as being the first Editor of its Journal.

At the time of his death in 1986, very little factual information on military intelligence work in WW2 was available, except for some books and articles on Bletchley Park in the UK and its work on the German Enigma codes. In the obituary notice written for the Royal Society in 1987, the following extracts summarise what could be gleaned at that time:

" Arrangements were made early in 1941 for a small group at the University of Sydney to study Japanese codes. They were Room (as leader, his colleague Lyons and two members of the Greek Department, A. D. Trendall and A. P. Treweek. In mid-1941, the Australian government set up a cryptographic analysis unit at Victoria Barracks in Melbourne. Its job was to work on the deciphering of Japanese diplomatic codes. The Sydney group was recruited into this unit by an intelligence officer, Captain T. E. Nave, the University of Sydney having agreed to its secondment to the Defence Department. Room was a senior member of the unit. Later in 1941, he went to the British Far East Combined Bureau in Singapore to gain experience in British code-breaking methods. A letter to the Registrar of Sydney University, Walter Selle, on Christmas Eve indicates that he had been hard at work learning Japanese: The two terms I have spent under Miss Lake have proved as useful in my present job as the twenty years mathematics!."

" the unit devised codes for the coast-watchers. Room was among those who took part in this work."

" When General MacArthur set up his headquarters in Brisbane in 1942, , a joint signal intelligence section, called the Central Bureau, [was formed] in conjunction with it. Room was transferred to [it], where he worked until the end of the war on the decoding of Japanese military signals. His work was described as spectacularly successful."

Release of further information

Over the past decade in particular, a number of official military and government archives, formerly classified as secret, and dealing with intelligence activities against the Japanese, has become available for examination. In addition, several books devoted to intelligence activities focused on the Pacific/Asian war zones have been published using some of this new material as well as information derived from persons who worked on aspects of codebreaking at that time. While some of the material published appears to us to be based accurately on available evidence, this evidence is incomplete and inconsistent. Thus, some facts remain incorrect and in general very little has been published that is directly relevant to Room.

We have devoted time to establishing the facts and then to sifting anecdotal and other evidence in order to produce as comprehensive a report as we can, and our intention is to place this soon on a website for ease of access. In this brief account, we shall summarise our findings and identify the principal remaining enigmas. In our opinion, everything so far written about events in the first half of 1940 remains somewhat speculative.

1. Sydney University 1905-1940

Less obvious, but apparent upon reflection, is the question: why was the University of Sydney the key university player in these cryptographic efforts, when the Defence Departments were primarily located in Melbourne?

On this point, we believe we have a rational explanation, deriving from the very long association that existed between the Commonwealth Department of Defence and the University of Sydney and which in fact extends back into the early years of the twentieth century. It had its beginnings in the establishing of the subject of Military Studies at the University of Sydney in 1906, with some government support, after other universities had declined to do so on financial grounds. This subject area continued to be offered until 1916, when the effects of WW1 forced the withdrawal of the key military officer from university duties to duties within the General Staff.

This aspect was not the principal underlying linkage in our view, but merely supplied the basis for a subsequent recommendation in 1917. The then Director of Military Intelligence, E. L. Piesse, suggested that the teaching of Japanese to cadets at RMC Duntroon be disguised via the establishment of a lectureship in Oriental Studies at the University of Sydney, supported by an annual grant from Defence. In this way, James Murdoch became (after a prior appointment at a lower level), in 1919, the first professor of Oriental Studies in the University, and an annual grant in support of the teaching of oriental languages continued to come to the University from Defence until 1948!

The terms of Murdoch s appointment required him to teach cadets at RMC and also to spend some time each year in Japan (is this the first case of Commonwealth funding supporting an academic s study leave program?). He was well connected in Japan and able to obtain for Piesse intelligence information on topics such as Japan s foreign policy and business directions, with his academic position providing both a rationale and a cover for his activities.

One of the RMC cadets, (later Captain) Capes, continued in the Army after 1918 and was responsible for identifying a naval cadet, Eric Nave, with considerable linguist talent. Nave had

studied Japanese privately and was sent to Japan for two years by the Navy to develop his skills.

[The National Archives of Australia [NAA] has a Recordsearch facility available on its web site; searching under `Capes Nave reveals this most important development.]

Unfortunately, Murdoch was in poor health and he died in 1921. His successor to the Chair, Sadler, does not appear to have had Murdoch s interest in language teaching or his Japanese connections, but he was still required to

provide language teaching to military cadets. Sadler took study leave in 1935 and a Miss Margaret Lake (mentioned by Room in the letter quoted above as having taught him Japanese in 1940) was seconded from the Teachers' College to provide this teaching in that year.

Further information about the teaching of languages in the services is held by the NAA. By the late 1930s, it shows that Melbourne University was interested in coming to the party and even in displacing Sydney as the provider of Japanese.

The official history of the University of Sydney mentions the development of what is now called the Sydney University Regiment from around 1900. The commandant throughout most of the 1930's was Victor Windeyer, later a Major-General and a judge of the High Court. At the time he was a barrister and a part-time lecturer in legal history. A prominent member of that regiment was A. P. Treweek, a lecturer in classical Greek who had studied both Greek and Mathematics for his Honours BA degree. Treweek was much later to obtain a PhD from the University of London on the corrections needed in the surviving copies of the writings of the ancient Greek mathematician Pappus of Alexandria. Treweek thus was well acquainted with R. J. (Dickie) Lyons [see below], a long-standing member of the Mathematics department.

