thirty secret years

A.G. Denniston's work in signals intelligence 1914-1944

Robin Denniston

Thirty Secret Years

A. G. Denniston's work in signals intelligence 1914 – 1944

When GC&CS moved out to Bletchley Park at the outbreak of war in September 1939 one observes that the founding fathers of BP – Commander Alastair Denniston, Nigel de Grey, Dilwyn Knox and others – had all learned their trade in the Room 40 … another war kept their hand in at GC&CS through two decades of peace. The tradition of the British is tradition.

Ronald Lewin, *Ultra Goes to War*

The transatlantic alliance forged at Bletchley Park was just as important as the codebreakers' effect on the war.

Michael Smith, *Station X*

Robin Denniston

ISBN 978-09553648 0 8

Published by
Polperro Heritage Press,
Clifton-upon-Teme, Worcestershire WR6 6EN UK
www.polperropress.co.uk

Cover design
Steve Bowgen

Printed in Great Britain by
Cromwell Press
Trowbridge
BA14 0XB

To

Margaret Finch

and

Libby Buchanan

with love

By the same author

THE YOUNG MUSICIANS (Chatto and Windus) 1955

THE MAN WHO MADE THE WORLD (Brockhampton Pesss) 1965

PARTLY LIVING: Some understanding of experience (Geoffrey Bles) 1967

ANATOMY OF SCOTLAND (Chambers) co-editor 1992

YARDLEY'S DIPLOMATIC SECRETS (Cryptologia) 1994

CHURCHILL'S SECRET WAR (Sutton) 1997

TREVOR HUDDLESTON: A LIFE (Macmillan) 1999

CONTENTS

Acknowledgements

Grateful thanks to Candida Connolly for starting me off, and to Ralph Erskine and Mavis Batey for encouragement and valuable information.

Preface

My father's death in Lymington cottage hospital in 1961 at the age of 79 was marked by no obituaries anywhere. He had been in charge of the Government Code and Cipher School from 1919 to 1942: firstly at the Admiralty where he had since 1914 been a long-serving watch-keeper at Room 40 OB (Old Buildings), whose staff spent their wartime years decrypting, translating, assessing and distributing secretly intercepted messages between the German High Command and the Grand Fleet. For this work he was made an officer of the newly created Order of the British Empire and entrusted by Lloyd George's postwar cabinet with the transformation of Room 40 into the Government Code and Cipher School - by 1941 rechristened Government Communication Headquarters. The new team of some 40 people, increased to 60 by 1939 successfully deciphered the diplomatic traffic of Italy, Spain, France, Turkey, several South American republics and Saudi Arabia.

This remained officially non-existent except for a yearly sum set aside for it in the Foreign Office budget. Resources were scarce as the Geddes axe nearly threw out (to mix metaphors) the baby with the bathwater. Nonetheless the product of GC&CS, assessed with care by my father and his helpers, was regularly circulated to a score of government departments and named individuals.

Churchill, by then out of office, had himself set up Room 40 in 1914, still managed to see interesting intercepts through Major Desmond Morton, a friend of his with contacts in the right places.

The interwar years saw a major crisis when the new Soviet leadership's traffic was intercepted and its cipher broken, thanks to Ernst Fetterlein, a Kremlin apparatchik who fled the country after the Revolution and settled in London, commuting daily to Whitehall, where the discoveries of GC&CS were revealed in Parliament, much to my father's disgust, as the new Soviet diplomats reverted to unbreakable one-time-pads. Later, Italian aggression in Abyssinia created a new source of relevant messages and the Italian section in Whitehall was reinforced by art history scholars of the Renaissance.

The great achievement of the interwar years began in July 1939 when my father and a colleague, A. D. Knox, crossed Germany by train and entered Poland to meet their French and Polish counterparts at Pyry near Warsaw. The two middle-aged secret agents - Denniston and Knox - returned through Germany, crossed the channel and, back in Whitehall, produced a German Enigma machine encipherer the Poles had given them. A fortnight later WW2 started and the department moved to Bletchley Park (see chapter 7).

The rest is indeed history. Why, then, did not *The Times* and the *Guardian* publish any reference to my father's life and death in 1961? I have spent time since then trying to find out. By 2001 his lifework had been scrutinised by leading historians of secret intelligence, and his entry in the new Oxford DNB by Ralph Erskine is a true and lasting tribute to this silent and enigmatic figure.

Following his retirement on 1 May 1945 on an annual pension of £591, my father took, briefly, to schoolmastering but found the going too hard, so he and my mother retired in the New Forest. Later, in 1958, my mother died of breast cancer, so my father went to New Milton where my sister Margaret lived with her family after she married the vicar there, Geoffrey Finch. She looked after the frail and distraught father she loved until his death two years later. It is to her memory that I dedicate this short book. I also dedicate it to his favourite niece and god-daughter who wrote this as the book was going to press:

> Alastair Denniston was not only my favourite uncle but also a very special Godfather. How lucky I was that my Mother, always deeply proud of her brother, asked him to undertake this extra duty! It made us especially close.
>
> This special warm relationship began when I was shipped off to school in Kent at the age of 13. At the beginning of each term he would meet a very fearful child off the train from Leeds at Kings X and take me quietly across London to the 'school train' at Charing Cross. In spite of the heavy burden he must have been carrying at this time - 1936-38 - he appeared to me to have all the time in the world for a very nervous homesick youngster, chatting warmly about his very special sister (my mother) and all our family 'doings', and telling me of the holiday escapades of his beloved son and daughter - my cousins Robin and Y.

I remember once he told me that he had decided to swap birthdays with his son Robin, who was born on Christmas Day. He and his wife had decided that a small boy should not have to cope with birthday and Christmas on the same day so that was why Robin should always celebrate his birthday on December 1st. He would be very happy to have his on Christmas Day, and so it was until Robin was grown up.

Holiday times often brought the two families together, either with us up in Yorkshire or in the South. I was invited down to their cottage at Barton-on-Sea. Uncle Alastair met me again in London and the drive down was yet another chance to get to know each other. He said to my mother after the trip that getting me past Walls Ice Cream 'Stop Me and Buy One' bicycles was like getting a dog past lamp posts! I remember that the sun always shone at Barton.

Perhaps one of the happiest and most recent memories of Uncle Alastair was well after the war when he would come to Yorkshire to stay with my parents in Upper Nidderdale. My father had a grouse moor and shooting days were full of expectation and excitement. Beaters sent out to drive the birds forward were an integral part of the organisation. Uncle Alastair - with no wish to use a gun -lined himself up with the beaters with his white flag and stumped across the heather. Everyone loved him and you could hear the other beaters call "Come on Uncle Alastair" or "Are you alright there, Uncle Alastair?" Everyone really enjoyed his company, not remembering that he had won the war for us, but because he was such a genuine quiet loveable person.

Beside my bed, in its original red and black Swan pen box, I always keep his silver pencil which his children gave me, accompanied by a letter written to me in Canada for Christmas 1960, signed, as ever, 'your affectionate Godfather'.

The letter from my father she refers to was written six week before his death and is reproduced in part overleaf to show how strong his handwriting remained.

Robin Denniston October 2006

New Milton 150

ABBOTSFIELD
BURLEY NR RINGWOOD
HAMPSHIRE
TEL. 3105

The Rectory
New Milton
Hants

2.12.60

My dear Libby,

A brief note to wish you
all a very happy Xmas. Thos
shown me the photo of the family
& I was amazed to see how big
they all are. Jamie seems almos
outsize for his years.
I can't help enclosing the usual
little book but please do any of
it is really superfluous & they have
most suitable ones in Canada
I shall quite understand & desist
but I am had several very cheerful visits
from your Mother who seems to be
getting off Mr. years rather than
collecting them. Nobody would

Part of the letter written by Alistair Denniston to his niece and god-daughter, Elizabeth Currer-Briggs, in December 1960 shortly before his death.

CHAPTER ONE

A. G. Denniston 1881 – 1941

I

My father was born on 1 December 1881, the eldest of three children. Their parents, my grandparents, had met in the early 1870s, and married when my grandfather, then a 23-year-old doctor who failed to get a post in Edinburgh where he graduated, took employment with the Stafford House Mission. This sent doctors, nurses and supplies to war stricken Turkey, and in 1878 Dr James Denniston found himself in charge of a large hospital in Erzurum, tending the Turkish soldiery dying daily from wounds, dysentery and frostbite in the inhospitable climate of the Eastern Anatolian plateau, attacked by their aggressive northern neighbours and ancestral enemies, the Russians. Dr Denniston's skilled work as a surgeon was highly rated by Turkey. He also wrote back to his fiancée describing vividly the plight of the young Turkish conscripts who suffered and died despite his ministrations and those of his colleagues. His fiancée was Agnes Guthrie whom I remember in the 1930s as a little old lady (barely 5ft) in quiet retirement in a Kensington nursing home, visited daily by her elder son, my father.

Back from Turkey Dr James took a job as GP in the wet and windy Argyll seaside resort of Dunoon where his children were brought up and schooled. This is not a book about him, but it is recorded how kind and skilled he was at tending the illnesses of his patients, mainly poor, who would reward him with a chicken if they could not pay fees. He started the cottage hospital in Dunoon, and his name and work is still respected there, in the records. He did not return from Turkey unscathed, for he contracted TB as a result of his work amongst the dying Turkish soldiery. When his children were very young the family moved south, to Cheshire, where it was thought the climate would be better for his condition. It was not. He was advised to make sea voyages, in the belief that the sea air would cleanse his lungs. It did not. He travelled as ship's doctor across the world, at one stage taking his wife and infant daughter, Biddy. He died when my father was 11.

Alastair Denniston, like his younger brother Bill and sister Biddy, was clever and resourceful. He kept many of the prizes won at Bowdon College. He did not go to a British university but to French and German ones – the Sorbonne and Bonn University.

These are hidden years. There are no letters. Perhaps there are records in Paris. Where did he stay? Was it a lonely life? Who helped him? We shall never know. He certainly became a trilingualist, able to compile a German grammar much used in British schools. He spoke and wrote French fluently, as did most Foreign Office officials.

He was a bright, resourceful young Scotsman with little behind him. He was also a brilliant athlete, playing hockey for Scotland in the 1908 Olympics. He played games when he became a language teacher at Merchiston Castle, Edinburgh and later at the Royal Naval College at Osborne in the Isle of Wight. He continued to play until his retirement in 1945.

