

ANNOTATED BIBLIOGRAPHY ON CRYPTOGRAPHY IN AUSTRALIA IN WW2

*Peter Donovan,
School of Mathematics,
University of NSW, Sydney 2052.*

and

*John Mack,
School of Mathematics and Statistics,
University of Sydney, Sydney 2006.*

copyright © Peter Donovan and John Mack 2002.

Although the completeness of any list of this sort cannot be guaranteed, it is more than enough to get any beginner started. A discussion of miscellaneous and archival material follows.

Richard Aldrich, *Intelligence and the War against Japan*, Cambridge University Press, Cambridge, 2000.

This book deal principally with the struggles over the potential re-establishment of European colonial administration in Asia and so is not directly relevant for present purposes. None the less some parts are quite interesting. Thus on page 12 he states that

The established literature on intelligence during the Second World War has tended to emphasise signals intelligence. The organising and exploiting of the invaluable ‘real time’ information derived from cryptanalysis (signals intelligence), in a manner that allowed it to effectively influence strategy and operations, was indeed remarkable. Much attention has been given to the Joint Intelligence Committee system in London and Washington which, by the latter phases of the war, provided an increasingly refined mechanism for overseeing this.

On page 14 he notes that General Macarthur complained ‘that he had to bargain like a rug merchant’ to obtain intelligence from the US Navy.

On page 23 the book notes that the FECB started life as the Combined Intelligence Bureau, Hong Kong, or just CIBHK. It mentions Commander Charles Drage as being involved at one stage. Some information is given on the FECB for the years 1935–1938. On page 26 it describes the difficulties with the high grade army code. On page 33 an account is given of the USN cryptography group, originally in Shanghai, that moved to Guam and the Philippines. Page 34 documents warnings that were given of surprise raids from the Japanese aircraft carriers. Page 36 states that the new interception site at Esquimalt was initiated in 1939. At the same time some interception was carried out on RAN ships.

Pages 234-258 cover ‘the politics of signals intelligence’ and gives some information on the Wireless Experimental Centre at Delhi.

Christopher Andrew, *F. H. Hinsley and the Cambridge moles: two patterns of intelligence recruitment*.

Location: in the book *Diplomacy and Intelligence during the Second World War*, edited by Richard Langhorne, Cambridge University Press, 1985.

This was written 40 years after the Denniston report and gives rather more information. In particular, it points out that Alfred Ewing, with an engineering background, was used in WW1 in the Room 40 cryptography group. On page 35 the paper remarks:

Despite Sir Alfred Ewing's own background in mathematics, Room 40 had been suspicious of mathematics, viewing their personalities with the traditional prejudices of the arts graduate. Wartime experience was held to show that 'the right kind of brain to do the work' was 'not mathematical, but classical'. It was not until lated 1938 that GC&CS, prompted perhaps by the problems posed by the German Enigma cipher machine, set out to recruit its first mathematician.

The first recruited was Peter Twinn. Some information about him is given.

Desmond Ball, *Allied Intelligence Cooperation Involving Australia during World War II*

Location: In the journal *Australian Outlook: Journal of the Australian Institute of International Affairs* 32 (Dec 1978): 299–309.

[Not yet reviewed.]

Desmond Ball and David Horner, *Breaking the Codes*, Allen and Unwin, St Leonards, 1998.

This book deals with post-war espionage in Australia by Soviet agents and supporters and so of the 18 chapters only the first four have any relevance here. None the less it is useful in that it describes some of the earlier activities of various people such as Bertrand Combes (senior intelligence officer, Army Headquarters, 1934–1939), Eric Longfield Lloyd, Rupert Long and Edmund Piesse. Chapter 1 gives the expected information on the secrecy of the signals intelligence process. Chapter 3 mentions Lt-Col Robert Little, assistant DMI 1943–1945, who, amongst other things, 'controlled the diplomatic Sigint section in Victoria Barracks, Melbourne'. Of greatest importance here is chapter 4 on 'The Development of Sigint in Australia'. Thus on page 49 the book states that:

The main work of developing one was initiated by the Navy. Through their connections with the Royal Navy, both the director of military intelligence, Commander Long, and the director of signals communications, Commander Jack Newman, had become aware of the extent and value of British Sigint. For example, in March 1939 Newman had represented Australia at a conference in Singapore on the 'Organisation of Wireless Intelligence in the Far East'.

Thus some effort was made to set up direction-finding equipment for radio messages and to start intercepting radio messages. On page 52 the book states that in January 1940 the Military Intelligence staff at Eastern Command asked Room and Lyons to begin studying codes, but disappointingly no new references are given. However the following quotation from that page is of interest:

Perhaps the Australian Army had been alerted to the need for cryptanalysis when, at the suggestion of the War Office, Major Roy Kendall, a regular Australian Signal Corps officer, had attended a one-month course in cryptography at the end of his training in England in March 1939.

Prime Minister R. G. Menzies, accompanied by Frederick Shedden, the Secretary of the Department of Defence Co-ordination, spent about three months in Britain in the first half of

1941. It is thus more than probable that they were both informed of the then current uses of cryptography.

The reference given for the above is Combes to DMO&I, 3 October 1939; MP 729/6, item 50/401/69. The rest of chapter 4 summarises material given in a different summary form in this account.

Geoffrey Ballard, *On Ultra Active Service: The Story of Australia's Signals Intelligence Operations During WW2*, Spectrum Publications, 1991.

The author was involved right from the start in signals intelligence in the Middle east. This was 'only' traffic analysis work but still provided useful experience for traffic analysis for Central Bureau later. It gives numerous anecdotes of the experiences of numerous people, but also has the basic story of Central Bureau, the signals interception posts and the advances to Hollandia (= Jayapura) and later the Philippines.

The situation when Macarthur arrived in Melbourne in March 1942 is described thus:

A diplomatic cryptographic and intelligence section under the control of the Director of Military Intelligence had been operating for more than a year. This activity had been pioneered by Commander T. E. Nave RN [formerly RAN] and the unit was subsequently joined by a group of distinguished cryptographers and academics including Professor A. D. Trendall who was Professor of Greek and Professor T. G. Room, professor of mathematics at Sydney University. Tucked away under the roof of Victoria Barracks, Melbourne, this unit had the task of de-ciphering the diplomatic and commercial traffic passing between Tokyo and the Japanese embassies in the Pacific region. The observations and reports of Japanese diplomats, as well as the instructions they received from Tokyo, provided a most valuable 'window' of Japan's aggressive intentions in the Pacific. The unit's most spectacular achievement was said to be the de-ciphering of a message dated 4 December 1941 from Tokyo to the Japanese Consul-General in Sydney, ordering him to destroy all his codes and ciphers — a sure indication of the imminence of hostilities.

There is a problem here: just what did the diplomatic section do when the flow of diplomatic messages stopped after the Pearl Harbor raid? The story continues:

A research and control centre, known as the Central Bureau, was established as a combined Australian Army, RAAF and American Army organisation set up at 'Cranleigh', South Yarra.

There is a further gap evident to those trying to work out Room's activities:

In July 1942 Macarthur transferred his HQ from Melbourne to Brisbane and Central Bureau followed in September. [Page 170] . . . into a mansion at Ascot. Appointments were made as the unit expanded. Another special appointment to Central Bureau was that of Professor T. G. Room from the 'Diplomatic Section' in Melbourne. He is believed to have been the only civilian officially invited to join the organisation.

However the book is full of useful information and is without doubt substantially accurate. In particular it corrects any latterday tendency to downplay traffic analysis.

V. James Bamford, *The Puzzle Palace*, Houghton Mifflin Company, Boston, 1982.

This book is an account of the National Security Agency of the United States. This was established in 1952 and may be considered as the present-day successor of various agencies that operated during the second World War. This review will deal with only those parts relevant to the years up to 1945.

Chapter 2 deals with the story of Herbert Yardley, and so describes the closure of his ‘Black Chamber’ in 1929. It also describes the publication of Yardley’s book. It then turns to the attempts by William Friedman to start a new interception and decryption organisation for the United States Army. This resulted in the creation of the Signal Intelligence Service in 1930 and (page 30) the appointment of Frank Rowlett, Abraham Sinkov and Solomon Kullback. These three between them knew French, German and Spanish. John Hurt was added to these three on the basis of his knowledge of Japanese.

The SIS is described on page 33 as having 17 personnel in September 1939 and 331 in December 1941. There were over 10,000 by the end of the war.