Eric Nave (born in 1899) joined the Australian Navy [henceforth RAN] as an RMC cadet. As already noted, the RAN sent him to Japan in February 1921 to master the language and he did extremely well in an examination set by the British Embassy in 1923. A British naval officer, Harry Shaw, was in Japan at the same time for the same purpose and had returned to Britain. Shaw had been transferred to the British decryption agency, the Government Code and Cypher School [GC&CS] and appears to have mentioned to Nave to his superiors. The British Navy [henceforth RN] asked for Nave to be transferred to a British ship, HMS Hawkins, working off the coast of China. His task was to work on Japanese coded material. Nave was given rank in the RN and worked on Japanese codes thereafter both in London and Hong Kong. Remarkably, he worked around 1930 with Victor Windeyer's cousin, Guy Windeyer, who had joined the RN as a cadet in 1914. Guy Windeyer had retired from the RN in 1933 and took up farming on Vancouver Island not far from the Canadian Pacific Naval base of Naden. He joined the Canadian Navy in September 1939 and spent some 15 months at Naden, presumably working on interception of radio messages, before being given command of a warship in the Atlantic Ocean.

Enoch Powell, later a British Cabinet Minister, had been appointed Professor of Greek at the University of Sydney in 1938. However he resigned at the outbreak of war to join the British army. Dale Trendall was then offered the Chair and took up the position around October 1939. His interests were in archaeology, particularly vases from the Greek community in Southern Italy of vintage around 350BC. Trendall later became Master of University House, Canberra and then moved to LaTrobe University. A gallery of ancient artifacts there is named after him.

2. Dickie Lyons

The next two paragraphs are extracted from the anonymous obituary of Richard Jenkins Lyons published in *The Medical Journal of Australia* on 22 March 1952.

" The University of Sydney is the poorer for the death on November 13, 1951, of Richard Jenkins Lyons, Senior Lecturer in Mathematics and Reader in Geometry. Richard Lyons was not only one of the university's ablest scholars, but one of its most loved and respected teachers. Educated at the Sydney Grammar School, he came up to the University of Sydney in 1903, with the entrance scholarship for mathematics. In 1906 he graduated with first class Honours and the University Medal. Two years later he was awarded a travelling scholarship to Cambridge and entered Saint John's College in 1908. He became a wrangler and Fellow of Saint Johns College. "

"After his return to Australia he became Lecturer in Mathematics and later Reader in Geometry in the University of Sydney. During the Second World War he was appointed to the Department of Naval Intelligence in Melbourne. For this work he learnt Japanese with remarkable speed and efficiency. His superior officer in the service has written not only of his work but of his `incurably merry manner' and of his `strength of spirit'. Throughout a busy life he found time to keep abreast of modern developments in Mathematics: in particular of the work of Professor H F Baker of the University of Cambridge. His work was mentioned and acknowledged in volumes II and III of Baker's *Principles of Geometry*. From time to time notes and papers, some in collaboration with others, appeared " ."

A report in the archives of the University makes it clear that the "superior officer" referred to above was Commander Nave [see above and below], the first Australian to work on Japanese codes. Nave wrote the private testimonial in November 1942 in the circumstances described in section 13 below. (In fact, Lyons was not appointed to the Naval Intelligence Department, but worked in Special Intelligence Bureau.)

Lyons took sabbatical leave in Cambridge "to work with Professor Baker" in 1933. It would appear that, during this time, he played some role in making the University of Sydney attractive to another student of Baker, that is T G Room, who accepted an invitation to become Professor of Mathematics at the University in 1935. Room's book, *The Geometry of Determinantal Loci*, was published in 1938. Its Introduction notes that Lyons had made a major contribution in the preparation of the book for publication. (A photograph survives of Dickie and Hilda Lyons on camels at the Pyramids en route either to England or Australia for that leave. Another photograph, published here for the first time, shows the Lyons with Room and two children at a picnic in 1936. Thanks are due to Mrs Barbara Cathers of Lindfield for the photograph; she and her brother, Ian Stafford, were the two children present in it.)

3. **The Secrecy**

The GC&CS was the successor of naval and military decoding groups operating in the First World War. The secrecy of these operations had been destroyed by the publication of a book in 1932 by Hugh Hoy, entitled *40, OB, or How We Won the War*. Likewise the American efforts had been compromised by the publication in 1931 by Herbert Yardley of *The American Black Chamber*. Indeed, the secrecy imposed on Second World War cryptologists must have been partly in reaction to these books. The University of Sydney Library still has a copy of the Yardley book obtained in the 1930s. Thus, although it is possible that Victor Windeyer had some knowledge of what his cousin had been working on for the RN, it is by no means certain that this was the case. Likewise it is unclear to what extent Richard Windeyer, father of Guy and a prominent member of the University

of Sydney Senate, knew anything about the work on Japanese codes being carried out by the RN.

Another coincidence must be mentioned here. A fellow student of Baker, Gordon Welchman, had been placed on the emergency list for GC&CS in 1938. Welchman's book, *The Hut Six Story*, is recommended and states that he was the second mathematician (after Alan Turing) into Bletchley Park in 1939. Bletchley then became the base for most of the activities of a rapidly expanding GC&CS. Welchman showed considerable initiatives at Bletchley in both technical and organisational matters. Welchman must have known Room at Cambridge. It is possible that the Australian Navy and or Army had sought advice from Britain about how to enter the decryption business and had been advised to seek out academic mathematicians. It is also possible that Room had been mentioned by name in such a message. However this is speculative.

4. **Intercepting**

The invention of radio made it possible to communicate long distance by Morse code. This was open to interception, so various enciphering methods were needed. This created military problems:

(*) Radio communication gave immense advantages; but

(*) The interceptor could use direction-finding apparatus (twice) to locate the sender;

(*) The individual radio set could be identified by certain equipment secretly brought in by the British for WW2;

(*) The style of tapping out Morse varied from person to person like handwriting so the operator could be identified, even if not by name;

(*) The quantity of information sent could be observed;

(*) Perhaps the identification of the desired recipient might be possible even if the full text could not be interpreted.

An Australian Army group operating near Tel Aviv in 1940-1941 became expert in `traffic analysis'. They came back for the Pacific war and so were able to be of great assistance in 1942-1945. They ended up working for Central Bureau.