In late 1914 he was called up to the Admiralty at the start of World War One, because of his German expertise. German naval wireless messages were being intercepted and their Lordships realised that if they could be decoded, translated and distributed within naval circles they might help the war effort against Germany. So he joined Room 40 OB in the Foreign Office, staying on till 1919 and later becoming head of the interwar bureau called the Government Code and Cipher School, which took over the wartime work of Room 40 OB. GC&CS flourished and succeeded, in absolute secrecy, in reading diplomatic intercepts from all the major nations recovering from the war, becoming, by 1938, the fledgling GCHQ which is still with us.

By his own efforts he remained head of GC&CS until 1942 when he returned to London from Bletchley Park and supplied the British Government with the diplomatic intercepts which kept the recipients in daily touch with the strategic thinking of friends, enemies, and particularly neutrals. That was his life work and his great achievement.

* * *

II

1941 was a terrible year for the Allied war effort. But when on 7 December the Japanese destroyed many of the US's finest ships at Pearl Harbor, relief was felt by all with privileged access to the daily progress of the war, and by none more than my father.

From 1940 he shared with the Prime Minister, the service ministries, the British commanders-in-chief and a few close colleagues at Bletchley Park where he worked, daily access to the intercepted, decrypted, and translated messages of the German Air Force (since early 1940) the Abwehr and the commanders of the U-boat offensive in the North Atlantic. He also monitored and distributed the diplomatic and commercial decrypts of all the major neutral powers like the USA, Turkey, Siam, and much valuable information from two of the three Axis powers, Italy and Japan.

It was within a day or two of Pearl Harbor that his colleague since 1916, Dilwyn Knox, with a few lady assistants of intelligence and discretion, broke into the German Police/Abwehr/Gestapo Enigma. It was another of my father's secret colleague over 25 years, Nigel de Grey, who mastered the implications of the Gestapo reports of the slaughter of hundreds of thousands of Jews in Eastern Europe, at a time when the USA and the USSR were still undecided whether or not to stay neutral in the European fracas, soon to become WW2.

In January Britain faced a bleak future. The invasion scare was still on. Her allies were few and far between – Canada, Greece, Australia, South Africa, India, New Zealand – while the enemy had conquered the whole of Eastern Europe from the Baltic to the Black Sea and were flushed with victory. We were not downhearted, but it's difficult with hindsight to see why we were not terrified out of our wits.

In the fourteen months that followed, many things went from bad to worse; but two important events, closely charted by Bletchley Park, assured those in the know that Hitler could not win. The first was when, after the early months of 1941, he expanded the Greater Reich – already in Jugoslavia and Bulgaria – into the Ukraine, Byelorussia (now Belarus) and to the gates of Leningrad and Moscow. Hitler had turned against his real enemy, the Soviet Union, and brought Stalin in on the Allied side on 22 June. The German eastward advance of the autumn against well prepared, brave and effective opposition from Soviet armour and soldiery, seemed and nearly was unbeatable. It stopped only at the gates of Moscow after the most gruelling and devastating land battles in history.

The second was in the Far East, where Japan's hostile intentions against British imperial interests had been followed as assiduously as those of the Axis powers by Bletchley Park. By the autumn indications were clear with those who understood the import of the diplomatic and naval 'messages' intercepted, decrypted and circulated by the Japanese section there, that the war would spread, and Japanese imperial aggression finally ensured American participation on the Allied side. That was what Churchill had worked for so unremittingly. It was this that saved Britain from invasion and ultimately ensured victory.

But before that and despite the successful British campaign in North Africa against the Italians and later Germany, our losses in the battle of the Atlantic brought us almost to our knees. Tonnages lost in those 14 months all but crippled the British war effort. Later in the year Japanese successes in the Far East produced yet another spectre of gloom, defeat and disgrace. The southward campaign which brought Hongkong under Japanese hegemony on Christmas Day 1941 was followed by the fall of Singapore in February 1942. Sir Alexander Cadogan, FO chief who had already been through so much, told his diary, 'This was the darkest day of the war'.

So 1941, though a horrendous year of crisis, new enemies, revelations of our own strategic and naval weaknesses against the might of the German *Wehrmacht*, saw also two events which eventually made victory certain – Germany's declaration of war against the Soviet Union in June and Japan's declaration against the USA, following Pearl Harbor on 8 December.

* * *

III

Churchill called in at Bletchley Park on January 31, 1941, to see the codebreakers at work. Under conditions of maximum security 2,000 specialists were now staffing this extraordinary institution and enjoying dramatic successes despite shortages of clerical labour and equipment. He must also have called at Lavendon Manor, where the Diplomatic Section was working on American, Hebrew, Spanish, Italian, Russian, Vichy French, German, Japanese and other diplomatic ciphers, because Cadogan's diary refers to WSC and Eden both happening to see an intercept which makes it look as though we might get the Germans out of Afghanistan. One section was even working on American cipher messages, and Commander Alastair Denniston, their chief, would recommend that ('in view of ultimate peace negotiations') they keep abreast of Washington's code changes, despite the currently superficially 'intimate' relations.

In February 1941 Bletchley Park was growing too fast for its existing management structure. The service ministries, in particular the War Office, found its anarchic, apparently chaotic and haphazard management unacceptable. The generals and colonels well knew the value of BP's product but felt administration should be in more professional hands. When it was discovered that two key positions – of chief billeting officer and of 'auntie' to the dozens of young female secretaries, cryptographers and service people – had both been filled by my father with his personal friends, it was inevitably assumed that he was out of his depth. Yet those two appointments actually turned out well. The billeting officer was Leslie Reid, our next door neighbour when we lived in Chelsea in the early 1930s; and the aunt-figure was the wife of the deputy head of MI6 reporting to 'C', Valentine Vivian. Both were able, experienced, efficient, committed and discrete managers; neither had any qualifications. It was to be over a year before the great change was made which resulted in his removal from Bletchley Park. And his hand on the tiller at Bletchley became more spasmodic in the first half of the year as a result of two things – his increasing ill health and his two visits to North America to build the USA-Canada three-way liaison with Bletchley – the success of which crowned his secret career and eventually brought his achievement into the history books.

On 27 February he was diagnosed in Harley Street with a stone in the bladder. Only two days later he was entertaining a trio of the top American cryptanalysts to lunch at the start of the close signals intelligence Anglo-American relationship, now documented in the archives of both allies.

Bletchley Park was of course in hourly touch both with the French cryptographic effort, evacuated and exiled as Vichy France took over the whole country, while the great Polish founders of the Enigma attack, barely escaping with their lives via Romania, France and Spain, fled from country to country until they reached England where they were left to low level interception at the Polish HQ at Boxmoor, Surrey.

So the productivity of Bletchley throughout 1941 contrasted with its chaotic management. In April AGD asked 'C' to ask Lord Hankey to recruit more mathematicians for BP. By June he had been away for two months without delegating full responsibility to his second-in-command. Lacking a leader, quarrels broke out. The service ministries never liked civilian control of their personnel or the product they had come increasingly to value. In C they found an unhelpful opponent. Yet he had little grasp of what was going on at Bletchley and confidence between him and my father was not strong. No contact between them appears in the released documents of the period. No-one knew how long my father's ill health would last, or whether and when he would return to full-time duty with facilities unimpaired.

Meanwhile, minutes of June management meetings show BP accused of sabotaging interservice co-operation; Birch became overlord of both Italian and German naval sections; Cooper called for more resources for his (air) section. BP was in direct touch with French crypto (Bertrand) and also supplying machines to the Finns. Also cipher breaking was increasing at the Middle East HQ. BP tasked eight Polish signals experts stationed at Stanmore to cover Soviet Air Force communications.

Security and adequate accommodation for new staff were constant headaches for the interim management. In July the diplomatic section was relocated from Elmer's school to BP. More Vichy and Free French ciphers were becoming available to BP. Travis reprimanded Saunders for going over his head about building needs for the expanding Hut 3, and threatened him with instant dismissal. BP's relations with RSS 'Radio Security Service' caused concern, and a bright spark from RSS, Hugh Trevor Roper, was declared persona non grata there. No future visitors by outsiders to BP were to be allowed unless sanctioned by Denniston.

With Russia an uneasy new ally and under great pressure following the Wehrmacht's successful invasion, cipher security as well as the need to get vital information to the Russian High Command – Stalin – quickly, accurately and convincingly, was making slow progress but in September BP reported to Churchill that Hitler was about to turn his armies against Kiev; the outline

of a Nazi plan to destroy three Soviet armies on the central eastern front, and that the German offensive against Moscow would begin on 2nd October.

In September BP's other star mathematician, Gordon Welchman, reported to Travis his plan to upgrade and extend the remarkable successes of Hut 6. It had been decided that, in the event of an invasion of Britain, still in everyone's minds as late as 1942, BP was to relocate to GHQ Home Forces and contingency plans were in place, though never tested. UK Sigint effort against the new ally Russia, the Soviet Union, was wound down and cipher cribs and clues exchanged with Moscow.

In the middle of October Churchill made his historic visit to BP. Later that month large scale building plans for BP's new needs were developed. In November Dilly Knox and my father corresponded vitriolically but affectionately about the current management and Knox's Enigma breakthrough. AGD reported on his trans-Atlantic visits, having deprived Herbert Yardley of his job running Canadian Sigint in Ottawa and re-established mutual confidence between BP and the American centre at Arlington.

On December 2 BP translated a second highly significant Japanese telegram from Bangkok to Tokyo, which reported that in order to 'set up' Britain as the aggressor against Thailand, elements in the Thai cabinet were suggesting that Japanese forces should land at Kota Bahru obliging the British forces in Malaya to invade from Padang Besar, whereupon Thailand would declare war on Britain.

The American codebreakers remained disgruntled to the very eve of war in December 1941. BP still refused to release the Enigma secrets to Washington. On Dec 5 the archives show, Commander Denniston nevertheless cabled to Captain Hastings (UK liaison chief) to Washington 'I (AGD) still cannot understand what Noyes (US) wants'. With regard to Purple (US cipherbreak) he grumbled the British had already given the American codebreakers all they asked for, thus enabling them to 'read all that we can read.' AGD continued: 'The main means of communication is ENIGMA. Twice, in Feb and July 1941, we captured keys for the month which we sent to Washington.'