The book also describes the development of OP-20-G and remarks (page 36) that Bainbridge Island, an American Island near Vancouver Island, was an interception base. It goes on to describe the re-organisation that followed the Pearl Harbor raid. It notes on page 42 that the first break into Japanese military traffic was made in the [northern] summer of 1943, this being done by the Experimental Wireless Centre in Delhi.

Chapter 8 describes the origins of the Britain-United States treaties on exchange of intelligence. These go back to the Enigma-Purple exchange of early 1941.

One curious mistake occurs on page 311, where the British cryptologist is described as ‘young’; whereas in fact he was a veteran of the previous World War. For this, see Michael Smith’s *Station X*.

A work of fiction written by Margaret Truman, daughter of President Truman, in 1993, states that ‘Puzzle Palace’ was or is a standard name for the Pentagon itself. The reference is page 7 of *Murder at the Pentagon*.

Jack Bleakley, *The Eavesdroppers*, AGPS, Canberra, 1991

This book is written mostly from the viewpoint of the RAAF, and thus shows that it was entitled to a quarter share in Central Bureau. It describes the interception facilities run by the RAAF. Each chapter begins with a summary of the development of the Pacific War over the relevant time interval, usually three months. Although it is not particularly relevant to the present work, it does mention the emergency intelligence arrangements set up in Melbourne as the Japanese advanced and mentions Room as playing an important rôle there. Like most books on this subject it contains mistakes, of which the most obvious is that it states that Eric Nave went to Japan totally ignorant of the Japanese language.

Bletchley Park Web Site.

Location: <http://www.bletchleypark.org.uk>

This is a quite informative web site set up by the trust that now runs Bletchley Park.

Carl Boyd, *General Oshima and Magic*

This book gives an extensive analysis of the messages sent to Tokyo by the Japanese Ambassador to Germany, Oshima. These were of very great use to the Allies. One particularly useful piece of information was the report made by the ambassador in Berlin on the defences in France in 1944.

For some details, see Hinsley’s volume III, part 2, pages 787-793.

Stephen Budiansky, *Battle of Wits: The Complete Story of Codebreaking in World War Two*, Free Press, 2000.

Location: ISBN: 0684859327

On December 3, 1941, officers of the U.S. Army Signal Intelligence Unit decoded a message sent from Tokyo to the Japanese embassy in Washington, ordering embassy staff to destroy its code books and other sensitive material. This, the officers determined, meant that Japan was preparing to break off diplomatic relations with the United States and go to war. When, they could not say; to gain a precise date, they would have had to break the Japanese naval codes. Therein, writes Stephen Budiansky in *Battle of Wits*, lay the rub: ‘Since mid-1939, America had not read a single message in the main Japanese naval code on the same day it had been sent. For most of the period from June 1, 1939, to December 7, 1941, the [U.S.] Navy was working on naval messages that were months, or even over a year old.’

For all their lack of preparedness and occasional inefficiencies, and for all the disdain with which some Allied ground commanders held the work of military intelligence, writes Budiansky, Allied cryptographers were of critical importance in determining the outcome of World War II. The decoding of Japanese and German encryption engines, for instance, helped the Allied navies gain victory in the battles of the Atlantic and Midway, while the translation of secret German railroad schedules allowed Winston Churchill to warn Josef Stalin that the German army was about to invade the Soviet Union—though Stalin refused to take the warning seriously. The codebreakers, in short, ‘averted disasters that would have been terrible setbacks to the Allied cause,’ and they almost certainly saved a considerable number of lives as they labored to crack such profound puzzles as Enigma and Purple.

Budiansky’s narrative is strong on the science of cryptography—so much so that readers without a background in mathematics and logic may have trouble following the arcana of key squares, bigrams, and all the other trade secrets of cryptanalysis. Readers willing to brave matters technical, however, will find Budiansky’s comprehensive account to be the best single book on the subject, and one well worth their attention. – Gregory McNamee, taken from Amazon.com website 2001.

A million pages of new World War II codebreaking records have been released by the U.S. Army and Navy and the British government over the last five years. Now, *Battle of Wits* presents the history of the war that these documents reveal. From the Battle of Midway until the last German code was broken in January 1945, this is an astonishing epic of a war that was won not simply by brute strength but also by reading the enemy’s intentions.

Amazon mentions that purchasers of this book also purchased: *Secret Messages : Codebreaking and American Diplomacy, 1930-1945* (Modern War Studies) by David J. Alvarez.

Robert W. Brown, *Professor T. G. Room and the Hut 9 Team*, Central Bureau Intelligence Corps Association Newsletter, December 1993.

Robert Brown worked under Room in the latter stages of WW2. His memories are set out briefly, together with a posed photograph of the team or some of the team. This is not the photograph in the *SIS Record*.

Frank Cain, *Signals Intelligence in Australia in the Second World War*, in the journal *Intelligence and National Security* vol 14, no 1, 1999: 40–61.

Like every other reference consulted, this text has elementary errors, such as in describing Room as a ‘university linguist’. Perhaps the author downplays the underlying competence shown by the Australian Army and Navy leadership in 1940 to 1941. However it sets out the basic background material with considerable clarity and may well be the best short article — as opposed to book — on the subject.

Ivan D. Chapman, *History of the Sydney University Regiment*.

Location: In SUR Commandant’s officer but not published commercially. Perhaps a copy is to be given to Fisher Library?

Apparently written after the fire of 1959 with oral contributions from various participants. In 1939 Victor Windeyer was commanding officer and Treweek was a Major in the SUR. This book gives some useful background information on Treweek. In particular Treweek joined the SUR in 1938 to improve its capacity in artillery, presumably because his mathematical background helped with the ballistics involved. This information is particularly relevant here because it shows that if the Windeyer family had raised the matter of a pilot cryptography group in 1939 it is likely that Treweek would have been invited before Room. In fact Room was invited before Treweek.

Robert Churchhouse, *Codes and Cyphers*, Cambridge University Press, 2001.

The publishers correctly describe this as a look at the historical development of secret communication from a mathematical viewpoint, describing how ciphers are constructed and how they might be cracked.

In particular chapters 9, 10 and 11 deal with the WW2 Enigma and Fish machines from a technical rather than a historical view-point. Chapters 12 and 13 describe post-war developments made possible by the electronic and internet revolutions.

Chapter 8 deals with the definition of random sequences of digits or letters and how these may be produced. However the presentation is not oriented towards the technology of the 1940’s. Chapter 7 of *Numerical Recipes* by W. Press and others (Cambridge, 1986) is recommended in Churchhouse’s Mathematical Note M13.

After some account is given of 2-letter codes page 58 of the book mentions the 10×10 square used for Japanese naval code JN10. The source is Hugh Denkin’s article that forms chapter 27 of the Hinsley-Stripp book.

Although Churchhouse mentions the use of random additives to make codes harder to break, very little information is given about Japanese practice in WW2.

The book is appropriate for graduates whose studies included some mathematics.

R. W. Clark, *The Man who broke Purple*, Weidenfeld and Nicholson, London, 1977.

[Not yet examined.]

A. G. Denniston, *The Government Code and Cypher School between the Wars*, report dated 2 December 1944.

Location: Reprinted in *Codebreaking and Signals Intelligence*, edited by Christopher Andrew, Frank Cass, London, 1986 and earlier in the first issue of the journal *Intelligence and National Security*.

This is an important primary source on its subject. The author was commandant of GC&CS for many years. However it makes no mention of Eric Nave or Guy Windeyer. Minimal mention is made of the origins of the FECB.

Robin Denniston, son of the author, has published a book (not yet examined) *Churchill's Secrets: Diplomatic Decrypts, the Foreign Office and Turkey 1942-1944*.

Defence Signals Directorate Web Site

The DSD is the Australian Defence Department successor to the World War II codebreakers described here. The entry point is www.dsd.gov.au. Follow the path 'sigint and history' and then go to the HMAS *Sydney* Inquiry. This is a report on the sinking of the Australian warship *Sydney* in 1941. It sets out the various records that have been examined for any explanation of what happened, explaining that the World War II material has now (almost) all been declassified. It explains where this material is to be found.

The American NSA has a useful site www.nsa.gov/wwii that leads into pictures of the museum at Fort Meade, Maryland.

Peter Donovan & John Mack, Sydney University, T. G. Room and Codebreaking in WWII.

Location: *The Australian Mathematical Society Gazette* of June and August 2002. A copy is available on this web-site.