Long-distance Japanese messages were intercepted in Hawaii, British Columbia, Washington State, Australia, Ceylon and India.

5. **American Cryptology 1929-1941.**

In 1929 the then American Secretary of State closed the "Black Chamber", as the code-breaking group was called. In retaliation, its head, Herbert Yardley, published a book [already mentioned] on America's cryptology system. William Friedman then started a new interception and decryption organisation for the United States Army. This resulted in the creation of the Signal Intelligence Service in 1930 and the appointment to it of mathematicians Frank Rowlett, Abraham Sinkov and Solomon Kullbach. John Hurt was added to these three on the basis of his knowledge of Japanese. Sinkov and Kullbach got PhD's in Group Theory and Statistics respectively in the 1930's. The SIS had 17 personnel in September 1939 and 331 in December 1941. There were over 10,000 by the end of the war, including over 2,000 in Central Bureau [see below]. Rowlett played a significant part in the breaking of the key Japanese diplomatic code known as `Purple'. Kullbach, who is also remembered for key work in Statistics, ran the big US Army decryption base at Arlington, Virginia, for much of the war. Sinkov was sent to Bletchley Park early in 1941 to swap the Purple decryption device for information about the German Engima machine, and later ended up in Brisbane as commandant of the American element in Central Bureau.

The US Navy developed its cryptology group OP-20-G from the 1920's. Bainbridge Island, an American Island near Vancouver Island, was an interception base. Considerable progress was made in tackling JN25, the predecessor of the main naval code JN25b, before the Pearl Harbor raid of December 1941.

6. Classic decoding

We consider the Rosetta stone, now in the British Museum. It contained writing in three ancient languages, one of them (Greek) generally known to those interested in ancient Egypt, one being the hieroglyphs and the third being a latter-day adaption of hieroglyphs. It was reasonable to conjecture that the three texts said the same thing. A remarkable achievement was to use this `crib' and the massive quantity of other hieroglyphs to read essentially all ancient Egyptian texts. Cribs came into their own in the codebreaking activities of 1900-1950.

A standard non-mathematical trick used for decoding is the `pinch', that is obtaining information about the other side's codes and ciphers by armed force. This was done by an Australian Army group at Tel el Eisa near el Alamein in 1942. Another standard non-mathematical trick used is the `find'. Inevitably code and cipher material used in the field will end up getting mislaid, though the find at Sio (East New Guinea) early in 1944 was much more than anyone had reason to hope for. [It was a steel box containing the code and cipher library of a retreating Japanese division. It had been buried in the mud near a place where a stream was crossed and was found by a mine detector. It went to Central Bureau in Brisbane, and then copies were passed on to Arlington Hall near Washington.]

The well-known book by Chadwick *The Decipherment of Linear B* tells how Michael Ventris, who had previously worked at Bletchley Park, had interpreted the ancient writings from Crete after the end of World War 2. It is interesting to note that after a paper had been published challenging the validity of Ventris' work, Treweek wrote a reply that hinted at his experience in other decoding work. See the *Bulletin of the Institute of Classical Studies of the University of London* for 1957.

7. Japanese codes

There were numerous of these of differing levels of complexity. For example JN25, the main naval code in 1940, assigned to each word or letter in a codebook a 5-digit number divisible by 3. Thus perhaps Mexico is represented by 67893. This would be issued to all units. A table of random digits would also be issued together with rules for how the cipher clerk chose a starting place in it. Alternatively, the starting place could be encrypted into the message itself. The plain text was thus encoded by the code book and the appropriate segment of the random sequence added working modulo 10 in each place-no "carrying" was performed. The digital message then went over the air-waves. Thus the decoder had to (1) strip away the `additive'; (2) build up the code book; and (3) translate from Japanese into English. Other codes were used with 3-digit code words, still others with 4-digit code words. Various other

twists were introduced at various stages; see the report by Eric Barnes (1945). The codebreakers would seek to mechanise as much as possible the operations (1) and perhaps (2). This leads us to the problem of what could be done with the IBM tabulator of the time when an enormous supply of cards for punching is available and an essentially unlimited supply of female clerical assistance may be used. It seems most unlikely that the Japanese appreciated at the time the potential of mechanical assistance in stripping away the additive.

[Note that diplomatic codes were quite different; the Purple code was for diplomatic messages only and was broken by a specially built machine whose design was deduced from patterns in the messages. As already noted, this was achieved by an American Army team led by mathematician Frank Rowlett. It was used in 1941 for messages to the embassy in Washington. Lower level codes were used for messages to the consulates in Australia. Conveniently Purple was used throughout the war for messages from the Japanese embassy in Berlin to Tokyo: as Ambassador Oshima had access to the right people and even inspected the defences in Normandy his messages were well worth reading. See the letter from General Marshall to Governor Dewey in October 1944 asking him not to mention codes in campaigning for the American Presidency. References for this include B5555/2, a very detailed report on the Australian section in FRUMEL and another report apparently put together by Eric Barnes on the diplomatic code group in Melbourne. Anything in the postwar literature on this or any other aspect of Japanese codes should be treated with considerable caution.]

8. The situation in 1939

At the start of the European War in September 1939, Nave was working at FECB, the British radio interception unit at Singapore. This was later to secretly co-operate with the American Navy group in the Philippines. The Director of Naval Communications, based in Melbourne, was Commander Jack Newman, who was under no illusions as to whether Japanese Naval Communications should be monitored. The Director of Naval Intelligence, Long, is the subject of Barbara Winter's book *The Intrigue Master*, and had direct contact with his opposite number in London. The RAN had liaison with the FECB and also with the Dutch intelligence unit called Kamer 14 in Bandung. At some stage thereafter Room, Lyons, Trendall and Treweek formed a working group to gain experience with codebreaking. The details are rather obscure and likely to remain so unless the records of the British Director of Naval Intelligence or the records of the Sydney branch of military intelligence yield some new information. The following section is an attempt to work out what happened. Speculation about the role of the Windeyer family and speculation about suggestions being made by Welchman to the Australian military must remain speculations. The two key NAA files are the `Navy File MP 1185/8 1937/2/45 *Establishment of a Cryptographic Organisation in Australia* and the Army File A6923/3 37/401/425, which may be located by asking Recordsearch to look for Room Treweek. Other sources are the interviews conducted with Trendall and Treweek by journalist David Jenkins, Canberra academic Desmond Ball and former codebreaker David Sissons of Canberra. These interviews indicate that Trendall and Treweek entered the project rather later than Room and Lyons.