BP noted: 'I do not know if the American army cryptographers know that we are reading Japanese BJs'.

Denniston had confirmed the free exchange of all Axis intelligence during his August visit to the USA.

It was that summer of 1941 that the Americans sent a letter to BP asking for a cipher breaking machine. My father was aghast, as nothing was ever put on paper about 'E' - the Enigma secret. With a degree of frostiness in his reply AGD reminded the Americans that while 'E' was a matter of academic interest to them, it was a matter of life and death for the British... The Germans are always tightening up their cipher discipline and evolving new methods, and BP's codebreakers felt they were "teetering on the edge of a precipice, they might be struck blind at any moment by a sudden German innovation". The Washington visit talks would tackle the most sensitive subject namely the further exchange of codebreaking materials. At present, Denniston noted, this exchange is working very well but only on Jap - a ref. to the MAGICS.* Britain (noted AGD) could not transfer the Enigma secrets to the US, at most they might ship raw intercepts to Arlington and invite the US to try their hand at solving them. AGD hoped to set up a triangular liaison BP-Washington-Ottawa when he arrived on Aug l2, and 'would then visit Ottawa, if this could be arranged without meeting Yardley'.**

Denniston was shaken by what he found in Washington. He visited the US's radio monitoring station at Cheltenham, 30 miles from Washington but the country had nothing like GB's own empire-wide Y radio-monitoring service. 'It seemed incredible this feud between army and navy in USA, but this was what powerful vested interests involved had decreed.' The US, my father reported, had done wonders with Magic but neglected JN (Japanese navy material). As a result of AGD's visit the US naval codebreakers had only now undertaken to being collaborative with BP and the FECB in Singapore in investigating Jap naval cyphers and AGD stated they now regard this as one of their most important research jobs.

In my father's report on his US trip 31/10/41 (HW 14/45), he said he found the Americans - apart from their magnificent work on MAGIC - scratching at the outside of the Italian, French and South American problems. He subsequently sent them all he knew about these as well as the French Colonial, Brazilian, Portuguese, Swedish and other ciphers GC&CS had penetrated.

Some of these enigmatic messages were taken by permission of the author from *Churchill: Triumph in Adversity* by David Irving. They confirm the importance Churchill and the British government attached to my father's visit and its long-term influence on future US/UK co-operation in war and in peace.

* * *

* MAGIC was the code assigned to Japanese diplomatic traffic intercepted by US intelligence as a result of the breaking of Purple, the Japanese diplomatic code, in 1940.

** Herbert Yardley, a maverick American cipher-brain, was considered a security risk.

IV

My father had written to Menzies, regarding his American visit:

1. Our American colleagues have been informed of the progress made on the Enigma machine.
2. They undertake to carry out their instruction to preserve the secrecy of this work and only their directors will be informed under a similar pledge.
3. Complete co-operation on every problem is now possible and we are drafting plans for its continuity.
4. As we cannot contemplate sending any senior member of our staff at present, it may be necessary to select some officer in our Embassy at Washington to act as our liaison with their section. Perhaps you will nominate a suitable man.
5. As to telegraphic communications we have agreed to use the Anglo-American Naval Cipher with individual tables (OTP) which we are supplying (EWT). Our friends will arrange with their Embassy here for the receipt and dispatch of telegrams on their private cable. It will be necessary for us to arrange for a messenger to be available at Broadway to take or fetch telegrams on our behalf.
6. As to interchange of material, I presume we can use our diplomatic courrier (sic) service to Washington when the liaison officer referred to in para 4 has been nominated; they can no doubt use their courrier service and the bag can be collected by our messenger (mentioned in 5).

Denniston's radical and innovative scheme for the free and complete exchange of cryptanalytical tools and product with the Americans was not followed up. This may well have to do with his increasingly painful genito-urinary condition. On 27 February, he had been diagnosed in Harley Street as having a stone in his bladder but had nonetheless managed to give lunch to the main US cryptanalysts, Rosen and Kullback at Stapleford Mill Farm where the Denniston family lived.

He was fully stretched with the increasing workload and amazing productivity of Bletchley Park. Work often kept him at BP by night as well as by day. Thereafter the removal of his stone and consequent painful orchitis kept him hors de combat.

Hindsight causes me to wonder whether at some point Menzies intervened and provided at government expense the medical and surgical care my father desperately needed. But he seems to have paid both hospital bills himself. His illhealth continued intermittently until his second American visit in September

1941 when his hosts, and in particular William Friedman, by now a good and trusted friend, had organised hospital treatment for him in New York, where the doctors employed a new irrigation technique which completely cured him. Of this visit one of the three leading American cryptanalysts wrote later: 'that it laid the foundations for the collaboration between the cryptographic activities of the US and the UK which produced intelligence vital to the successful prosecution of World War Two. We spent considerable time together discussing the technical activities undertaken by both countries and worked out some of the details of our early collaborative efforts.'

* * *

V

My father shared with Churchill, Menzies and few others access to all Enigma messages (Ultra) of the German armed forces, as well as the diplomatic and commercial secret messages of the leading neutrals, particularly Turkey and Spain. The early months of 1941 were devoted by the British Foreign Office to attempts to pull Turkey into the war on the Allied side. It was in the end a failure, but Churchill pursued it unceasingly from 1941-3. Hitler had already overrun Poland, Hungary, Romania and Bulgaria and in early 1941 Jugoslavia, threatening Greece and Turkey. The brave Greeks resisted and joined the Allies while the Serbs added new strength to Axis activities in the Balkans. The British first sent the BEF (British Expeditionary Force, last seen at Dunkirk) to Greece, but pulled it out when it was clear there was no way Greece could be defended from the Nazis as well as Britain itself. The German invasion of Crete completed German superiority in the Eastern Mediterranean. All eyes then turned on Turkey.

For me, my first year as a scholar at Westminster in exile included a scout camp which ended on 16 August, when I returned to Stapleford Mill Farm. My father was far away. He had left on 10 August for the first and shorter of his two transatlantic visits. After a week at home with Y (our mother still worked at BP but was given compassionate hours to look after us) he was still away. We had no news of him. The Battle of the Atlantic was in full swing and we only knew that he had flown rather than gone by sea, as he had expected ('Voyage', he wrote tersely in his diary, later changed to 'Flight'). BP were worried, my mother was worried, we were desperately worried. My dog Jaimie had walked into a ditch and died doing his bit to save rations. In fact my father was safely flown by Transport Command but many such planes were regularly shot down by the Luftwaffe. Crossing the Atlantic by sea was still more dangerous. By 8 pm on 23rd August we were reduced to sitting in the blackout, waiting and wondering. Perhaps my mother had some inkling that he was all right, but not certainly. There was a heart-stopping moment before we heard the crunch of car tyres on our farm track. Could it be? It was too much to hope. But it was.

It had taken him 15 hours flying from New York to Gander, Newfoundland, across the North Atlantic to Prestwick in the bomb rack and thence to Hendon where he was collected and driven home.

It was the best moment of all our lives. He had had an amazing week but he could not tell us anything about it. That did not matter. What mattered was that he was alive and okay. I relive that moment even today. Travis had cabled

him on 8 August that 'All well Soulbury 7' (our telephone number) but we had no word from my father until his return.

* * *

VI

BP had had a successful war, and Whitehall by now was well aware of it. BP could write its own future as well, later, as record its own past. The result was two-fold. The future of GCHQ is a matter of record. It became a leading player in the Cold War, with huge investment in electronic surveillance, in alliance with NSA. But its future was a product of its past, building on the successes of Sigint interception, cryptanalysis and decryption on the work of BP.

But this past extended back well beyond the war years of BP's glory. It extended back to 1919 when the GC&CS was first set up and transferred from the Admiralty to the Foreign Office, and in fact to the autumn of 1914 when the interception of wireless messages passed between German ships to German High Command brought into being the vital cryptographic work of Room 40 OB. My father was one of the earliest recruits to Room 40, in 1914, became the Head of GC&CS in 1919 and remained so until February 1942.

He was thus the right person for senior staff at BP to have contacted when writing up its war work. But by 1944 there were few there who had any inkling of the importance of GC&CS prewar. Received wisdom by 1944 insisted that GC&CS was completely unprepared for war, failed to take on the mathematical needs of machine decipherment, run by amateurs unable to cope with Treasury mandarins, the needs of the armed forces or the requirements of BP's enhanced wartime capability.

My father was quite aware of this. Though after February 1942 he seldom went to BP, he kept in touch with some old friends. It was in this context that he decided in late 1944 to offer his own account of GC&CS's interwar years which began with a remark of Group Captain Sir Eric Jones, BP's supremo after my father and Travis, about this period. 'It would indeed be a tragic and retrograde step for intelligence as a whole and therefore.... for the future of the country if GC & CS were to slip from the record.'

In December 1944 my father wrote, and my mother typed, 'The GC&CS between the wars'. It was circulated within the office and carefully studied by its recipients, comments were sent hither and thither between Whitehall and BP. They are all now in the National Archives. No criticism was made of any of the facts though there appears to have been no comment on the generosity with which he praised his colleagues.

My own reaction to it, after I read the comments, was to focus on critiques

by his colleagues who also remembered the interwar years – in particular Josh Cooper and Nigel de Grey. Since I knew, having visited him shortly before his death, that Josh retained friendly memories of my father I was surprised at some of the apparently dismissive comments he made until I realised that he was addressing himself at this time to a group of BP leaders and historians who had fixed ideas about the inadequacies of GC&CS before 1940 in general and AGD in particular, so would not, perhaps could not, voice openly what he may have felt. So I referred the filed critiques to Sir Harry Hinsley, and asked in 1996 for his comments. In an undated reply on the back of college meeting minutes he had interesting remarks about the Cooper and de Grey's critique:

'Josh in Para 9 is right to stress that it was AGD who recruited the wartime staff from the universities with visits there in 1937 and 1938 (also 1939 when he recruited me and 20 other undergraduates within two months of the outbreak of war). I believe this was a major contribution to the wartime successes – going to the right places and choosing the right people showed great foresight … There were many predators (the Services seriously thought of winding GC&CS down when the war came) and Josh would agree, I'm sure, that it was necessary to be diffident and understandable to be nervous. He quite rightly adds at the end of para 20 that AGD remembered WW1 very well but was tied by the narrow terms of reference imposed on him from above. This is an accurate conclusion.'