The present document was put together over a period of 18 months to serve as background notes on the material in the Australian Mathematical Society Gazette paper. The emphasis in the paper is on Room. It does not attempt to do justice to Central Bureau.

Richard North has an article based in part on the above paper but including material from Archbishop Robinson and David Sissons in the *University of Sydney Gazette* of September 2002.

Robert J. Donovan, *PT 109: John F. Kennedy in World War II*, McGraw-Hill, New York, 1961.

This book is of relevance here only in so far as it describes an incident in which the future US President had his small US Navy boat rammed by a Japanese destroyer off the Solomon Islands on the night of 1 August 1943. News of the incident was sent back by a coast watcher, Lt A. Evans, RAN. Kennedy and the other survivors were ultimately rescued. The Evans report on this incident takes up two pages in the Willoughby *Short History* preserved by the Australian War Memorial as file AWM59. The question arises: did Evans use a code provided by any of the Sydney University four or by Nave? If indeed Barbara Winter is correct (page 221 of *The Intrigue Master*) the message was sent using a simple Playfair code. Winter also makes it clear that Nave was the one who designed codes for the coastwatchers. Yet Nave in his memoirs (at the AWM) says Room joined in on this project. The Kennedy incident will be disregarded.

Edward J. Drea, *Macarthur's Ultra*, University of Kansas Press, 1992.

Although this book makes no mention of Nave or Room, it presents the American side of the story reasonably completely. In particular it gives background knowledge on most of the key American participants in the Central Bureau, such as General S. B. Akin. It describes the development of the Purple machine that deciphered the 'Purple' diplomatic code. It gives an account of the 'station 6' decoders in Corregidor (Manila Bay). This unit was relocated in Melbourne. This became by May 1942 a key ingredient of FRUMEL. It then moves on to the establishment of Central Bureau in April 1942 and the development of techniques to handle Japanese army traffic. This was of great service in the battles in northern New Guinea. It finishes with a discussion of the extent to which signals intelligence influenced the decision to use nuclear weapons.

[The Ball-Horner book listed above describes Drea as 'chief of research and analysis, US Army Center of Military History'.]

Peter Dunn, Private Website of World War II.

Try home.st.net.au/~dunn/sigint for what appears to be the only Australian private website on the subject. It is quite interesting. In general, searching the world wide web for 'FRUMEL' tends to pick up this subject without too many irrelevant other topics.

P. Elphick, *Far Eastern File: The Intelligence War in the Far East 1930-1945* H & S, London, 1997.

Synopsis: This book deals with Japanese subversion and ground-level intelligence gathering in China, Indo-China and Malaya before the war. It makes some considerable mention of the radio eaves-droppers. It may give the best account of the FECB. It then goes on to give a (briefer) account of intelligence gathering during the war years. Very much recommended.

John Ephron, *An American Cryptanalyst in Australia*.

Location: In journal *Cryptologia* 9, no. 4 (Oct 1985), pages 337-340.

[Not yet reviewed.]

Basil Fogarty, *The Ultra Factor*, privately published 1995.

Location: Author: POB 133, Terang Vic 3264.

Not yet properly examined. Its cover describes it as the 'unrecorded intelligence background to the campaigns in New Guinea, New Britain, Bougainville, Borneo and the air raids on Darwin.'

J. Garlinski, *Intercept*, Dent, London, 1979.

This is an early book. Evidence as to the difficulty in researching the matter at the time may be found on page 126, where we learn that Mrs. Ruth Thompson confirmed on 9 December 1977 that Bletchley Park had a Japanese section. Until then the author had not discovered this aspect.

Rather curiously, on page 176 it is stated that Winterbotham set up units at ... Brisbane in Australia without any proper mention of Central Bureau.

G. Hermon Gill, *Royal Australian Navy 1939-1942*, Australian War Memorial, Canberra, 1957.

This book is quite useful as a source on the steps taken by the Navy prior to the start of the Pacific War. In particular, pages 420–421 describe the special position of the Naval Intelligence Department under Lt-Cdr Long.

In August 1940 this organisation was amended by the establishment of a Combined Operational Intelligence Centre (C.O.I.C.), on a recommendation of the Joint Planning Committee which was ratified by the Defence Committee. . . .

On the other hand the Naval Intelligence Division was long established, was a separate Directorate, and was a direct branch of British Admiralty Intelligence with its world-wide network. Practically all the intelligence received by C.O.I.C. was naval in origin and importance, a great deal of it from the Admiralty dealing with the future movements of naval and other important ships . . .

It is likely that much of these messages survive in the London Public Records Office. See also the book by Barbara Winter.

G. Hermon Gill, *Royal Australian Navy 1942–1945*, Australian War Memorial, Canberra, 1968.

This text contains no mention of FRUMEL and gives inadequate space to the battle with the Japanese submarines. However it very usefully describes developments elsewhere as it explains the various events, particularly those to the north of the country. It nicely complements David Jenkins' *Battle Surface*.

This series of official war history books includes an army series giving full details on the war in New Guinea.

Robert D. Haslach, *Nishi no kaze, hare : Nederlands-Indische inlichtingendienst contra agressor Japan*, Van Kampen, c1985.

This 224 page book in Dutch deals with espionage, military intelligence and cryptography in the Netherlands East Indies during the Second World War. Note that the book by John Prados listed below gives more information on page 247. In particular, Prados mentions liaison with Australia.

Paul Hasluck, *The Government and the People 1942–1945*, Australian War Memorial, Canberra, 1970.

This book is generally relevant to any study of the allocation of resources to defence from 1942 onwards. However for the purposes of this exposition three extracts are particularly relevant:

(1) On page 728 some brief details are given of the career of Lt-Col Eric Longfield Lloyd (1890–1957), Australian Government Commissioner in Japan 1935–1940.

(2) On page 153 various references are given for the the proposition:

The principle that the European theatre should be the decisive theatre had been established at the highest level even before Japan entered the war.

(3) The rivalry and lack of co-operation between the US Army and the US Navy in the years leading up to 1942 are discussed on page 154. Adequate references are given, including page 30 of Eisenhower's *Crusade in Europe*.

Jean Hillier, *No medals in this Unit*, privately published 1996.

Location: Author lives at Mundalla, SA.

Not yet examined properly. May well be personal reminiscences.

F. H. Hinsley and others, *History of British Intelligence in the Second World War*.

Very complete for the European side of the war. But see pages 4 and 5 of Elphick's book:

British Far East intelligence efforts received no coverage at all in Hinsley's monumental official publication *British Intelligence in the Second World War*. In a letter to this author dated 1 May 1995 Professor Hinsley said that the reason for this omission was that when he compiled his volumes from 1979 onwards, only about a quarter of the Far East material was available in the United Kingdom, and that no authoritative account could be provided unless intelligence material is co-ordinated with operational decisions, of which most in the Far East were made by the Americans.

The official Australian histories of the war were written mostly before 1974 and contain no reference to the role of the codebreakers.

F. H. Hinsley as a young man was engaged in putting together fragments of information from decoded messages and other sources about the German navy. He appears in a photograph opposite page 247 in Ballard's book attending with a dinner given by the Governor of Queensland in March 1944. He is described there as 'Aide to Sir Edward Travis, Director of the GC&CS'. Travis and Hinsley must have been looking at a part of what had become a world-wide intelligence network.

F. H. Hinsley and Alan Stripp (eds) *Codebreakers: the inside story of Bletchley Park*, OUP, 1993.

This book was written by various people who worked at Bletchley Park and edited by two of their number. Hinsley later became a distinguished historian; by 1944 he had become an aide to the director of the GC&CS, Sir Edward Travis. [Reference: Ballard, page 284.] It describes the size of the Bletchley Park operation in the preface:

As early as the end of 1942 it was reading some four thousand German high-grade signals a day, with slightly smaller numbers of Italian and Japanese signals.

Plate 11 in this book is a photograph of part of Japanese Air Force 6633 codebook; plate 24 is part of the decrypted and translated version of the message that revealed the plans for what was to be the last journey of Admiral Yamamoto.

Chapter 26, by Michael Loewe, gives information on Japanese naval codes.

The present writer can say nothing of the way in which the machine ciphers were broken; the greater part of the work on which we were engaged consisted of 'stripping', that is recovering and removing the reciphering tables that had been applied to the underlying code-groups, and 'book-building', that is recovering the meaning of those groups. Long weary hours of the war were thus spent in subtracting figures from figures or indexing the code-groups. These were in the form either of four figures [= digits], in JN 11, which was used by merchant shipping; or of five figures in JN 25, the main naval code.