9. The Sydney Initiative

Document 318 from the Army File is a submission from the Director of Naval Intelligence dated 25 November 1939. It suggests that the British authorities be asked for advice on whether a cryptographic organisation should be established in Australia. It states that for some years prior to the commencement of the war every effort has been made to locate cryptographers, but apart from one or two amateurs who are obviously of no value unless trained, no professional cryptographer has been located. It has been suggested that the reference to amateurs means Room and Lyons but this seems quite unlikely.

However file A 816/1, item 43/302/18 contains a minute by Nave of 12 November 1941 stating that the General Staff had founded (about the middle of January 1940) a small cypher section at Sydney University. This appears to contradict information in document 313 of the Army file, which consists of notes of a meeting of the Defence Committee on 15 February 1940. Document 311 of the Army file is a letter from then Prime Minister Menzies to the British Government and dated 11 April 1940. These indicate that nothing had been done by the Defence authorities to that date. But the date of January 1940 for a start by Room and Lyons remains plausible. It gives reasonable lead time for the group to have developed the skills mentioned in Document 298 of the Army file, dated October 1940,viz: "The work of the cipher-breaking group continues and that exceedingly good results are either anticipated or in view.". Document 279 of the Army file consists of notes of a meeting held in Melbourne in May 1941, with Room and Treweek present. It states: " Appreciation was expressed of the progress made by the unofficial Sydney group, which started without any assistance." [The official notes of this meeting refer throughout to Professor Roon and Major Treweeke. This double mis-spelling suggests that those present from Melbourne were not well-informed of the composition of the Sydney group.]

Interviews with Trendall and Treweek by Ball, Sissons, and Jenkins make it clear that Room and Lyons were the initial members of this group. The cycle of University work, with examinations in November/December, supports a starting date of January for the group.

Among the various scenarios that may be proposed for the stimulus that led to the formation of this group, one is that Welchman suggested that Australia copy the Bletchley mixture of mathematicians and linguists. Another is that the Army decided to approach the one university possessing some capacity in Japanese and/or with some special connection to the Military. A third is that Victor Windeyer, independently, suggested that something be done.

Document 298 also states that, by October 1940, work had been concentrated on an attempt to break down the Japanese commercial and diplomatic codes by reducing the cipher groups to a Romanised Japanese text, which could then be read freely by Japanese interpreters.

10. The return of Nave

Eric Nave returned to Australia on sick leave in February 1940. He had been working for the RN in Singapore at FECB, which effectively was a specialist branch of the GCCS. Later that year, he attempted to set up a decryption group for the Naval Intelligence Department in Melbourne. He had great difficulty finding suitable staff for this. By early 1941, he had become aware of the Sydney group and visited them. This resulted in his instigating the May 1941 Melbourne meeting mentioned above.

Since this meeting resulted in a crucial alteration to the status of the informal Sydney group, and to the subsequent roles of its members in Military Intelligence in World War II, it is appropriate to quote below the full text of the minutes of this meeting.

"D.D.M.I. SECRET

NOTES ON CONFERENCE 2/5/41 1200 hrs.

1. Attendance.

NAVY Commander Long, Commander Nave.

ARMY – Col. McKenzie, Lt.-Col. Edwards, Major O'Connor, Capt. Fleiter.

From Sydney – Professor Roon, Major Treweeke (*sic!!)*

2. After informal general discussion Col. McKenzie withdrew. Commander

Long intimated that the Navy already had a nucleus section functioning, and he then withdrew. Lt.-Col Edwards outlined position relative to interception of traffic, and stated he was available at call on any matters of a technical nature.

3. Discussion then ensued on the work already done by Professor Roon and Major Treweeke in Sydney.

4. . It was considered that-

a. the breaking of Japanese diplomatic codes could be regarded as a feasible proposition;
b. that it was desirable that a section for this purpose should be organised – it being considered that existing facilities at Singapore may not always be available;
c. the present strength of this section should be four officers and three clerks additional to the existing Naval nucleus organization. One officer to be a competent Japanese linguist;
d. the section should be of a combined service nature, for the benefit of all services. Although initially the work would mainly be concerned with naval codes.

5, Commander Nave considered Professor Sadler to be the only suitable Japanese linguist for the work. Doubt was expressed as to whether he could be available, but it was thought that discreet enquiries should be made and that he should be approached in this regard.

3. Professor Roon and Major Treweeke *(sic!!)* were willing, subject to the concurrence of the Sydney University authorities, to undertake the work, and come to Melbourne for this purpose. It was thought that Mr. R. J. Lyons of Sydney University could also be made available if necessity arose.
4. The future of the unofficial Sydney section was mentioned, and Commander Nave expressed the view that this would lapse, if most of the members came to Melbourne.
5. Appre ciation was expressed of the progress made by the unofficial Sydney group, which started without any assistance.
6. Professor Roon and Major Treweeke were anxious that they should have the earliest practicable advice if their appointment in Melbourne were decided upon, in order that private and University affairs might be arranged. The current University term concludes about the end of May.
7. If the Section remains as at present, in Sydney, there is sufficient material obtained through Eastern Command, for them to work on.
8. The detailed discussion on the work carried out by Professor Roon and Major Treweeke and confreres, was left to these gentlemen and Commander nave, subsequent to the conference.