Of de Grey Hinsley wrote:

> 'He says that more was achieved cryptographically before the war than is generally recognised, but that the over-all effort was limited by lack of funds as well as forgetfulness of the lessons about signals intelligence in war. But he added that the fault was not all or mainly the fault of GC&CS. "National policy was directed by axemen – very difficult to fight".'

Of my father and Tiltman, Harry Hinsley wrote:

> 'In 1939, I was interviewed in St. John's College, Cambridge, briefly and informally, by two men I came to know very well: A. G. Denniston, the head of Bletchley, and John Tiltman, the chief cryptanalyst.' (*Codebreakers* p.77)

* * *

VII

Churchill himself was no stranger to the type of work done at Bletchley Park. 25 years earlier, as First Lord of the Admiralty, he had drawn up the protocol under which naval intercepts of German navy signals were decrypted, translated and assessed in Room 40 at the Admiralty. The orders he then issued to cryptographers, among them my father, were unworkable but the thinking behind them was sound. Britain had a secret weapon of vital importance to the war effort if properly and discreetly used. Room 40's great triumph in World War One was the breaking of the Zimmerman telegram, in which the German Foreign Office urged Mexico into the war against the United States. Decrypted by two of my father's colleagues, the Rev. William Montgomery and Nigel de Grey, it was successfully 'spun' by Admiral Hall, his boss, and eventually became instrumental in bringing America into the European conflict. In 1924 Churchill told Austen Chamberlain, 'All the years I have been in office since the autumn of 1914 I have read every one of these flimsies (papers on which relevant messages were distributed in Whitehall) and attach more importance to them … than to any other source of knowledge at the disposal of the state'.

The 'flimsies' had by this time been called 'bjs' (blue jackets). My father, who in 1919 was appointed head of the Government Code and Cipher School, took forward the work of Room 40 into and beyond the interwar years; thus he and his colleagues all knew in 1940 that GC&CS had in the new prime minister a keenly attuned ear and eye to their product – information on the German Wehrmacht provided, on a daily basis, in absolute secrecy.

Throughout the interwar years Churchill, mostly out of office, still saw bjs, probably through his friend Major Desmond Morton, and read the monthly volumes circulated to a few in Whitehall.

* * *

VIII

After February 1942 AGD and about 70 staff from the diplomatic section at BP (housed separately from the main buildings at Elmers End) removed from Bletchley, so they had just over a year to re-establish themselves in Berkeley Street, above a couturier's shop. The staff grew rapidly in numbers to 200 including the commercial section (the suppliers of information to the Ministry of Economic Warfare on German imports of manganese, bauxite and other raw material for making war) in nearby Aldford House in Park Lane. It was a simple job to re-establish the way they worked at 55 Broadway before the war. They were well dug in by May 1943 when Colonel McCormack made his recently declassified report on British diplo successes against enemy, neutral and friendly nations.

In that time the war itself had at long last turned in the Allies' favour. The low point, for Churchill, had been the fall of Singapore in March 1942, while the war at sea was still dominated by Doenitz's U-Boats whose cryptographers had early on mastered the British naval ciphers, though BP's success against German naval enciphering, still spasmodic in 1943, was eventually to give our admirals the upper hand, so that convoys could cross the Atlantic to and fro without catastrophic losses in naval tonnage, which Churchill admitted in his subsequent war history 'gutted my bowels'. Victories in North Africa and some successful negotiations with Palestine and Transjordan still occupied him as well as 'getting Turkey in'. Wavell's low level international diplomacy irritated the great man until he found in General Auchinleck a less risk-averse commander-in-chief for the whole area. At this point Churchill turned his attention to the neutrals in general and Turkey in particular. Earlier Churchill had written to General Inonu, the Turkish premier, giving him good strategic advice on how to keep his country out of trouble by letting the Anglo-Saxons use his aerodromes to take off against the Luftwaffe and thereby try to wrest air supremacy from the Germans in the Eastern Mediterranean. The notion of air supremacy was news to the Turkish generals who had few combat aircraft of their own, no knowledge of the new wonders of radar, still less of international cipher-breaking now practised by both sides, so Inonu remained unconvinced, and stayed that way throughout the war, equally unimpressed by similar German diplomacy, conducted by their highly placed ambassador, Fritz von Papen, in Ankara.

So AGD's diplomatic and economic work moved to the forefront of Churchill's armament of information which by mid-1943 was thought of as equal in importance to BP's service work; Colonel McCormack's report makes this clear. But before the full account of this magisterial report, a confirmation of

the high standing of Berkeley Street is to be found in a rarely cited message: Philby's dry account of how he involved AGD in the study and use of thousands of mostly Ankara-Berlin diplomatic decrypts Philby had obtained by sleight of hand from Allen Dulles in Switzerland: solving these finally enabled AGD and his colleagues to break the German diplomatic cipher. For Philby explains to his readers – primarily the KGB in Moscow, followed by the many Russian readers who liked spy memoirs as much as British readers did, and eventually to readers in half a dozen foreign languages, including Serbo-Croat – that he went to AGD rather than BP since it was common knowledge for the cognoscenti that Menzies had hived off diplo from service traffic the previous year. Philby's memoir was published in 1976, some years before the existence of Bletchley Park and its war work and workers were officially acknowledged.

According to P.W. Filby (no relation), Berkeley Street worked 18 hours a day 7 days a week, and achieved many successes. Colonel Alfred McCormack, the influential deputy head of the US army's special branch, which supervised signal intelligence in the US War Department, was extremely impressed by Berkeley St. during a lengthy visit to GC&CS in 1943. He informed the department that 'it would be absolutely astonished 'by the resources of intelligence … here in Denniston's show, waiting for someone to tap them' (cable 4952 of 2 June 1943, 'Colonel McCormack's trip to London) - Denniston continuing his policy of co-operating fully with the US, had turned his people over to us for questioning and give us a free run of his place, more than anyone else in GC&CS (conversations with Denniston) Colonel McCormack's trip to London'.

McCormack wrote lengthy reports on Berkeley Street which the National Archives in Washington DC released only recently.

McCormack was not the only officer to be impressed by Berkeley Street and its 62-year-old head. Brigadier Telford Taylor, who later went on to understudy the chief American prosecutor at the Nuremberg trials, became a close family friend and used to come to our house at weekends, where he played tennis, swam and drank whisky which he thoughtfully brought with him as it was unobtainable round our way. My mother and sister both fell in love with him – this handsome hero, like Cary Grant, my mother said later, but taller. Telford, my father and I went on a bicycle tour of the Cotswolds that year and I have a photo somewhere of the brigadier in full uniform mounting my mother's low crossbar bike (skirts were worn by lady bicyclists) about to pedal up the long hills on deserted roads.

CHAPTER TWO

Room 40: 1914-15

Written by A. G. Denniston in 1919, and now held at Churchill College, Cambridge as DENN1/2

This is the personal memoir of the build up and staffing of Room 40, the government's signals intelligence centre in Whitehall. Work started in 1914 and as the scope of the work increased new talent – people with fresh blood – were needed. Yet there were never more than 40 people working full time shifts on the deciphering work. It will be necessary to mention many names but without giving the biography of the owner. In the earlier stages of development, new men were sought who had but two qualifications; a good knowledge of German and a reputation for discretion.

Cryptographers did not exist, so far as one knew. A mathematical mind was alleged to be the best foundation, but it must be noted that except for Sir Alfred Ewing, Henderson, Russell Clarke and Hopkinson, no one had such a reputation, and in fact the majority of those chosen had actually had a classical training. As time went on, when assistance of a less skilled nature was urgently required to work for these self-trained cryptographers who knew German, ladies with a university education and wounded officers unfit for active service were brought in, and finally expert typists were admitted when the need for their help was almost too apparent. It should be noted in the light of later experience that the last should have been the first, or at any rate let it be said that every expert cryptographer must possess at least one typist skilled in sorting, filing and analyzing.

On the outbreak of War in late 1914, the Admiralty W/T station appointed for police duty received various signals, of which the only thing that could be said was that they were not British. These were at once supplemented by signals intercepted by various stations belonging to the Marconi Co. and to

the Post Office. The Admiral in charge had no staff prepared to deal with this unknown and unexpected occurrence. He therefore suggested to Sir Alfred Ewing, the Director of Naval Education, that Education would probably be considered of little importance for the next few months and that, further, this mass of intercepted telegrams was possibly in code, a subject in which the D of E was known to have interested himself. He also provided Sir Alfred with the photograph copy of a German Code obtained by the Secret Service. (This ultimately proved to be no good).

Teachers at the naval colleges of Osborne and Dartmouth being on leave, the D of E was able to obtain the services of several of the modern language men from these colleges and thus it happened that several men who ultimately became permanent members joined up temporarily in August 1914 (including myself, Anstie, Hooper and Bond who all first met German signals at this period).

It is necessary to digress here to introduce the activities of the War Office. The same phenomena of intercepts had been observed in the Military Intelligence Directorate and in the first week of the war Colonel Macdonagh called in Sir Alfred Ewing to inform him that the W.O. had instructed Brigadier General Anderson to investigate these intercepts and to propose some form of amalgamation. Sir Alfred agreed to send a representative to work with General Anderson and what might be called the prenatal life of the cryptographic section began.

In those days the very amateur and inexperienced staff were greatly elated if they could obtain some sense from the P/L intercepts. It was the time now of the German advance into France, and their movements could be directly observed from the study of the en clair. Code and cypher were however not neglected. Sir Alfred's party had fastened on to an obvious 10 letter code sent out by what were now known to be high power German stations to receiving stations in Africa and elsewhere. The staff included no one who knew anything of W/T procedure but, with the help of Mr Bradfield, a manager of the Marconi Co., various call signs were identified as German possessions. Code books of German commercial firms were collected and the investigations proceeded without, however, any discovery beyond the fact that Germany was communicating with her colonial governors and others.

The staff under General Anderson learned how to analyze. This they did with the utmost enthusiasm and entire lack of discretion. It was afterwards clear that military cypher messages were confused with naval codes and call signs figured as standard groups. But this staff did learn how to file and analyze. In

the course of a few weeks codes and cyphers could be separated, and when about the middle of September the French gave G.H.Q. the method and the key of the military cyphers, no time was lost in settling down to decipher. Watch keeping was organised in the W.O. with the assistance of some of Sir Alfred's staff and the improvement in W/T interception began to make itself felt.