Chapter 27, by Hugh Denham, gives more information on naval codes and ciphers. Chapter 28, by Maurice Wiles, gives some details on army codes. Finally Chapter 29, by Alan

Stripp, gives information on air force codes. The exercise of learning Japanese at Bedford is described in detail. However minimal mention is made of Melbourne or Brisbane and none of FRUMEL and CBB.

J. W. P. Hirschfeld and G. E. Wall, memoir published in *Historical Records of Australian Science*, vol. 7, no. 1, 1987.

Location: Published by the Australian Science Archives Project on ASAPWeb, 1995

The following is just the section entitled **War Years 1940-45**

Two separate honours were conferred on Room in 1941. The first was the award of the Thomas Ranken Lyle Medal for outstanding work in mathematics or physics. This was awarded at that time by the Australian National Research Council. The second was his election as Fellow of the Royal Society of London. A citation referred to his remarkable insight into spatial relations and made special mention of his general theory of the freedom of manifolds.

From 1941 to 1945, he was engaged in military intelligence work for the Australian government. He never spoke about it himself but some information is available.

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 Command Bureau in Singapore to gain experience in British code-breaking methods. A letter written 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!'

Many islands immediately to the north of New Guinea were occupied by the Japanese forces in the first half of 1942. A network of Australian 'coast-watchers' remained behind the Japanese lines, reporting movements of shipping and aircraft by wireless to the Allied forces. At the request of the Australian Army, 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 March 1942, the American and Australian authorities agreed to form a joint signal intelligence section, called the Central Bureau, in conjunction with it. This embraced all armed services and many Allied nations, and its members possessed an extraordinary array of diverse talents. Its name is said to have come from Kafka's novel *The Castle*. Room was transferred to the Central Bureau, where he worked until the end of the war on the decoding of Japanese military signals. This was a particularly difficult task but one of vital importance to the Allied operations. His work was described as 'spectacularly successful'.

D. M. Horner, *Special Intelligence in the South-West Pacific Area in World War II*,

Location: In journal: *Australian Outlook: Journal of the Australian Institute of International Affairs*, 32 (Dec 1978), pages 310–327.

[Not yet reviewed.]

D. M. Horner, *Australia and allied intelligence in the Pacific in the Second World War*, Canberra, Australian National University, 1980.

Location:

[Not yet reviewed.]

Hugh Cleland Hoy, *40, O. B., or How the War was Won*, Hutchinson, London, 1932.

This may be the first book exaggerating the importance of signals intelligence in the First World War. There have been others for the Second World War. In *The Intrigue Master* Barbara Winter states that Hoy's book influenced Cdr Long, the Director of Naval Intelligence. Regardless of this, Hoy's book must have been a factor in the total secrecy imposed from 1945 on WW2 sigint activities.

Sue Jarvis, *Japanese Codes*. Bletchley Park Reports, 1997.

Location: See Bletchley Park website. Copies cost GBP2.50 + postage.

[Not yet inspected.]

David Jenkins, *War of Words*, *Sydney Morning Herald*, 19 September 1992. Pages 37–38.

Although this is mostly incorporated into the book mentioned immediately below, it sets out most of the basics of the story. Being based on professional interviews of Jamieson, Trendall and Treweek it is undoubtedly of high reliability. Furthermore David Sissons of Canberra has records of his interviews with Trendall and Treweek; these confirm the Jenkins version.

David Jenkins, *Battle Surface: Japan's Submarine War Against Australia 1942–44*, Random House, Australia, 1992.

This is a major work on an aspect of the war not covered by earlier books. The author went to great trouble to interview people on both sides. In particular, he spoke to both Trendall and Treweek, and so was able to record in print their recollections of the matters discussed here.

There is a mistake on page 42 in that Jenkins states that the Sydney University group started up in January 1941. In fact the Army file (NAA 37/401/425) contains a letter of 18 October 1940 that indicates the group was in existence then. However the records of interviews with Trendall and Treweek are beyond doubt substantially accurate and of considerable interest for present purposes.

The list of documents in the National Archives include a few very relevant here. They are the letter from Prime Minister Menzies to the Secretary of State for Dominion Affairs, 11 April 1941. This is MP 1185/8, file WP 1937/2/415. There is also a report by Commander Jack Newman to Commander Nave of 19 March 1941, on his visit to Singapore. This is MP 1185/8, file MP 1937/2/415. Dominion Affairs, 11 April 1941. This is MP 1185/8, file WP 1937/2/415. The order to the Japanese Consulate, Melbourne, to destroy documents, 2 December 1941 may be found at CRS A 5954, item 558.

The Trustees of the Australian War Memorial would do well to reprint one significant book on the Australian involvement in past wars each three months. This work would have considerable claim to be included in such a reprint program.

David Jenkins and Peter Hastings, Sequence of articles on WWII 50 years on, part 4. *The secret war of, and between, the codebreakers*.

Location: *Sydney Morning Herald*, 30 August 1989.

This mentions some disharmony between the Sydney academics. It contains reports of some interviews.

David Kahn, The Codebreakers, Weidenfeld and Nicholson, London, 1973. [There is a revised second edition dated 1996.]

The first edition of this relatively early book has considerable merit. For example it has the basic facts about Central Bureau and some details of Abe Sinkov's postwar career with the National Security Agency. [For more on this, see pages 37–38 of the Maneki book.] Although it has much other information it says very little about codebreaking in Australia in 1940–1941. The following few sentences from page 266 have considerable interest:

In January 1941, however, a four-man American cryptographic team accompanied a PURPLE machine to establish technical co-operation with British cryptanalysts. Britain had not cracked the PURPLE machine but they had more in the way of cryptanalysed intercepts than the United States and this was the quid pro quo. This co-operation between the two English-speaking nations in the most sensitive of areas tells the depths of their friendship. The American Special Intelligence Service and OP-20-G radioed the PURPLE keys to London daily. Co-operation extended to the small Australian communications-intelligence unit and to the units at Singapore and Canada assisted in making sure that all got all Japanese intercepts.

The second edition (1996) contains much more information, including an account of stripping away additives.

Solomon Kullback, *Statistical Methods in Cryptography*.

Of interest as some evidence of Kullback's professional prowess.

D. H. Laidlaw, *Anecdotes of a Japanese Translator 1941-1945*, Adelaide, 2001.

The author is shown in the 1945 *SIS Record* photograph taken with Room and the then Hut 9 team. This little book has another photograph of Room in Brisbane.

The author was born around 1924 and joined the army in December 1941. being colourblind he was allocated various non-combatant duties that enabled him to pick up some Japanese. In February 1943 he joined Central Bureau as a linguist. On pages 32 to 35 there is a simple explanation of the structure of CB and the positions of Room and Sinkov in the Cryptographic unit. In June 1943 he was sent to an interception station somewhat south of Darwin and returned to Brisbane in February 1944. He describes the work done in such remote locations and gives a clear impression of the style and substance of Central Bureau.

Ronald Lewin, *American Magic = The Other Ultra*. Hutchinson, London, 1982.

This relatively early book makes a fairly minimal mention of the Central Bureau on page 149. It is written from the American viewpoint almost exclusively. However it contains

much useful information, such as the growth of staff at Arlington Hall from 181 in December 1941 to 7000 in August 1945.

Sharon A. Maneki, *The Quiet Heroes of the Southwest Pacific Theater: An Oral History of the Men and Women of CBB and FRUMEL*, National Security Agency, USA, 1996.

Location: Available free from the NSA.

This booklet gives accounts written by people who were there, including Sinkov and Richard. It makes some use of the earlier Ballard book. It seems well worth while to state what is there:

The importance of traffic analysis as an ingredient and sometimes as the only information available is made clear. Indeed, the Australians had experience with traffic analysis in the Middle East and so were able to complement the Americans. Maneki states (page 95) that by the end of the war CB had 4339 personnel. This was made up of 4338 assorted military and 1 civilian, presumably Room. In June 1945 no fewer than 126929 Japanese messages were logged.