(Signed) J.C.W. O'Connor Major G.S. (M.I.) 5/5/41. "

11. The move to Melbourne

Commander Nave, in his personal memoir lodged with the Australian War Memorial in Canberra, writes of the period from his return to Australia in 1940, until the formation of what became known variously as the Melbourne Communications Intelligence Unit or the Special Intelligence Section, as follows:

" Perusal of the files gave little cause for optimism, and I then went to Sydney. The Military Intelligence people had told me that M.I. Sydney had a small group at the University who were studying Japanese cable messages. This showed most commendable planning by the Army and also an excellent spirit on the part of the University staff who gave their time in the interests of the country.

" I met the gentlemen concerned; they were Professor T.G. Room, a distinguished mathemetician *(sic)*, Richard Lyons, mathemetician, Professor Dale Trendall, a linguist of many talents, and A.P. Treweek, from the language area. All agreed to come to Melbourne and the necessary arrangements were made by the Army with the University."

[It is worth noting that the Military was prevented from any earlier formal setting up of an Australian Cryptographic Intelligence Unit, which it had suggested in 1939, by the then Prime Minister, Menzies, who felt that the British would be able to supply all intelligence needed. He wrote to the British in April 1940 seeking their advice and did not receive a reply until late in 1940. Following that, Nave was able formally to create a very small unit in Melbourne early in 1941. It included Lieutenant Jim Jamieson.]

Treweek, already a Major in the Militia, by virtue of his association with the Sydney University Regiment (then part of the Militia), was the first to report to Melbourne, in mid-June. Some negotiation over the proper rank and pay for Room eventually led to an agreement whereby Room retained civilian status, the title of Professor, and his professorial level pay. (He became the sole civilian member of the ultimately 4,000 strong Brisbane-based Central Bureau!) He and Lyons took up duty in mid-August, with Professor Trendall following later, in January 1942.

The immediate consequence of this was that, by late August 1941, Australia had in Melbourne a viable nucleus for a cryptography group, led by Commander Nave. Within a few weeks, Room and Lieutenant Jamieson were sent to Bandung (Java) to study the techniques used by the Dutch (Kamer 14) and to Singapore to study the work of the British at FECB - the Far Eastern Combined Bureau. This was an arm of the London-based Government Code and Cipher School (GC&CS), as was Bletchley Park.

FECB had been, since January, working secretly with a U.S. Navy unit in the Philippines, and had become well aware of the value of tabulating machines in codebreaking. Thus Singapore probably was the site of the first meeting between an Australian academic and an effective tabulating device. A very significant observation is that the Japanese appear to have remained unaware of the effect of utilising machines of this kind, together with a massive intelligence and clerical effort, in breaking a range of military and other codes, often in a very short timeframe.

12. The Pearl Harbor Raid, 7 December 1941

The Melbourne unit was able to pick up and decipher the diplomatic coded message sent from Japan on Tuesday 2 December ordering that the Consulate in Melbourne burn all documents relating to codes or coded messages. Nave was able to warn the Navy that war was likely, probably starting at the weekend. The U.S. Navy had a liaison officer in Melbourne. No aggressive act had occurred in Asia, or in the Pacific anywhere West of the International Date Line, on Saturday 6th, or at dawn on Sunday 7th. It is remarkable that this fact was not interpreted anywhere as a strong indication that something might happen at the principal worthwhile target East of the dateline 18 hours later!

13. 1942

The early months of 1942 were chaotic both for the citizenry and the military alike. As the Japanese advance forced continual evacuations, the U.S. Naval Intelligence unit from the Philippines was brought to Melbourne, while the British FECB Singapore group retreated first to Ceylon and then to Kenya. General MacArthur moved his HQ to Melbourne after evacuating the Philippines and the American Army sent cryptography staff to Melbourne, forming a group given the name Central Bureau (CB), operating initially from a large domestic house. Its somewhat absentee commandant was the American General S. B. Akin. The initial commandant of the American section was Colonel Sherr, who died in an accident in 1943. Following this, Major Abe Sinkov, a key figure in the history of military intelligence, took over (see also below). CB absorbed traffic analysis and radio interception units fairly rapidly.

The Navy unit was named FRUMEL (Fleet Radio Unit Melbourne) and worked initially in a block of flats, which also housed Nave's group. (For photographs, ask Google to search for 'FRUMEL Monterey'. The Monterey building is still standing in Arthur Street, South Yarra.)

The initial important successes came from naval intelligence, in collaboration with other such units in Hawaii and Washington DC. Enough intelligence was obtained about Japanese intentions to invade Port Moresby from Rabaul to lead to the Battle of the Coral Sea in May, and separately to lead to the Battle of Midway in June. It is clear, in fact, that Treweek gravitated fairly quickly towards naval intelligence, because his wife, Mrs Hazel Treweek, recalls his coming home on the day of the Battle of Midway, saying "I cannot tell you more, but we have just won the war!". Some firsthand evidence of the Melbourne involvement in the Midway intelligence coup may be found on pages 80-81 of the Maneki book *The Quiet Heroes of the Southwest Pacific Theatre.*

14. November 1942

Nave had maintained regular communication both with Central Bureau and with FRUMEL, and it seems that this was a factor in the development of a worsening relationship between him and Commander Fabian, the head of FRUMEL. This is suggested, because there was a lack of trust between U.S. Naval intelligence and other intelligence units of the U.S. Military evident even prior to the outbreak of the Pacific war. This extended to include British codebreaking units at Bletchley Park and elsewhere in the GC&CS network. For example, Smith, in his book *The Emperor's Codes*, writes on page 151: " The Americans also insisted that the naval section of Nave's unit be totally absorbed by Fabian's FRUMEL; that Nave, an Australian, 'be sent back to Britain';' .".