Early in September, Russell Clarke called on the D of E and told him that he and his friend, Hippisley, had been obtaining German intercepts on their receiving sets in London and Wales. Both these men had been enthusiastic W/T amateurs since the earliest Q days. It is not clear why the police or the Post Office had not sealed up their apparatus, but it can well be imagined that some rash official had tried his best on Russell Clarke and had been forced to retire the worse for wear. These two men had no difficulty in persuading the D of E that, given reasonable conditions, they could produce all that was needed by the Admiralty to study the intercepted signals of the German grand fleet.

Sir Alfred obtained permission for them to install their apparatus at Hunstanton Coast Guard Station. Geographically the position was most satisfactory for the tapping of the Flanders air and, as events soon proved, it was the ideal place for the work they were soon to initiate and develop to such perfection. But Hunstanton was chosen because there was a Coast Guard Station equipped with W/T and it was suitable for interception in Flanders and North France. Russell Clarke and Hippisley brought along another W/T amateur, Lambert, and with the assistance of C.G. P.O., a continuous watch on the German field stations was kept, thus giving a very necessary duplication to Stockton (the Admiralty police station) and the Marconi stations. Work on these cyphers continued in the Admiralty and W.O. by day, while the night watch worked in the W.O.

One is bound to admit that the signs of jealousy were not absent even in this small section of men drawn from many branches of civil life. It must be remembered that, at this time, civilians deciphered and translated the messages which all concerned the Western Front and were of immediate value to the Intelligence Section of G.H.Q. whither they were transmitted by wire and by daily bag. But it must also be remembered that by day they were also deciphered and translated in the Admiralty, and if of no immediate value, they were occasionally of extreme interest and could hardly be concealed from those in supreme control. It is said that a climax was reached when the all highest on one side of Whitehall was told a translation of great interest (actually, proposals for treatment of Indian prisoners) by his opposite number before his own section had managed to get the information through to him.

It might be stated here that the colleges had now reopened and had claimed the services of certain of their staff who had worked with the D of E during August and September. Sir Alfred's staff therefore now consisted of Naval Instructors Parish and Curtis, and Professor Renderson when their other duties permitted them and, as watchkeepers doing night duty in the W.O., Denniston (who had obtained leave from Osborne), Hershall and Norton. The first three knew something of mathematics and little of German; all six were singularly ignorant of cryptography, but they were becoming expert analyzers, filers and translators of German military telegraphese.

Most likely they were never in the office altogether for it was the Director of Education's room and was crowded for three. Likewise, Sir Alfred had a certain amount of naval education to look after and people to see in his office, and occasionally it was necessary for the cryptographers(!) suddenly to pack up their papers as innocently as possible and scuttle into the small box-like room occupied by Mountstephen, Sir Alfred's secretary. Sometime about the middle of October, Sir Alfred's desk was cleared mysteriously and frequently on the arrival of the Russian attaché. There were some days of tense peace when little was seen of the D of E and the cryptographers were almost rudely discouraged from their visits to Mountstephen's room, now occupied by an unknown naval officer, who came early and stayed late. Sir Alfred encouraged the sorters to seek out the hitherto neglected messages, all of which disappeared. Then, one fine day, the D of E remarked that it was blowing hard in the German Bight and in reply to direct questions explained what was afoot.

The Russian Naval attaché had brought a copy of the German Naval Signal Book which had been salved from the light cruiser *Magdeburg*. The quiet ever-working Naval Officer was Fleet Paymaster Rotter, the Head of the German Section of the Intelligence Division, whom the D.I.D. had lent to assist in tackling the new problem. The Russians alleged that the salved book was the one now in force in the German Navy, and that any naval intercepts we possessed must be decipherable by that book.

So far it had been discovered that the weather reports alone came directly out of the book and that all other signals were submitted to some process of reciphering which Rotter was now investigating. In a few days he solved the key which proved to be simple substitution, and within a few days of the solution the key changed! He set to work again and in a short time produced the current key which was to last for three months.

The material he had to work on was the numbered series of messages sent out by Nordderch (K.A.V.) to all ships (A.S.). The Germans, whose folly

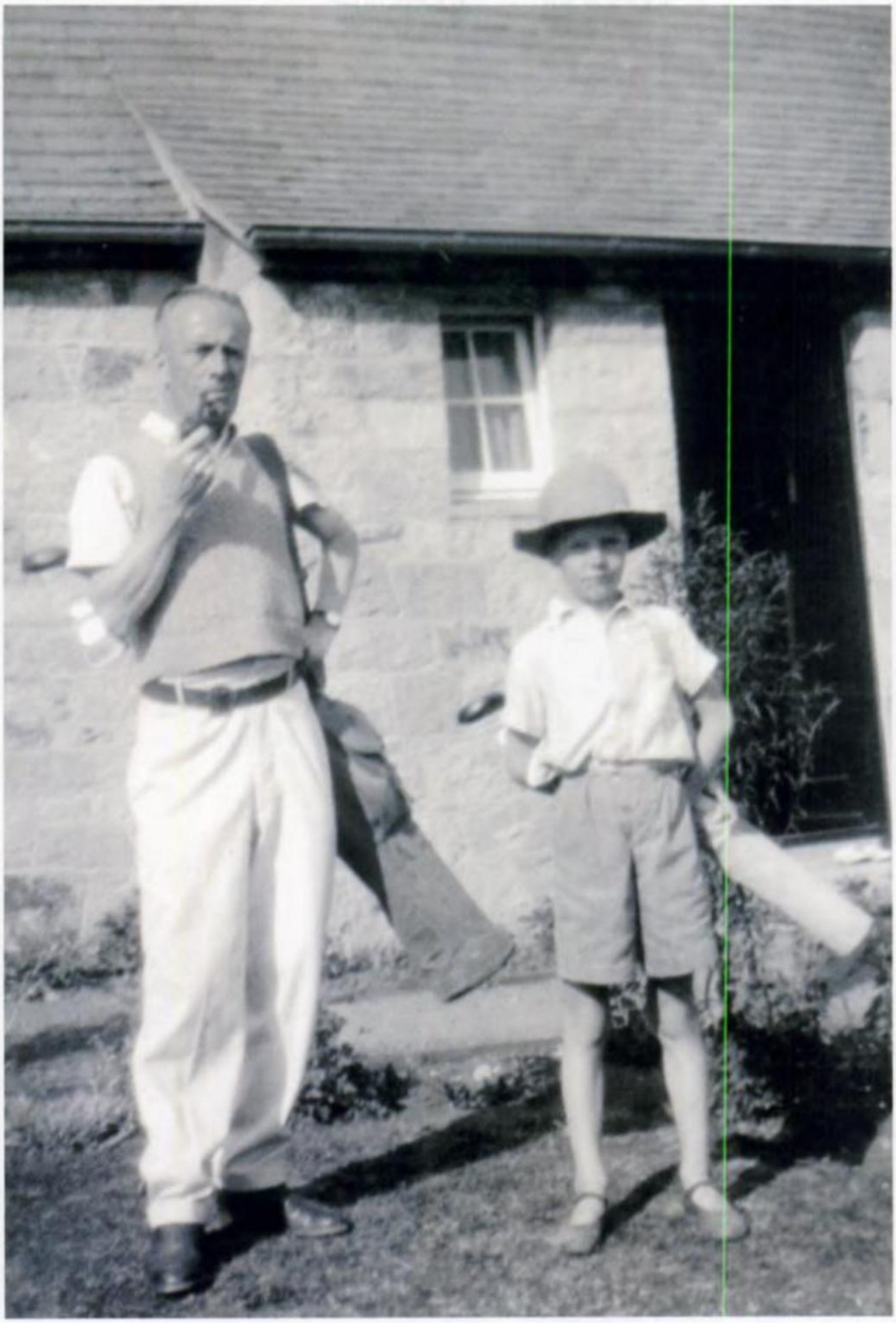
was greater than our stupidity, reciphered the numbers of the messages thus offering the simplest and surest entree into their reciphering tables. Before very long, Rotter was able to instruct the office in the use of the Signal Book and the key, and the current messages could be read.

Then Russell Clarke happened to come up from Hunstanton and look into the office. He saw these new signals and exclaimed that he could intercept hundreds of such messages daily on short waves which, if read, would give the daily doings of the German Fleet. K.A.V. to all ships were merely the intelligence reports circulated by the German naval staff concerning the movements of enemy shipping. The movements of the German Fleet would be of supreme interest.