The book gives Joseph Richard's account of the breaking of the Water Transport Code. It gives Abraham Sinkov's account of CBB, including (page 39) a mention of Room's task as heading a small group handling 'low-level traffic, transmitted under low power'. It describes how certain key cryptographic information was obtained by direct capture of the relevant paper. The following extract from page 42 is quite significant:

Changing the codes presented a great problem for the Japanese as the war progressed. As Japanese troops were isolated by the Americans, the Japanese were forced to communicate code change instructions in the old system. We read these instructions and followed them. We had the information for the new codes at the same time as the Japanese troops. Two examples of prudence by the Americans were Rabaul and Bouganville. We could have forced the Japanese to surrender in these locations. Their isolation was a great source of information for us.

Some description is given of the use of the IBM machines.

Neville Meaney, *Fears & Phobias: E. L. Piesse and the Problem of Japan*, National Library of Australia, 1996 (Occasional Papers, number 1).

Piesse was born in Tasmania in 1880, had worked for the Intelligence Section of Military Operations in Melbourne from November 1914. In March 1916 he became the first Director of Military Intelligence. In 1919 he became head of the Pacific Branch and Foreign Affairs section of the Prime Minister's Department. He resigned in 1923 and returned to private legal practice, but had some continuing influence through his writings.

To prepare to meet the Japanese menace, the Australian government in early 1915 requested the British Ambassador in Tokyo and the NSW Trade Commissioner in Kobe to send them all available information relating to Japan's attitude towards Australia and the Pacific. It also ordered the intelligence services to keep a close eye on Japanese in Australia to detect espionage or other suspicious activities. The Defence Department appointed James Murdoch, a British-born scholar and language expert who had spent many years in Japan, to a lectureship in Japanese at the University of Sydney. In addition to teaching two days a week at the University and three days a week at Duntroon Military College he was to be available to translate intercepted Japanese documents and to advise generally about Japanese politics and

policies. Both the Defence Department and the Navy department produced reports on the Japanese question.

Later Meaney describes how Murdoch's Chair of Oriental Studies was financed provided that Murdoch was allowed 'an opportunity to visit Japan annually during the long vacation and such part of the first term as may be necessary'.

Meaney is in error in asserting that the Defence Department appointed Murdoch. In fact it made an offer to the University to support this idea, which it was able to accept once they got some advice on Murdoch. The Department made further strong representation to the University to offer him a chair when he was showing signs of returning to Japan. After another check, it did. This appointment process would not get past step 1 these days. The University archivist has a file on the Department of Oriental Studies.

The booklet continues with the developments of the 1930's, including Australian worries about the validity of a defence policy based on holding Singapore against the Japanese.

Meaney has published another book (not yet examined): *Towards a New Vision: Australia and Japan through 100 Years*.

Hugh Melinsky, *A Code-breaker's Tale*, Lark's Press, Dereham, 1998.

Melinsky was a Cambridge undergraduate sent to the Bedford crash course in Japanese language with Alan Stripp. Details of this course are given. He was one of twelve sent to Brisbane in April 1944. The remark on page 10:

Apparently Britain and America between them could find fewer than forty people who were competent in the language.

may well not be totally accurate. However a nice sample of a Japanese code book is given there.

Melinsky's colleague Barry Smallman was allocated to Room's team. Melinsky himself was sent to work on 'Naval Air', that is messages from that part of the Japanese air forces controlled by the Japanese Navy. (The other part was controlled by the Japanese Army.)

Our task was to decode and translate messages picked up by wireless units which listened to Japanese aeroplanes flying anywhere from Tokyo to Singapore, and their bases, and sent the messages to us in Brisbane. These told us a great deal about what the Japanese were doing and were intending to do, and Captain Nave passed vital information immediately to the staff of General Macarthur who controlled all the American and Australian forces in the South-West Pacific Area.

Melinsky makes it clear that Nave was extremely experienced and competent. Valuable details on the practicalities of code-breaking are given. Curiously the book seems not to mention the process of stripping away the additive. Anyway, the following from pages 23 and 24 describe 'two great helps in this process':

The first was being familiar with the shape of the message. . . .

The second were 'cribs', something which ought never to happen with well-trained wireless operators. . . . The operator repeats the identical message in code 23, which the interceptors have already largely broken. So it is easy to read off all the groups in code 24.

Page 24 mentions also a major source of Japanese encoded material: in January 1943 two RNZN ships forced a Japanese submarine to beach on a reef near Guadalcanal. Page 33 mentions the material found at Sio in January 1944.

After spending 6 weeks at Central Bureau in Brisbane, Melinsky was posted to a RAAF radio interception base near Darwin. This sent information to Nave at Central Bureau directly by landline teleprinter, using a Typex machine to prevent interception. later, in 1945, he was sending such intercepts by wireless back to Nave from Borneo.

Chapter 5, entitled 'The Wider Picture', is a simple narrative of the development of the Pacific War. Hopefully the text given in this account is as clear as that of Melinsky.

R. S. Merrillees, *Professor A. D. Trendall and his Band of Classical Cryptographers*.

Strategic and Defence Studies Centre, ANU, Canberra. Occasional paper WP355 ISBN 0 7315 5404 3.

This describes the personnel involved Australia's third cryptographic group, that working on diplomatic material. A paper currently in draft form by David Sissons explains the role of this group in the overall British effort to monitor Japanese diplomatic traffic, including the key Oshima material. See also Carl Boyd's book mentioned above.

Eric Nave, *An Australian's Unique Naval Career*.

Location: Unpublished manuscript 1183, at Australian War Memorial. The AWM website describes it as 'restricted access. Donor's permission required.' [Enquiries should be made through the AWM rather than directly to Nave's surviving relatives.]

Perhaps disappointingly, this does not give much insight beyond what is in the Rusbridger-Nave book, but it is not polluted by Rusbridger's speculations. It should end up on the AWM website. See *SMH* 28 June 1993 for an obituary of Nave (born 1899).

Richard Overy, *Why the Allies Won*, Cape, 1995.

Reviewed by Gilbert Taylor – *BookList*

Analytically incisive, Overy constructs a self-assured interpretation of how the Allies reversed Axis aspirations in 1942/44. Given Germany's and Japan's utter ruination, the answer to victory seems superficially obvious: Allied material superiority. But in the knife-edge years the odds were even, and Overy examines in the book's first part five critical battles — Midway, Kursk, the Atlantic, and Normandy, and the bombing offensive. The last, commonly regarded as of dubious utility and doubtful morality, Overy restores to critical strategic importance for having drawn off the Luftwaffe from the Eastern Front, where the war was fundamentally decided in unparalleled savagery. In his second part, Overy judiciously appraises non-material factors, such as leadership and national morale, which fed into the ironies of victory: the Western Allies were saved by a partner slightly, if at all, more palatable than their Nazi enemy; and the Soviet peoples won almost nothing, except life, for their sacrifices. For readers deeply steeped in or just beginning to brew the war, Overy evaporates its nimbus of inevitability through persuasive and well-aimed argument.

This book takes the line that signals intelligence, while very useful, was not the key factor. It was a major component in Midway, the Atlantic and Normandy. This is well worth reading.

John Prados, *Combined Fleet Decoded*, Random House, NY, 1995.

Location: Reduced to USD20 at amazon.com.

This 800 page book is essential reading for those seeking to understand the role of FRUMEL in the Pacific War. In fact it may well be the authoritative work on Allied and Japanese naval intelligence in the Pacific War. The dust jacket quotes one expert as saying ‘In his account of the shadow conflict John Prados has all but re-written the history of World War II in the Pacific. This is not just an important work but an immensely readable one.’

The difficulty in explaining the Pacific War lies not in describing how the Allied Forces did so well but in detailing how Japan fared so poorly. ... The true achievements of intelligence in the Pacific war lie in the day-to-day accumulation of a fund of knowledge regarding the adversary. Cryptology, traffic analysis, aerial photography, prisoner interrogation, document capture and translation and technical intelligence each became pillars of an overall effort greater than the sum of its parts. ... This is by no means to say that force was not important.

The book explains on pages 387–390 how Japanese intelligence was in general defective. It improved towards the end but the damage had been done. Page 299 explains how little the Japanese understood the situation in Australia in 1942. Page 302 mentions FRUMEL’s role in April 1942 in deciphering messages that detailed the organisation of the Japanese force. Page 318 mentions that:

Melbourne’s first key contribution was a decrypt showing that the Japanese [after the Battle of the Coral Sea] has abandoned the plan for an amphibious landing at Port Moresby in favour of an offensive across the Owen Stanley mountains. This made Halsey’s carriers superfluous in the South Pacific and enabled Nimitz to justify recalling them [for the Battle of Midway].