There are two contemporary documents which indicate the level of tension in Melbourne at this time. In a memo written to the Director of Military Intelligence late in October 1942, Lt. Col. Little, who appears to have been in charge of Nave's unit at that time, writes: " My feeling is that since the advent of the U.S.N. Crypto Sec under Lt. Comdr. Fabian Army have not been treated fairly as although Army provided about 1/3 of the staff and all the intercepts all Army was allowed to have was a precis of the diplomatic material. More recently we have been permitted to read through in the presence of a M.O. some of the diplomatic messages that Comdr Nave was good enough to pass to us. These were taken away as soon as read." This memo is to be found in the 319 page 'Army file', obtainable from National Archives Recordsearch by asking for 'Room Treweek' and then asking for the digital scan.

Lyons, writing to Vice-Chancellor Wallace of Sydney University on 19 November, to inform him of receipt of the Vice-Chancellor's decision that Lyons should return to the University, includes the following: " However, before Commander Nave, the Head of the Bureau, left, I had the satisfaction of receiving from him what may be called a contingent invitation to go to the Foreign Office. When the decision was made to transfer control of the Office to the Americans Commander Nave told Room that if he were willing to go to London he could get him placed at the F.O. I was not surprised to hear this, because Room's intellectual power is phenomenal, but I was exceedingly gratified when he announced that the offer included me, adding that this was for my part in some rather spectacular success we had had earlier in the year. Room's immediate reaction was to accept enthusiastically, and for one thrilling morning I thought we were in for the super experience. However, when Room had weighed all the pros and cons of the proposal, he decided that much though he would have liked to go to London, his gifts could be used more effectively in Australia, and the invitation lapsed."

The GC&CS was called either 'The Foreign Office' or 'London' at the time.

The British Admiralty had been requesting the return of Nave to the Royal Navy but accepted the return of other British personnel instead. It seems clear that the Australian military did not want to lose the use of Nave's unique experience in handling Japanese codes. Thus, if he could no longer be used in Melbourne, transferring him to Central Bureau was the obvious thing to do. Presumably either on Nave's recommendation or on the basis of known ability and achievement it was decided to send Room to Central Bureau too. As noted above, Lyons, who was much older, returned to Sydney University.

15. The Road to 1943

After a few months in Melbourne**,** MacArthur moved his headquarters to Brisbane. Central Bureau followed, moving initially to the large house at 21 Henry Street, Ascot (this is still standing but is now a private residence again) and then taking over Ascot Park as well. Henceforth, Central Bureau is abbreviated to either CB or CBB.

Some account of the career of Abe Sinkov is needed here. He joined the American Army as a civilian cryptographer in the early 1930's and earned a PhD in finite group theory on the side. He published papers from this work in the *Annals of Mathematics* and the *American Journal of Mathematics* in 1937. At the invitation of H. S. M. Coxeter, he rewrote the chapter on codes in the 1939 new edition of Rouse Ball's *Mathematical Recreations and Essays*, first published 50 years earlier. In January 1941 he was sent to Britain to exchange the American device that decrypted material in the Japanese 'Purple' cipher for the technology that broke German 'Enigma' messages. He was given full access to Bletchley Park. The high point of his career appears to have been the work of CB in Brisbane during the war. Afterwards, he continued working with military cryptography, finishing in the present-day National Security Agency. This is believed to be the biggest employer of mathematicians in the world.

Despite the adverse opinions of Nave held by some elements in the U.S. Navy, his work in CB was greatly appreciated by the U.S. Army. His competence has been attested to us by certain veterans of that era.

16. Trendall, Treweek and Barnes

Trendall remained in a small diplomatic cipher group in Melbourne that eventually took on Eric Barnes. Barnes had been studying Mathematics and French at Sydney University and graduated early in 1943 with first class honours in both. It is likely that Trendall had identified him as a good prospect for codebreaking, because he was assigned to the Melbourne unit almost immediately upon his enlisting for military service. After the War, he obtained a PhD in

Number Theory at Cambridge and then returned to the staff at Sydney prior to his accepting a Chair at Adelaide in 1959. The 319 page "Army file" (see section 14 above) gives significant information on Barnes' wartime career.

Indeed, pages 46-48, dated 30 April 1943, show that Barnes was then one of three cryptographers, of whom Trendall was the senior, in a small Diplomatic Codes group. A document of the 3rd January 1943, which is pages 93-96 of the file, is a request to the Director of Military Intelligence that one additional person with special skills be appointed to the group as soon as possible. As Barnes was not part of the group in January, he must have been the person chosen.

The true magnitude of Treweek's work in codebreaking is recorded in file B5555/2, held at the National Archives Office in Melbourne. This extensive file, to which Treweek himself was a major contributor, lists the significant achievements of the Melbourne group as well as giving quite detailed information on the nature of the work undertaken.

The best accounts of Trendall's work known to us are those by R.S. Merrillees (Working Paper No. 355, Strategic Defence Studies Centre, ANU, January 2001) and a contemporary document, apparently written largely by Eric Barnes, located at the NAA as Item 1 of A6923/2. It is entitled *Japanese Diplomatic Cyphers: Cryptographic Survey, being a report of the Special Intelligence Section, HQ Australian Military Forces, 1946*. This gives a list of personnel involved and thus provides the Australian mathematical community with some hard information on Barnes' career in cryptography.

17. Central Bureau in 1943

So, at the end of 1942, Room and Sinkov were the two senior mathematicians at CB in Ascot. This was developing into becoming the Australian version of Bletchley Park, with huts, interception bases (Darwin, Townsville and others), and communication with the American Army cryptographic headquarters at Arlington Hall near Washington DC. There was also some contact with the British experimental wireless centre in Delhi. CB was roughly 50% US Army, 25% Australian Army and 25% RAAF. At the end of the war it had over 4300 personnel.