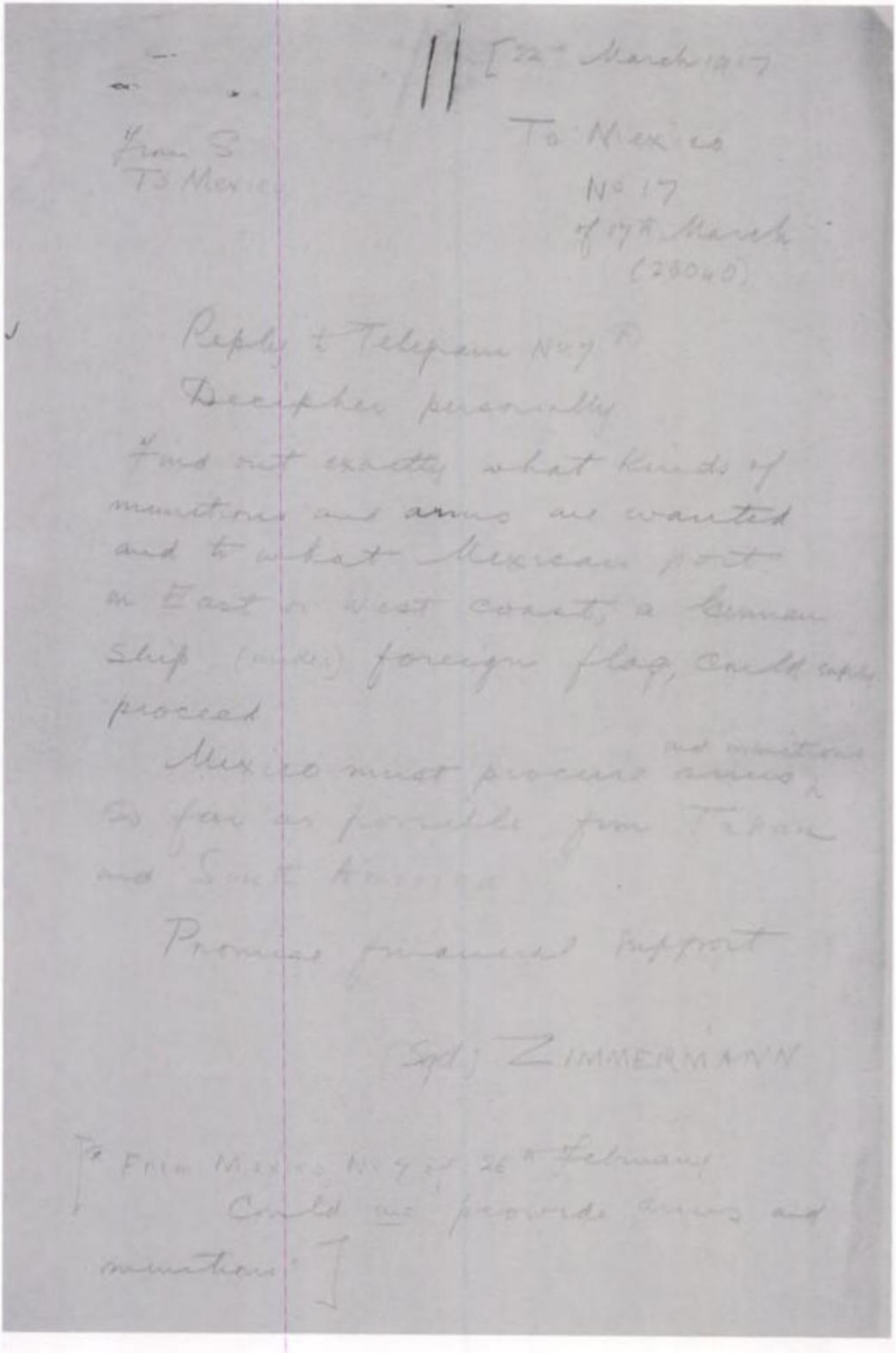
There was, however, only one aerial at Hunstanton which was doing good work on military interception, and the D of E was a little loathe to lose good stuff for a pig in a poke. However, he agreed to a week-end trial which was of course conclusive. From what we could read of the stuff intercepted at Hunstanton alone, it was clear that we should from now onwards be able to follow every movement of the enemy fleet, provided always they used the same key, call signs and book.

It might be noted here that the German Signal Book used four additional morse letters to which they gave the names alpha, beta, gamma and rho (delta, epsilon and lambda were added in later books). Ordinary morse had no signs for these and the transmission on the land lines caused the office endless confusion. Russell Clarke evolved a suitable alphabet in which he instructed the Admiralty Telegraph Room, who in turn instructed the various intercepting stations. Later on in the War the army evolved another alphabet and the French yet another, but 40 OB refused to come into line, and stuck to the plus sign and equals sign and the rest of them which Russell Clarke had invented and which had been learnt in the pain and turmoil of those early days.

It was now clear that the Admiralty cryptographic section had found a task which concerned the Navy alone, and that there might be an enormous outlet for their energy. The watchkeepers were therefore recalled from the W.O. and started to keep a continuous watch on the naval signals. As stated above, the relations between the two offices were already somewhat strained and, as the new activities in the Admiralty were a closely guarded secret, a definite breach occurred which endured till the Spring of 1917 when, as will be seen later, a liaison under completely new conditions was effected. Looking back over the work of those years, the loss of efficiency to both departments caused originally



AGD and son Robin with golf clubs, 1936


11

[22nd March 1917

From S
To Mexico

To Mexico

No 17
of 19th March
(2800 D)

Repeat to Telegram No 7

Decipher personally

Find out exactly what kinds of munitions and arms are wanted and to what Mexican port on East or West coast, a German ship (under) foreign flag, could safely proceed

Mexico must procure munitions

So far as possible from Texas and South America

Provide financial support

(Sgd) ZIMMERMANN

To From Mexico No 7 of 26th February

Could we provide funds and munitions?

A transcription of the Zimmerman telegram in 1917. Intercepted by British codebreakers, it was instrumental in persuading the USA to declare war on Germany.

SECRET.

156/S.A.

D.I.D.

The following information has been asked for by Captain Hope.

The South American countries with which we are able to deal are the following :-

Argentine.

Brazil.

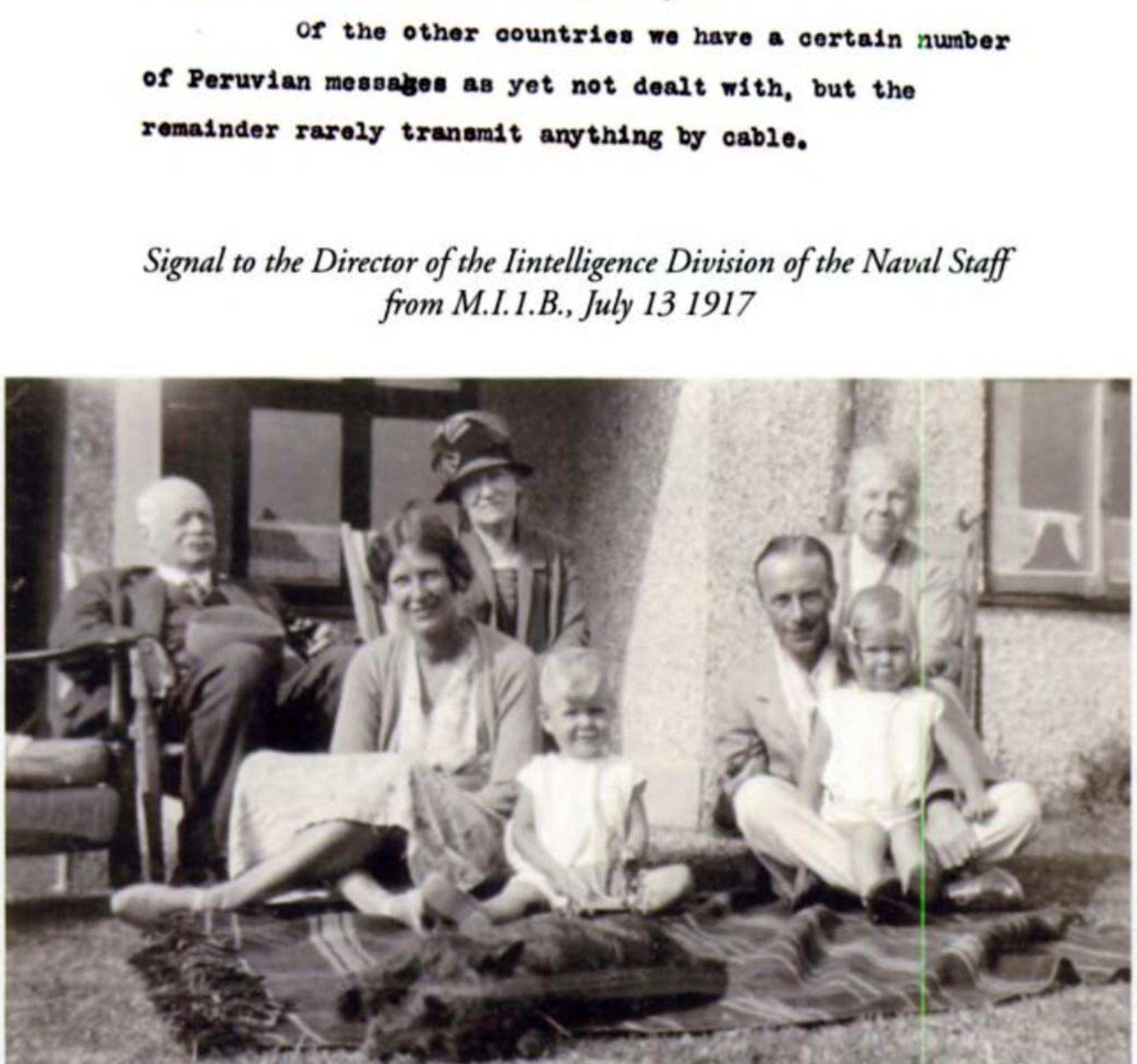
Uruguay.

and Chile,

which we are at present doing for you.

Of the other countries we have a certain number of Peruvian messages as yet not dealt with, but the remainder rarely transmit anything by cable.

Signal to the Director of the Iintelligence Division of the Naval Staff from M.I.1.B., July 13 1917



(Back row) AGD's father and mother-in-law. Between them, the author's mother and (centre) the author. On the right (back) AGD's mother, AGD and daughter 'Y' in 1931.

AGD's family outside their home at 48 Tedworth Square, London, 1936

by mere official jealously is the most regrettable fact in the development of intelligence based on cryptography.

The watch on the naval signals began with the staff mentioned above in Sir Alfred Ewing's room. Work was complicated by the crowd, the need for secrecy and the equal need for charwomen. Sir Alfred's visitors were now denied entrance to the room and it is remembered how the august Assistant Secretary to the Admiralty was refused admittance by a temporary civilian ignorant of his identity. This apparent indiscretion bore good fruit, for very early in November a new room was placed at the disposal of the Section. This was the original 40 OB where the work was carried on till once again the growing staff was overcrowded.

To preside over this room came Herbert Hope, then Commander. It has always been alleged by himself that he knew no German, no cryptography, nor why he had come. His official duty was to keep the operations Division and Intelligence Division informed of the activities of the German Fleet as elucidated by the D of E's cryptographic staff. Before very long, however, he was able, by his constant presence, to be the connecting link between the watches and to be the guide and helper of all such as were in difficulties, either with the German language or cryptography.

The First Lord, Winston Churchill, now took official note of the existence of the Section and issued its charter. As is seen, he laid down certain instructions for the distribution of the translations. One is bound to confess that the First Lord's view of the possibilities of cryptography appear now distinctly limited. To have carried out his instructions literally would, no doubt, have safeguarded the secret but must also have nullified the value of the messages.