Pages 415–424 describe the career of FRUMEL with some mention of Central Bureau. The significance of Commander Jack Newman, RAN Director of Naval Communication, emerges. Previously the coastwatcher set up by the Naval Intelligence Department of the RAN is praised.

The author appears not to have been aware of David Jenkins’ book *Battle Surface* or of Barbara Winter’s book *The Intrigue Master*. This may indicate a lack of detailed knowledge of the Australian viewpoint. Still, Prados’ work is most informative and valuable.

Fletcher Pratt, *Secret and Urgent, the story of Codes and Ciphers*, Robert Hale, London, 1939.

Location: State Library of NSW.

Note: This copy has the date ‘18.4.40’ marked on it in pencil and so it could well have been the copy consulted by Treweek and others. On page 191 a typographic error has been indicated by a pencilled ‘?’ and so someone must have read it carefully. Note that Trendall was a trustee of the Library at the time.

The book begins by stating that the only other book in English on codes and ciphers is that by Rosario Candela. Page 16 mentions the important fact that in the pre-computer era complicated ciphering tended to produce garbled messages. Among the tricks then available were ‘nulls’, that is ‘letters or words introduced to confuse a decipherer’. Chapter 1 deals with the Rosetta stone and the even harder task of handling ancient Persian writing. After that much detail is given on messages sent in enciphered form from 1500 to 1900.

There was a revival of innovation from 1850 onwards. Ciphers were used in the Franco-Prussian War. However for present purposes the main interest is in the account given of the use of codes in WW1. This undoubtedly would have helped get the four academics started.

James Rusbridger & Eric Nave, *Betrayal at Pearl Harbor*, Summit Books, New York, 1991.

The Rusbridger-Nave book moves towards the startling claim that the British Government had advance knowledge of the raid on Pearl Harbor (7 December 1941). For this we should read pages 182–183 of Peter Elphick's book.

Rusbridger's case largely rested upon information which he indicated had been supplied by his co-author, cryptographer Captain Eric Nave. However, in an interview in 1991 for Japanese television, Nave repudiated a large slice of what Rusbridger had written, calling it speculation. In addition, Nave had apparently forgotten that on 1 December 1940, a year before the attack on Pearl Harbor, the Japanese had replaced code JN-25, which was being at least part-read by Britain, with another the Allies called JN-25b. No mention of this new code, which the American navy cryptographic section in Washington (OP-20-G) was also working on, was made by Rusbridger. This new code proved a very hard nut to crack. So much so that when the RAN's Director of Signals Communications, Commander J. B. Newman, visited FECB in March 1941, he reported that most Japanese codes were still unable to be read and that at that time FECB was almost wholly dependent for naval information on traffic-analysis and direction-finding.

There are other flaws with this book, such as describing Ian Longfield Lloyd as one of the four Sydney University academics. However it most certainly has its uses, particularly in setting out the various steps in setting up the early cryptographic establishments of the future allies from 1920 to 1940. It also indicates the difficulty Rusbridger had in getting at the official files around 1985. The conclusion that lack of co-operation between the US Navy and the US Army on cryptography was a root cause of the Pearl Harbor raid being such a disaster for both rings true, even if the lack of appreciation of JN25b spoils the second half of the book.

Another book on alleged Pearl Harbor conspiracies is that by Robert Stinnet.

Rusbridger died in 1992 in somewhat unusual circumstances: the world wide web may be searched for further information. David Sissons has reviewed this book in the *Journal of Intelligence and National Security*, volume 9, number 2 (1994).

Simon Singh, *Code Book*, Fourth Estate. London, 1999.

This is an interesting book both for its accounts of code-breaking up to 1920 and its accounts of modern developments, including the possible effect of the hypothetical quantum computer. A television series was based on this book.

However chapter 4 is the sole part relevant for present purposes. It is called *Cracking the Enigma*, and begins with some account of the early work by Polish mathematicians assisted (1931) by a German traitor. The French Government had paid the necessary bribe and passed the information on. In the Polish Government Cipher Bureau, one Marian Rejewski was the key worker.

In July 1939 the Polish Government, anticipating the invasion of September 1939, passed the decoding technology on to the British and French decoding bureaus.

Here only the British reaction is relevant. The Polish success created the impetus to build up a team in Britain, and furthermore drew attention to the merit of having a mixture of linguists and mathematicians. 'These were recruited mostly via the old-boy network.' 'During the [north] autumn of 1939, the scientists and mathematicians at Bletchley learned the intricacies of the Enigma cipher and rapidly mastered the Polish techniques.'

This may indicate the timing of British advice to the Australian Army on how to get something going in advance of a prospective Pacific war.

Although not directly relevant, this book discusses the career of John Chadwick, who was involved in breaking Japanese codes at Bletchley. A classicist, he learned of Michael Ventris' work on the ancient language 'Linear B' and formed a partnership to work on the language. After the accidental death of Ventris he wrote the well-known book *The Decipherment of Linear B*. As already noted, Treweek wrote a paper on this topic and had it published in 1954.

SIS Record Association, *Special Intelligence Service in the Far East 1942–1946: An Historical and Pictorial Record*, SIS Record Association, New York, 1946.

Location: Scarce in Australia. Presumably currency restrictions made it very difficult for Australians to buy copies in 1947.

This book could not state what the SIS had been up to but does give some account of the personnel aspects. The photographs are of great value. The following letter from General MacArthur of 11 November 1945 is well worth quoting:

1. On the eve of the deactivation of the SIS of the South West Pacific Area and of the Army Forces, Pacific, I wish to commend this organisation and its members for their efforts in the war against Japan.
2. This service, which grew from a mere handful of Americans and Australians to a strength of more than 3,000, has been outstanding in its achievement.

Page 19 gives photographs of Ascot Park in the Central Bureau era.

Actually most sections combined the aspects of such a laboratory, a grammar school and the Ford assembly line. The work often provided the sort of thrill that is known only to scholars and labyrinth makers. Independent and individualist characters of several nationalities were always around to provide local color.

A list is given of 750 Americans involved at the end of the book.

Room together with a staff of 16 from Hut 9 appear in a posed photograph, most likely taken in August 1945.

A list of the 14 Allied services involved, such as the Royal Navy and the Australian Army, that had contributed to Central Bureau is given on page 73. The US Navy is a very conspicuous omission.

Bradley Smith, *The Ultra-Magic Deals and the Most Secret Special relationship 1940–1946*, Airlife Publishing, Shrewsbury, 1993.

This is very useful on its topic. Thus (page 19) it informs the reader on how in 1937 the USN and the RN were exchanging information about the Japanese Navy. Remarkably at the same time Britain and Japan were exchanging information about the Japanese Army. Page 35 gives the date of October 1940 for the final breaking of the ‘Purple’ code. Page 48 gives the details of a meeting in London on 22 October 1940 which initiated US-GB co-operation on cryptanalysis. The Sinkov mission to Bletchley followed three months later. Page 97 states that the Welchman letter to Churchill of October 1941 resulted a few months later in the removal of Denniston from the directorship of GC&CS and his replacement by Travis. Page 106 notes that the American cryptanalysts from Corregidor brought a Purple machine with them to Melbourne; thus it was available for FRUMEL. Page 175 states that the American Sigaba (1942) and Sigum (1943) encoding machines were a generation ahead of the Enigma. This was also true of the British Typex.

Desmond Smith and David Horner, *Breaking the Codes : Australia’s KGB Network, 1944-1950*, Allen and Unwin, 1998.

Begins with much detail on the Central Bureau. The following is the Amazon synopsis: In December 1944 General Blamey, the Commander in Chief of the Australian Military Forces, was handed a file. It contained decrypted radio intercepts which proved that the Imperial Japanese Army was receiving top secret information – US and Australian war plans. Material that could lead to the death of Allied servicemen in the Pacific. The most likely source: Canberra. So began a hunt which took five years, involved the world’s most secret intelligence organisations and resulted in the exposure of neutralisation of a Soviet espionage network in Australia. ‘Breaking the Codes’ is a story of international counter-espionage and signals intelligence. It tells of a secret war which showed the seeds of suspicion in Moscow, Washington and London, seeds which flowered in the Cold War and led to the creation of ASIO. This ground-breaking study shows how signals intelligence helped uncover the KGB’s activities in wartime Australia. It tells how counter-intelligence, through a partnership with MI5, provided the details — the names and roles of members of a network of informants run by the Soviet Embassy in Canberra. Australians who, whatever their motives, were playing a dangerous game as a World War was being fought and a Cold War was being born.