Most regrettably, no full history of CB has ever been written. Most of the records of CB were taken to the United States after the war and are now in the National Archives and Record Administration. We have not examined these records and do not know the extent to which they describe Room's career from December 1942 to August 1945.

Colonel Sandford, Commandant of the Australian Army section of CB, met with Commander Denniston of GC&CS in England on 30 April 1943. The record of this meeting survives as pages 46 to 48 of the Army file. Sandford explained the roles of the three cryptographic groups in Australia at that time. The first was FRUMEL, somewhat reduced by that time. [The American Navy was concentrating its cryptographic efforts in Hawaii and Washington DC by then.] The second was CB, located in Brisbane and described as dealing with Army, Army Air and Naval Air Japanese traffic. The absentee Director was General Akin and the Assistant Director was then Colonel Sherr, later (as already noted) replaced by Sinkov. Other personnel named were Squadron Leader Booth of the RAAF and Commander Nave. Additionally, CB had `Cryptographers and a large clerical staff'. The third organisation was the diplomatic group based in Victoria Barracks, Melbourne and effectively led by Trendall. This meeting discussed co-operation between the Japanese section of GC&CS and the Australian cryptographic groups.

This paper cannot discuss further developments in co-ordination of Allied cryptography.

Thus Room was working in CB at the time as a cryptographer. However as the Army file contains little information on CB from then on, it is not clear when he moved to head what became known as Hut 9. The accompanying photograph, taken from the *SIS Record* and kindly lent by Room's elder daughter Rosemary and her husband David Murdoch, shows those remaining at Hut 9 at the end of the War. Quite evidently, the Americans would not have tolerated a highly paid anomalous civilian cryptographer, and given him leadership of a team, unless he was useful.

FRONT ROW: Donald Laidlaw, J. Roe, E. W. Bennett, Thomas G. Room, Walter Scott, B. G. Smallman, C. Hill, Wilfred Varn. SECOND ROW: Robert Cochran, Max Gershun, R. Brown, Alan Cole, Frederick Lamb, A. A. Ashbolt, C. T. Baker. THIRD ROW: D. A. Gross, C. E. Bevan.

Various references and reminiscences indicate that CB was progressively improving its performance in breaking Japanese ciphers from 1943 onwards. See, for example, the previously mentioned book by Sharon Maneki commissioned by the U.S. National Security Agency in 1996. A major coup in January 1944, and already mentioned in section 6, was the discovery at Sio, New Guinea, of a metal box which, when analysed at CB, was found to contain very substantial quantities of cryptographic information relevant to Japanese Army codes.

18. Brisbane in 1944

At some stage, Room was appointed head of Hut 9 at CB, dealing with meteorological codes. These were used by the Japanese to indicate weather conditions over targets of forthcoming air raids. The area covered was all of New Guinea, Bougainville in the East and extending to Halmahera in the West. The Chief of the Air Staff, writing an introduction to Jack Bleakley's book in 1991, wrote "Throughout the South West Pacific area, particularly at Darwin and the various New Guinea bases, signals intelligence provided innumerable air raid warnings and a constant flow of tactical air intelligence. This resulted in successful Allied interceptions, on the one hand, and the destruction of enemy aircraft on the ground, on the other." This introduction makes it clear that CB information had many applications.

19. Hollandia and Beyond

Hollandia, now called Jayapura, in West Papua was not heavily defended early in 1944. Allied signals intelligence discovered this using the Sio "find" mentioned above and MacArthur decided to take it, thus cutting off Japanese forces to its East. Large sections of CB were then moved `forward" to Hollandia. Room, being a civilian, remained in Brisbane, continuing in Hut 9. Later, elements of CB advanced further, to the Philippines.

20. The Water Transport Code

In September 1944 Governor Dewey was campaigning for the American Presidency and was known to be considering making cryptography an issue. General Marshall, then the Commander of the U. S. Army, wrote to him pointing out the disastrous consequences of such an action. This letter is reprinted in full in Ronald Lewin's book *The Other Ultra*. It stresses the importance of signals intelligence from the Battle of the Coral Sea onwards. It makes particular reference to the breaking of what became known as the Water Transport Code by Joe Richard of CB. Joe Richard, who co-authored in 1999 a paper on recently released CB documents, has written to us expressing his high opinion of Room. It is well worth while to quote a paragraph from Marshall's letter. "Operations in the Pacific are largely guided by the information we obtain of Japanese deployments. We know their strength in various garrisons, the rations and other stores continuing available to them, and what is of vast importance, we check their fleet movements and the movements of their convoys. The heavy losses reported from time to time which they sustain by reason of our submarine action, largely result from the fact that we know the sailing dates and routes of their convoys and can notify our submarines to lie in wait at the proper points."

21. The End of Central Bureau

CB was disbanded soon after the Japanese surrender. The huts in Ascot were not as substantial as the later bomb-resistant buildings in Bletchley Park and were completely demolished. Room took a well-earned holiday and then returned to the University of Sydney. The story of Central Bureau remained secret for many years.

22. Other aspects of Room's work.

Commander Nave, later in his memoir previously cited above, writes:

> "I had other demands on my time and knowledge, one of the important ones being to design codes for the coastwatchers".
>
> "To design a code simple enough to be handled in a hut and at times with a hurricane lamp for light was not difficult, but each was to be different so that in the event of capture others would not be compromised by interception of the messages. However, when they wanted them to inter-communicate it was more difficult to keep it simple and safe. This they desired for reasons such as a new arrival passing through another territory. I felt they could handle this problem by other means such as using a native courier, but with Professor Room's assistance the problem was handled successfully."

Room had ample opportunity to appreciate the utility and power of the IBM tabulating machines in use at CB. In April 1944, while still at CB, he wrote to the Faculty of Science at Sydney University, proposing two motions for its consideration:

a. That the Faculty set up a Committee to investigate the use that could be made of an International Business machine, and the practicability and cost of installing such a machine, and
b. That the Faculties of Engineering and Economics and the Administrative department be advised of this action and invited to appoint members to the Committee.