The Operations Division under the Chief of Staff should have been most interested in these messages, but this Division was at first most sceptical. Two unfortunate incidents in the days before the staff moved to 40 OB were perhaps the cause of this scepticism. Owing to poor interception and lack of knowledge on the part of the staff, a signal was circulated alleging that the *Ariadne* was proceeding to the Jade. The Operations Division knew that the *Ariadne* was sunk in the Heligoland Bight action. Worse than that, a message was circulated on two or three successive evenings purporting to order destroyers to patrol the Inner Gabbard. The C.O.S. took counter-action and, at some considerable trouble and expense, English destroyers also patrolled that spot and never found the enemy . Subsequently it was found that the German destroyers had merely been ordered to proceed to Heligoland, which island could only be distinguished from the Inner Gabbard by the bar over the

letter 'A' which had escaped the notice of the inexperienced and geographically ignorant watchkeeper.

Further, any signal which could be read was circulated without comment and for reasons best known to W/T experts, many of those emanating from Bulk were among the best intercepted and hence most easily read. The poor watchkeepers had the haziest of notions as to the whereabouts of Bulk but the Operations Division cannot be blamed for their lack of enthusiasm for the times at which the Kiel barrier was opened. The watchkeepers knew nothing of the German Fleet, very little of the geography of the German coastline, while their ignorance of English and German naval phraseology was profound. Hope did his best for them, while Lord Fisher pointed out that warships did not 'run in' and begged the staff to adopt the word 'proceed'.

At the beginning of November 1914, the work of watching the German Fleet seriously began and the organisation known popularly as '40 OB' began its career. The personnel was as follows: Sir Alfred Ewing in charge, Commander Hope and Fleet Paymaster Rotter dealing respectively with the intelligence and cryptographic, sides of the work, Herschell, Denniston and Norton watchkeepers in 40 OB, Russell Clarke and Hippisley at the Hunstanton intercepting station. The permanent educational staff of the D of E, Naval instructors Parish and Curtis and Professor Renderson, gave all the assistance they could when their other duties permitted.

The gear consisted of one copy, the original, of the Naval Signal Book. However, Russell Clarke turned himself into a photographer and his private house into a studio and by the end of the month three additional copies were available. Lack of apparatus forced him to reduce the size considerably and as time went on it was found that the strain on the eyes of the watchkeepers using electric light was too great, so the Admiralty provided a suitable apparatus and Naval Instructor Curtis again reproduced this book (and many others) in the course of 1915.

The other 'gear' arrived from Australia during November. It was the Handelschuffs Vertehrsbuch (HVB) captured very early by the Australians, photographed and sent home for distribution. It had been found that the merchantmen acting with the German cruisers used this book for communication, *but once in 40 OB it was soon discovered that the whole High Sea Fleet and especially outposts, submarines and airships used it very extensively of course always in reciphered form. It continued in force till March 1915 and was of the greatest value, especially in the matter of air raids.*

With this gear, then, the staff started work. There was no traditional routine to be followed. New methods had to be evolved to meet new needs. It may be of interest to sketch out the daily routine as it was in November 1914. Hope and Rotter were present daily from 9am till 7pm, the former dealing with the translated messages, the latter working on the many fragments and examining the unknown. The man on watch had to sort, decode and translate the new.

Hunstanton, Stockton Leafield and Hall Street had direct lines to the Admiralty. There was a never-ending stream of postmen delivering bundles of intercepts. In a few months these men were replaced by an automatic tube which discharged the goods into a basket with a rush which shook the nerve of any unwitting visitor and very much disturbed the slumbers of a night-watchman taking his time off.

In the very early days every message which appeared to give sense to the man on duty was 'logged' and 'sent'. That is, the translation was written in the current log book and three copies were made for circulation, one for the C.O.S., one for D.I.D. and one for Hope. With luck, there were three or four copies of every message from the various stations. These had to be pinned together and stacked in the file of logged messages. But still there was a vast number of fragments, of messages which failed to satisfy the fastidious German taste of the watchkeeper, or messages in unknown codes and languages. All these were bundled into a tin on which was printed large and black 'N.S.L.'. It was a very important tin, nearly always very full in those days, but to explain it to the many newcomers was one of the most complex points in a very complicated system. Truly N.S.L. only meant 'neither sent nor logged'. When the war was finished there was still a box called N.S.L. when there had been no log for the last two years. N.S.L. was a living thing with a specific meaning, and it is recounted how a night watchman woke trembling in a sweat - he had dreamt he had been sent in the N.S.L. and got lost.

The log became an object of hatred before long. The First Lord had called into being that particular form of filing the current work and it was over two years, when its originator was elsewhere, before a more labour-saving and less soul-destroying method was allowed to replace it. In the days when a watchkeeper averaged 12 messages it could be written up, though even then it was the fashion to let the messages accumulate and allow the new watch to write up the log, and thus appreciate the situation! But it was beyond a joke when naval actions were pending or zepps fluttering and the watchkeeper had 12 to 20 pages of the book to write up.

For two months at least the night man had a lonely time, though he was

probably too busy to note it. It was no good bringing pyjamas in those days or hoping the Admiralty would provide a bath. All that was needed was plenty of sandwiches. Tastes in drinks varied and only one man is alleged to have worked throughout the night with a revolver at his elbow.

It was already obvious that an increase of staff was essential when a further access of 'gear' made it imperative. Trawlers working in the neighbourhood of the spot where four German destroyers had been sunk on .... dragged up a heavy chest with German markings. This was at once forwarded to D.I.D. and was found to contain a copy of the V.B. (Vertehrsbuch), a most secret code book used by the German Admiralty and senior officers, also a mass of secret papers dealing with navigation. The D.I.D. handed over the former to Sir Alfred Ewing and collected a staff under Herschell to translate the latter.

The V.B. was found to be of the greatest immediate value in dealing with the German cruiser fleet, while the fact that it was solely used for the correspondence with the Naval Attaches abroad, especially in Madrid, escaped notice for some months. The pressure of purely naval work on the small staff rendered research into new problems impossible in those days. To fill the vacancy caused by Herschell's transfer to D.I.D., and to bring the watches up to two-man strength, Monk Bretton, Hopkinson, Freemantle, Lawrence and Morrah joined in December.

None of these men had more qualifications than the original men. They knew ordinary literary German fluently and they could be relied on. But of cryptography, of naval German, of the habits of war vessels of any nationality, they knew not a jot. Their training was of the shortest before they were sent off in watches of 2-men each and given the responsibility of looking after the German Fleet. Worse than that, they had to learn the intricacies of the office routine . They probably had more than their fair share of log-writing, and they had to sort and circulate. They had to turn the German squared chart into latitude and longitude of which they had not heard since the geography class of their school days.

It is to be imagined that Hope had an anxious time when he arrived each morning, fearing to find that the German mineseekers had found a mine apparently off New Zealand which on closer examination proved to be off Heligoland and then a hurried correction 'in our no. XYZ for so and so please read thus and thus' would be circulated in triplicate. However, it was already a cheerful party by New Year in 1915.

Everything the Germans said was contained in one of the three books in 40

OB and in those days the Germans were by no means discreet or cryptic in their W/T. The exact disposition of the High Sea Fleet, the submarines and the airships was mentioned from time to time, and duly read and circulated.

It is not the function of these notes to go into any details of the actual signals but merely to record how and why the organization which read them grew. When 1915 began, 40 OB was fairly pleased with itself in its innocence. All German naval signals which the stations could intercept were read and circulated. No attempt was made to develop any intelligence side of the work, beyond Hope's duty of instructing the authorities on the real meaning of certain signals. The request that 40 OB should be allowed to keep a flagged chart of the German coastline was vetoed as an unnecessary duplication of the work in the Operations Division. (In May 1917 this request received sanction.) But all naval signals were read even if without intelligence. True it is that in certain cupboards there were increasing piles of 'stuff' which was not read but it was not naval German. *The art of reading other peoples' telegrams was still in extreme infancy; no one then imagined that all those piles contained telegrams possibly of the greatest interest which could be read and, in 1915 it may be said, read without extreme difficulty.*

In those days the possibility of a change in the cypher key was prophesied with bated breath and the authorities were informed that such a danger must be reckoned with. Should it happen, it was generally considered that our source of intelligence would dry up for several days at the very least. At last, one evening early in January, the watch was confronted with signals which would not yield to the ordinary treatment. The dreaded change had come! All the available staff were summoned by telephone and after a night long struggle the new key was obtained to the joy and admiration of all concerned. The First Lord called early next morning and congratulated the experts who had solved the key so promptly.

In the course of the day it was discovered that the key had <u>not</u> changed but that the existing key had been 'slid' and that the actual work involved need not have taken five minutes. This discovery 40 OB kept to itself and when, a few days later, the key really did change one morning, the new one was produced quietly and without much trouble in a few hours.

Two years later when the key changed every night at 12 o'clock, the night watchmen were greeted by the cold contempt of their relief had they failed to evolve the new key.

During the early Spring of 1915 the increase in the number of intercepting

aerials controlled either by Russell Clarke or the Marconi Company led to a very large increase in the numbers of telegrams received. It was, of course, necessary to have two or three copies of each message in order that the text might be absolutely sure. But the intercepting officers were now learning a lot about the methods of German naval W/T and it was possible to allot aerials to various wavelengths and even districts. Thus the operators soon realised that the Baltic and North Sea Fleets were on different circuits and under different controls. The submarines formed a separate group and the small outpost craft in the Bight yet another. 40 OB learnt these things too and, even at this period; Baltic messages received scanty treatment.

It was again found necessary to enlarge the staff to cope with the increased daily bag and Lytton, Young, Talbot and W.L. Clarke came in, one into each watch. There was at this moment no thought of enlarging the scope of our activities, but merely competing efficiently with the current naval messages. However, one day in April, D.I.D. produced a fresh line of goods - treasure trove in Persia it was said, obtained by sandbagging said one, by payment said other. Later it was alleged that the India Office had obtained the effects of a German Consul expelled from Persia and, knowing nothing of such things as code books, had turned the lot over to D.I.D. The so-called cryptographers examined the books. They were obviously not naval but diplomatic codes but were no good to us unless we also had the telegrams. So the cupboards where the 'stuff' was piled were made to disgorge.

CHAPTER THREE

Scapa Flow 1919

After his war at Room 40 OB, AGD was given a medal and sent north to Scapa Flow to interpret for Admiral Beatty, C in C of the British navy, at the surrender of the grand fleet to the victors. This is his report (Churchill College Archives).