The second author was author of *Australia and Allied Intelligence in the Pacific in the Second World War* published by Australian National University, Canberra, 1980.

Michael Smith, *Station X*, Boxtree Press, London, 1998.

This is the companion work to *The Emperor’s Codes*, and is less relevant for present purposes. However it does throw some further insights into the whole saga, such as making it clear that Turing, Milnor-Barry, Alexander and Welchman were very influential in the development of Bletchley Park. In particular it describes Welchman’s contribution to the organisation of the institution. On page 112 it describes the size of the ‘Y’ service, that is the actual interceptors. in 1940 and 1941. On page 116 it describes the role of ‘Mr Freeborn’s section’ in using punched cards to make cross-references accessible. The duties of a traffic analyst are described on pages 124-126.

The author, together with Ralph Erskine, has edited another book *Action This Day*, Bantam, 2001, which contains 22 essays on the Enigma saga. This does not seem particularly

relevant to the Pacific war. One essay is of particular interest in that it discusses the reasons why German suspicions that Enigma codes were being broken never lead to any practical action. [This last paragraph is based on the review in *New Scientist* of 3 November 2001.]

Michael Smith, *The Emperor's Codes*, Bantam Press, London, 2000.

The author also wrote the '#1 Bestseller' *Station X* on the Bletchley Park operation. This book is subtitled 'Bletchley Park and the breaking of Japan's secret ciphers', and has access to Eric Nave's unpublished memoirs (Australian War Memorial, document 1183.)

The book is an essential requirement for anyone trying to get a grasp on what went on. It is more interested in the British viewpoint than the Australian, but does cover most of the story in adequate detail. References to official files, including the British files, are given. Its flaws include overlooking the roles of Commander Long and Major Treweek. The author appears to have found neither Treweek's document B5555/2 nor the Willoughby *Short History* in AWM59.

An extended review by Red Harrison was published in *The Weekend Australian* of 10–11 February 2001. Michael Smith wrote an account of this material in the 13–19 September 2000 issue of the *London Weekly Telegraph*.

Alan Stripp, *Codebreaker in the Far East*, OUP, 1989, 1995.

The author was there! Apart from memories, he describes what was done and how it was done. Very enlightening.

Judy Thomson, *Winning with Intelligence: A Biography of Brigadier John David Rogers, CBE, MC, 1895–1978*, Australian Military History Publications, Loftus, NSW, 2000. [Joint venture with the Australian Army Intelligence Unit.]

Rogers had served in the first World War under Blamey. This had involved some intelligence work. He came back to the Australian Army as a Major in June 1940. The following is taken from page 83:

Overseas developments in wireless telegraphy and cryptography appear to have been almost ignored by the military hierarchy. In March 1939 the British War Office suggested that an Australian officer, serving in the UK, attend an elementary cryptography course. But by April 1940 Prime Minister Menzies was still querying his Defence Committee's proposal for Australia to have its own code breaking units when the British were handling such matters. It was fortunate that certain naval officers were being trained elsewhere. [Presumably at FECB.]

The reference for this is MP 1185/8 at the National Archives of Australia, Melbourne. Other references are MP 729/6: Secret correspondence files 1936–1945; MP 729/8: Classified correspondence files 1936–1945.

Rogers went to the Middle East in August 1940 as a principal intelligence officer. Thomson uses Ballard's book as a main source on Australian signals intelligence in the Mediterranean area.

Rogers returned to Australia in January 1942 and remained in military intelligence work. Pages 138–139 of the book give some account of the emergency precautions taken in the first six months of 1942. Little new light is thrown on Central Bureau. Indeed on page 142 Thomson erroneously states that:

A small group from naval intelligence under Paymaster Commander R. E. (Eric) Nave [sic, should be T. E. Nave] and Professor A. D. (Dale) Trendall who had been working on Japanese diplomatic codes also joined the [Central] Bureau.

Rogers was appointed Director of Military Intelligence for Blamey effective 1 July 1942. Chapter 14 gives a valuable analysis of the role of military intelligence in the battles in New Guinea in 1942; chapter 15 gives a similar analysis for 1943. Thomson has made proper use of AWM 59, the Willoughby report.

Another error is to be found on page 173: the Japanese code material found in Sio in January 1944 is mentioned but the use of the IBM machines in using it is misunderstood. However the use of signals and intelligence that lay behind the advance in April 1944 to Hollandia, now Jayapura, is properly explained on page 176:

Prior to their landing Kenney's air force had destroyed a great many planes on the ground. Sigint had provided the lucky break for both him and MacArthur.

Pages 179–180 give a useful account of a conference held in London in August 1944 on the co-ordination of all British Empire anti-Japanese military intelligence and co-ordination of it with the Americans.

This book complements Barbara Winter's work on Commander Long of Naval Intelligence.

Barbara W. Tuckman, *The Zimmermann Telegram*, Random House, NY, 1958, 1966.

This book deals with an incident in 1917 in which the then German Foreign Minister, Zimmermann, sent a telegram instructing the German Ambassador to Mexico to try to organise some deal under which Germany and Japan would assist Mexico recover Texas, New Mexico and Arizona. This was a major factor in getting the United States to enter a war against Germany. The interest here is that the whole concept of Japan invading the United States through Mexico was not considered ludicrous. Perhaps the American punitive raid of 1916 on Mexico had left hard feelings. It also describes the relatively minor rôle played by Japan in the First World War.

Mark Urban, *The Man Who Broke Napoleon's Codes: The Story of George Scovell*, Faber, London, 2001.

Location: [See the London 'Guardian' newspaper, 25 August 2001.]

The book describes an interesting early example of the use of code-breaking in war.

E. Van der Rhoer, *Deadly Magic: an account of Communications Intelligence in World War II in the Pacific*, 1979.

This gives the view from Washington of the events being played out in the Pacific. It is not relevant to the Australian sigint scene. However there is some comment on the teaching of the Japanese language to prospective American decoders. More on this matter is to be found in the Maneki book *Heroes of the South West Pacific*.

Gordon Welchman, *The Hut Six Story*.

This account of Bletchley Park, written by a senior member, is relevant here for the account of how the author was recruited and also for the 'hut' structure that was copied by Central Bureau in Brisbane.

C. A. Willoughby, *Brief History of the G-2 Section, GHQ, SWPA, and Affiliated Units*, US Army, Tokyo, 1951.

Location: Australian War Memorial Research Centre, where it makes up file AWM59, and needs four boxes.

The relevant section of this once secret detailed report — it is anything but brief — has been incorporated in section 15 of the main text. It is quite evidently essential reading for anyone carrying out serious research on the Pacific War. It does not appear to be widely known outside Australia.

The Aldrich book mentioned above lists in its bibliography a book *The Guerrilla Resistance Movement in the Philippines* (Vantage, New York 1972) edited by General Willoughby. It contains a chapter *Intelligence at War: A Brief History of MacArthur's Intelligence Service, 1941–1951*. This has not yet been located or examined.

Barbara Winter, *The intrigue master: Commander R B M Long of Naval Intelligence*, in *The Royal Australian Navy in World War II*, edited Dale Stevens, Allen and Unwin 1996.

and also

Barbara Winter, *The intrigue master: Commander Long and Naval Intelligence in Australia*, Boolarong Press, Brisbane, 1995.

Long was responsible for the coastwatchers network before the war. This played a significant rôle in the Solomon Islands and elsewhere in sending information back to Australia. There was also a less significant mainland coastwatchers network.

Besides the coastwatchers' valuable obvious work, they played an unforeseen and unrecognised role. When the Japanese learnt of their existence, they sometimes blamed the coastwatchers when their plans were unaccountably thwarted, instead of suspecting the extent of Allied wireless traffic analysis and cryptanalysis; thus they failed to change wireless procedures in ways that could have made Allied wireless intelligence in the Pacific more difficult.

Long was Director of Naval Intelligence and so played a crucial rôle in setting up Nave's cryptographic activities in Australia.

It was Long who provided the ammunition for the CNS to fight Menzies for approval to set up a RAN cryptographic unit, the Special Intelligence Bureau, under Captain Nave.

The short version does not refer to her sources. However the book, of 330 pages, is the fruit of many years of research and does, for example, give the reference to Prime Minister Menzies letter of 11 April 1940 opposing the creation of a naval cryptographic unit. It also describes the establishment of FRUMEL.