The Faculty referred the matter to the Professorial Board and a Committee appointed by it reported back, advising that due to the cost and the lack of identified need, such machine use should be obtained by hire from the British Tabulating Machine Company in Sydney. It also noted the possibility of the CSIR (precursor of the CSIRO) obtaining such machines.

Undeterred by this, Room continued to see if he could obtain something of value from CB for his University. The NAA file A6923/3 SI/2 contains a message from the CB Executive officer, Colonel Sandford, to the DMI, Adv IHQ, dated 23/8/45, advising that Professor Room suggests that the Mathematics staff at Sydney University would be interested in the technical investigations needed in the development of Signals technique, utilising a modified IBM machine, and that Major Z. Halpin of the U.S. Army would be pleased to offer his services for this purpose. (Halpin was, we believe, in charge of the "machine room" at CB.)

As far as we know, nothing useful eventuated from this and, if the destruction of all Bletchley Park machines is any guide, it is quite likely that all CB machines were similarly destroyed.

23. The Letter of Commendation

In September 1945 the Secretary of the Department of the Army wrote to the Vice-Chancellor of the University of Sydney as follows: "It is desired to inform you that in view of the unconditional surrender of the Japanese it will be possible to release Professor T.G. Room as from 12 October 1945 after which my Department will cease to pay his salary. The Army desires to take this opportunity to place on record its appreciation of the very valuable contribution made by Professor Room to the Allied War Effort since 18 August 1941 and the generosity of your University in forgoing his services for so long."

24. Reference Material

Richard Overy's 1995 book *Why the Allies Won* attempts to answer the key question about the relative importance of code-breaking, addressing the Battle of Kursk, the Battle of Midway, D-Day and other major turning points, and is strongly recommended. A useful summary of the Pacific war in three-month stages is given by Jack Bleakley in *The Eavesdroppers* (1991). This gives information on CB from the viewpoint of the RAAF. A second major

Australian book is Geoffrey Ballard's *On Ultra Active Service: The Story of Australia's Signal Intelligence Operations during WW2,* also published in 1991. This gives the Army viewpoint and complements Bleakley's book. Parts of David Jenkins' book *Battle Surface: Japan's Submarine War against Australia 1942-1944* (1992) are most enlightening.

The British author Michael Smith has complemented his books on Bletchley Park with his 2000 book *The Emperor's Codes*. The American General C.A. Willoughby wrote a secret *Brief History of the G-2 Section, GHQ, SWPA, and Affiliated Units* for the U.S. Army in 1951. This is a very valuable document available in the Australian War Memorial Research Centre and perhaps nowhere else. It should be read by any serious student of the subject.

Two other books are available from the American side. The first is the *SIS Record*, being an account of the American involvement in CB with numerous photographs of personnel but no explanation of what they were doing. This came out in 1947 and Room received a copy. Much later the National Security Agency published a booklet on CBB and FRUMEL, entitled *The Quiet heroes of the Southwest Pacific Theater,* edited by Sharon Maneki. [This is available free from the Center for Cryptologic History, NSA, 9800 Savage Road, Suite 6886, Fort George Meade, MD 20755-6886, USA.]

A detailed analysis of the present-day literature of some aspects of this topic is available on the University of Sydney Mathematics Website. It gives some sort of review of books by most of the following authors: Richard Aldrich, Christopher Andrew, Desmond Ball & David Horner, Geoffrey Ballard, V. James Bamford, Jack Bleakley, Carl Boyd, Stephen Budiansky, Ivan Chapman, Robert Churchhouse, R. W. Clark, Robert J. Donovan, Edward J. Drea, Peter Elphick, J. Garlinski, G. Hermon Gill, Robert D. Haslach, Paul Hasluch, Jean Hillier, F. H. Hinsley, Huch Hoy, David Jenkins, David Kahn, Solomon Kullback, D. H. Laidlaw, Ronald Laidlaw, Sharon Maneki, Neville Meaney, Hugh Melinsky,Eric Nave, Richard Overy, Fletcher Pratt, James Rusbridger, Simon Singh, Bradley Smith, Desmond Smith & David Horner, Michael Smith, Alan Stripp, Judy Thomson,E. van der Rhoer, Gordon Welchman, Barbara Winter, F. Winterbotham, J. Winter, Ray A. Wyatt and Herbert Yardley. This analysis follows a document giving numerous details of where to find numerous pieces of information. Thus it is not particularly obvious that for Room's trip to Bandung one should ask Recordsearch to look for 'Kennedy Intelligence'. The website will eventually contain a shorter version of this paper and hopefully a copy of Eric Barnes' report on diplomatic codes.

Its address is http://www.maths.usyd.edu.au:8000/ww2codes/ .

25. Acknowledgements

Various members of the Central Bureau Intelligence Corps Association, including Archbishop Don Robinson, Rob Brown, Judith Carson and Helen Kenny, have been of considerable assistance. Mrs Catherine Spencer of Victoria BC has assisted with details of the career of her father, Guy Windeyer. Tim Robinson, archivist of the University of Sydney, deserves considerable thanks. The Research Centre of the Australian War Memorial has been most co-operative, as have many staff at the National Archives in both Canberra and Melbourne and at the National Library. Mrs Barbara Cathers who, with her brother Ian Stafford knew both Dickie and Hilda Lyons well, has provided photographs and other information. David Sissons of Canberra has generously provided much expertise. Although Room did not tell his children much about his war-time work, they have provided what help they could.

26. Appendix: Stripping off the additive

Our section 7 had a brief description of a simplified cryptographic problem of one of the types faced by Central Bureau. Pages 440 to 444 of the second (1996) edition of David Kahn's book *The Codebreakers* show how this exercise may be handled.