On page 66 of Nigel West's book *MI6* a paragraph is devoted to the British Naval Intelligence Division under Admiral Godfrey in 1939. It was reasonably well staffed and efficient.

There are some mistakes, such as the start of the venture at Sydney University is given as January 1941 on page 52. However the author has performed a major public service in assembling so much information from such diverse sources. It seems appropriate to quote her comment on mistakes given in the introduction to the book:

Intelligence is a fascinating and infuriating subject. Deceit, mystification and secrecy are inherent in Intelligence. You know from the outset that you will not get the full story, not will you even be correct in all you write. In few fields of research will you meet more obstruction and be told more lies. You can only do your best, add a little more to the existing edifice of knowledge, provide a basis on which others may build a little more, and not be too desperately embarrassed about a few cases when you may not have been quite right. No doubt I shall have made some errors and more omissions: in this I shall be in good company. In this field, no writer has got it all correct. Every writer can find faults in the work of every other writer. Some faults are honest mistakes. Some are omissions or untruths to cover information considered too sensitive for the tax-paying public to know. Some are to provide sensations for writer who will not let truth spoil a good story.

F. Winterbotham, *The Ultra Secret*, Weidenfeld and Nicholson, London, 1974.

F. W. Winterbotham's relatively early memoirs explain his role in supervising the distribution of decoded information. Before the war he had picked up valuable information by pretending to have extreme right-wing sympathies, going to Germany, and encouraging various Nazis from Hitler downwards to talk. Sometimes the simplest methods are best! This book makes it clear that the allied code-breaking operation stretched around the world with communications by secure 'one-time' codes.

J. Winton, *Ultra in the Pacific*, Leo Cooper, 1993.

Cited by Aldrich, but not yet seen.

P. G. Wodehouse, *The Swoop, or how Clarence saved England*, Alston Rivers, London, 1909.

Location: This book is quite rare. It was reprinted once and even the reprint is scarce enough.

The Ball-Horner book mentions that the present surge of interest in the gathering of secret intelligence happened before in Edwardian times, but gives no references. This short novel is a spoof on the whole business. However there is some substance to the claim that 32 years later Bletchley Park did save England.

Ray A. Wyatt, *Yank Down Under: from America's Heartland to Australia's Outback*, Sunflower University Press, Manhattan, Kansas, 1999.

Not yet inspected, but apparently it gives the story from the viewpoint of an interceptor of radio messages.

Herbert O. Yardley, *The American Black Chamber*, The Bobbs-Merrill Co., Indianapolis, 1931.

Note: This copy was in all probability consulted by the four academics in 1940.

This is an account of Yardley's interesting career spent between 1913 and 1917, but especially from 1919 to 1929, when in 1929 an incoming new Secretary of State decided that he did not wish the secret messages of other governments to be decoded and ordered that the activities of the Black Chamber cease and the unit closed down. The book is devoted to the detailed descriptions of various methods of coding, from the use of secret inks etc

to telegrams and cables (but apparently with not much derived from radio interception), and to the various types of decoding/decryption he actually learnt/developed during this period, applied to espionage and diplomatic materials. There are also numerous examples of codes, of decoding techniques, and of some of the more serious outcomes from decoding of messages.

Yardley began in the State Dept and remained connected with it. He was recruited by the War Dept during WW1 to set up MI-8, the official designation of the Cryptographic Bureau of Military Intelligence Division, and in fact his work was used by a number of Departments in the Administration. He had shown by 1917 that the coding methods used by the US State Dept and the US Military were childish and easily read, but even in 1929 the State Dept persisted in using easily broken coding methods. He avoided pushing his luck on the encryption side with seniors who felt the development of new methods unnecessary. Of particular interest is the fact that in 1919 he turned his attention almost exclusively to Japanese secret codes, as the US was intensely interested in the diplomatic discussions round the world leading up to the Armament Conference that would be held late in 1921. He managed a major breakthrough either late 1919 or early 1920, and this brought some urgency to the problem of finding good reliable translators of Japanese. It is clear that this was difficult, even in the USA. Yardley writes, on page 275, and I think he is referring to some date late in 1919 or early in 1920:

I had already discussed with General Churchill the advisability of subsidising the Oriental Language Department of some university, giving a four-year language course to about 10 students, then sending the best to Japan for three years, and from the remainder selecting two or three and offering them a future in the American Black Chamber. But this plan would take seven years, and I wanted the job done in seven months!

So the Australian Department of Defence anticipated Yardley by at least two years!

MISCELLANEOUS MATERIAL

The BBC television series *Great Mysteries and Myths of the 20th Century* includes a 30 minute documentary on the intelligence failure relevant to the Pearl Harbor Raid. It was shown on the Australian ABC on 7 January 2002.

A list of items from the *Sydney Morning Herald* follows:

10 Mar 1989	Hastings	Nave too old for legal battle;
10 Apr 1989	Hastings	Warnings of possible Pearl Harbor raid;
30 Aug 1989	Hastings	Codes, wars between codebreakers;
30 Apr 1992	Jenkins	Revisionist Coral Sea history revised;
14 Aug 1992	Jenkins	Invasion warnings were ignored;
19 Sep 1992	Jenkins	War of Words;
28 Jun 1993	Jenkins	Man of compulsive secrecy.
10 Jul 1998	Obituary of Frank Rowlett (1908–1998).	
1 Sep 1998	Obituary of Douglas McCallum.	

And the *Weekend Australian* of 9–10 March 2002 ran a picture on the women of CB; more was published in the Brisbane *Courier Mail*.

There is also a specialist journal: *Intelligence and National Security*

It is published in London and held at ADFA and ANU Libraries. The most interesting paper from the present viewpoint was published in it in 1999. The authors, Drea and Joe Richard of Water Transport Code fame, discuss the documents recently released to the United States National Records and Archives. The Denniston report of 1944 appeared in the first issue.

A NOTE ON ARCHIVAL SOURCES

The following note on archival sources was provided by the Archivist of the Defence Signals Directorate in August 2002.

Central Bureau Technical Records were prepared at the end of the war to summarise the work of the joint Australian-US Sigint effort. The Technical records covered the following areas:

- Part A: Organisation
- Part B: Naval Air-Ground Communications
- Part C: Army Air-Ground Communications
- Part D: Three Figure Systems
- Part E: Naval Short Weather Synoptic Weather Reports – JN36
- Part F: Code Book Analysis and Permutation Studies
- Part G: Mainline Army Systems
- Part H: Traffic analysis
- Part I: Translation Section
- Part J: Field Sections
- Part K: Critique
- Part L: Bibliography
- Part M: Examples of traffic

The National Archives of Australia record series number under which they are filed is B5436, and they are to be found under the title Central Bureau Technical Records. In addition to this material, National Archives of Australia also have a number of other Central Bureau files, under the same record series number in Melbourne, and under the A10908 series, located in Canberra. The Canberra series also contains an interesting report on the wartime history of the Australian special Wireless Unit, prepared by Lt-Col Ryan in December 1945.

Army Directorate of Military Intelligence (DMI) files held at National Archives of Australia in the series A6923 contain much historically interesting material on wartime Australian Sigint in India, Southeast Asian, the Middle East and other theatres. National Archives of Australia have made their record index system available to the public via the Internet, accessible from their home site at <http://www.aa.gov.au>. The Australian War Memorial also has some material, though mostly related to the service wireless units, accessioned as AWM Series 51 and 52.

Central Bureau files are also kept by the US National Archives and Records Administration, as many Central Bureau records were repatriated to the US along with those of General MacArthur's General Headquarters Southwest Pacific Area (GHQ SWPA) after the war. They have been accessioned in the NARA series 'Record Group (RG) 457', which contains material on Sigint in the SWP Theatre; 'RG 111', which are the records of the Office of

the Chief Signals Officer 1940-54; and 'RG 38' which is predominantly US Navy, and so contains FRUMEL records.

There are some other NAA references. Thus 66/301/232 deals with the proposed awarding of American honours to Sandford and Booth. If one searches under 'Sinkov' in 'awm59' the recordsearch system leads to the organisation numbered CA6999, which is Central Bureau, and then to FRUMEL. Then you get to B5554, B5555, A10909, B5553, B5555, CA7137. B5555/2 is particularly important.

The key army file may be found by asking recordsearch to look for 'Room Treweek'.

The University of Sydney archives have useful material in the personal files of Lyons, Room, Trendall and Treweek.

There may be relevant material in the London Public Records Office.