It appears necessary that I should write a few lines on my travels to the north, for which I have not yet received a bar to the O.B.E. Let me issue a word of warning. I was a landsman on board a battleship, and a lot of my time was taken up in trying to conform to the life therein, no easy matter if you remember that it is really a foreign land where the inhabitants have a distinctive mode of life, even a distinctive language and very distinctive habits which to learn in a few days is not an easy matter for a visitor to this foreign land. My impressions of this particular foreign land have nothing at all to do with the matter in hand, namely the surrender of the German Fleet and the end of the motive power which has driven the British Navy for the last twenty years and made it into such a wonderful machine. First of all I should like to confess that, for the last four years I had considered myself, and the department in which I worked a very important cog in the machine; now for the first time I ran across the 'business end' of the weapon and I realised most strongly what a little cog we were. Practically no one I met had any idea of the existence of such a cog, which was satisfactory to know, as we had tried to conceal our identity. I had to keep a straight face, and lie right well to many an old friend from Osborne days whom I met up there, who wanted to know what my job was. On the whole I fancy I gave myself and my department a highly sensational appearance, such as would rejoice the readers of William le Queux.

Very well, let me miss out all the strange impressions in this foreign land, and get on to the business.

I went up to act as interpreter at the surrender of the German Fleet. I had

practically no interpreting to do! This was the reason - on arrival at Rosyth, I went at once to the Q.E. [HMS *Queen Elizabeth*] the flagship of the C. in G. to find out what my duties were. There I at once met an old friend, one Spickerwell, now secretary to the Admiral. "You are allotted to us," said he, and thus I was to do my share on board the flagship. But the C. in C. had detailed the Admiral commanding the 1st Battle Squadron to arrange for the actual examination of the surrendered ships, while he himself concentrated on the general policy to be adopted and only concerned himself with his opposite number, the C. in C. of the German High Sea Fleet, with whom he parleyed by means of wireless. My duties therefore consisted in acting as go between in all these discussions, and I need say no more of them, save that Sir David Beatty is a very wilful man, and has no mercy on a man or nation he despises.

Such a thing as a review by the King seemed of little importance on the day of my arrival, so I pass on.

The Q.E. got under weigh about 2am of the 21st. I know it well for the process entailed propping the iron decks just where my cot was swung, involving much hammering. However, I got over it, and slept peacefully on, and, waking at 7am I went on deck and was very much surprised to find that we were now outside May Island, in fact at sea. I bustled along, and when action stations was sounded at 9am, I trotted along with the Secretary and a Dictionary through miles of passages, manholes and ladder, and finally found myself on the signalling bridge where the Admiral had his sea cabin. There was plenty of noise here for the signalling to the whole fleet was carried out from this bridge and when there are a hundred odd ships at close quarters there's all to be said, by means of searchlights, flags and wireless. At 9.30am the Hun ships wore first spotted about 5 miles away, and then the thrills began. The first lot were the Admiral's particular pets for he had been close to them, but never had enough time to examine them so closely. Everyone was pointing out features in the ships they had noted - I myself had read much about them, and volunteered entirely inaccurate information which was gratefully received. As the rest of the fleet came along the C. in C. dictated his signal to the Admiralty that he had taken over the German fleet. It was a dramatic signal but he wished he could have wired he'd sunk the lot in fair fight, and he said so, and a lot of other unpleasant things about them. Then the whole British Fleet turned round which made the Q.E. the leading ship, and we proceeded towards the Forth. Once inside the Q.E. stopped, and the climax of the day arrived. Close on the south side of us the Germans passed, led by a small English cruiser, in very good order, but silent and sullen, hardly a man to be seen on deck, their flags flying for the last time, for the C. in C. now made his

second-signal that the German flag had to come down at sunset, and not to be hoisted till further orders. On the north side of us ship by ship went the British Float, including the American squadron, which was called the 6th B.S. and was acting as part of the British Fleet. Every ship was dressed, the bands were playing, and as they passed cheered Beatty who stood greeting them from the bridge. The 1st B.S. rounded up the Huns, and bringing them to the fixed anchorage proceeded to examine them. This intimate part I missed, I was sorry but I couldn't have had both. Then the Q.E. put on full speed, and once again passed the English Fleet full of beans and cheering. At last after mooring the Admiral came down, and this time his own crew rushed to cheer him. As he passed down to his own cabin acknowledging the cheers he cried "I always told you they'd have to come out".

At 6 in the evening we had the thanksgiving service on the quarterdeck under the huge 15in. guns. It was quite dark all round, but the deck was lit by two arc lamps, and there about 1000 men leaving their work for about half an hour assembled, and did really the most English thing that could be done - a thing I doubt whether any other nation would have done. And that ended "der tag", the toast of the German Navy ever since its beginning.

"You've not come face to face with the Huns," said the secretary, so he announced to A.C. 1st B.S. who remember was in charge of the show, that I had now completed my duties with the C. in C. and was available. It had been arranged by the latter that the English Battle Cruiser squadron were to accompany the German Battle Cruisers to the Orkneys, and take charge till he, A.C. lst B.S. should come up with the rest of the Huns. So he transferred me to the *Lion*, the flagship of the B.C.S., and off I went with joy to this foreign land for a Cruiser is no more like a battleship to live in than England is to France. I found some very good friends there to whom I yarned like a pressman during the frequent periods when there was nothing else to do but yarn.

The C. in C. came on board to say Good-bye an hour before we left and made a speech to the assembled Officers and Men which was never meant to get into the papers, but did in parts. Luckily we have or had then a Censor capable of dealing with not only indiscreet remarks but with those which might better have been left unsaid.

If you know English Naval history at all, you will agree that some rich man should endow a society for the prevention of public and political speeches by Admirals of the British Navy.

One of the most thrilling moments to me was when the 5 German Battle Cruisers weakly and orderly fell into line astern of the lion and proceeded on to voyage to the north. Owing to the poorness of the German coal, and the bad condition of their engines we had to take 16 hours over a trip which normally takes the English Fleet 12.

One Hun, the *Dorfflinger*, a fine modern ship fell 4 miles astern during the night, but at 8am on the Monday morning escort, and surrendered ships passed through the double 'gate' which guards the entrance to Scapa Flow. The 'gate' is the mine free passage, which is opened and closed by trawlers, through the mines and nets which keep the submarines out. But a month before a daring U Boat had attempted to get through in the wake of a store ship - but that is another tragedy.

Once inside the enemy had to be taken, or rather had to go to the last home, so with the navigatoring officer, a midshipman and two POs I went on board the German flagship, the *Seydlitz*, and did her last journey with her. No comfortable companion on board this ship - we had to swarm up a rope ladder with our charts and gear. The Officers who met us were dignified Huns, and spoke their own lingo. However, I insisted we had to see the Commander, so at last he came on deck, and addressed us most correctly in English. Whereupon his other Officers continued in English perfectly well. They insisted on navigating the ships themselves under our instructions, and they did it to the admiration of our navigator, who, he told me, learnt how several things should be done.

I confess I did feel sorry for the senior Officers there. They were keen efficient men, who had learnt their work, and made the German Navy their career, and this was the end of it. We knew that many of them there had fought a gallant action at Jutland, in fact, the Commodore, a fine looking old Norseman with now a very sad expression had been captain of the *Seydlitz* at Jutland where she had been very badly hit. Only fine seamanship on his part had got her home, and now he had saved his ship for this end. Of a different stamp were two young obviously Prussian lieutenants; as we came into view of the English fleet they heartily damned Erzberger for his folly in signing the armistice. The representative of the Sailor's Council came up on the bridge as we were steaming along, but he didn't know why, and looked very self conscious. The captain had a friendly word with him, and he soon mouched off again. The crew, not at work, slouched about, a proper set of rascals they looked. They seemed interested in the scenery of the Orkneys, by now they'd had enough of it to last them for ever! The ship was filthy. No paint, no brass work, no scrubbed decks, a scene of desolation, and a smell of rotten cabbage.

Cabbage was apparently their staple diet, there were tubs full of the smelly stuff everywhere. Yet we know well how the ship could, and did fight. T*he Huns told us their ships were built to fight not to live in, and that is really the story of the German Fleet.* It was built for a battle in the North Sea against the British Fleet, and for nothing else. The rest of my stay at Scapa needs no description. It was dull beyond words. One of the most wonderful things our Navy has done in these four years is to preserve an almost unimpaired morale and discipline amid the dullest and most comfortless conditions.

Just remember that probably 60 per cent of the ships end men never saw a hun nor fired a shot at them, but night and day for four years they had to be ready. No leave, constant alarms, and fruitless trips, patrols, and as their base Scapa Flow, a few islands whore they could land, and play football in the mud and heather on the side of a hill for the men, primitive golf, and a little wild shooting for Officers, and that was all. But they won the war, and I am glad it was for them a bloodless victory, at the end for I was with the C. in C. when he said that the whole German Navy was not worth the life of a single English blue jacket.

This is my father's second report. Two more follow after chapter four. I believe they speak for themselves. Passages of particular interest have been printed here and elsewhere in italics.

CHAPTER FOUR

His Secret Years: Strengths and Weaknesses

What follows is based on a paper I wrote for a scholarly monograph on US/UK approaches to signals intelligence co-operation, published in 1986.

I

The professional career of Alastair Denniston is of more than personal interest as it illustrates three important trends in the development of Anglo-American signals intelligence in the formative years of the Second World War.

The first is that the concept of a total intelligence service provided by GC&CS's interception and cryptanalysis was developed earlier than some historians hitherto thought.

The second is the continuity provided by the length and consistency of AGD's working life from watch-keeping in Room 40 OB in 1914 through to the establishment, growth, and development of the Government Code and Cipher School from 1919 into GCHQ's crucial work throughout World War II.

The third is the priority placed by its management on total trust and maximum information flow between the UK and USA, and this in a context in which secrets of the importance of Ultra would normally be withheld from friends as well as enemies, since allies may change their allegiance, governments may misuse their secret information, and individuals may use their privileged access to further their own career or even merely to impress their friends.

Despite the subsequent post-war MI6 débâcles and understandable fury of the US authorities, the US-UK understanding on secret intelligence mirrored in the Friedman-Denniston correspondence remained, and remains, in force and still plays a part in the crises of the post 1945 world.

Alastair Guthrie Denniston was born near Greenock on the Clyde on 1

December 1881 and died in hospital in Lymington, Hants, on 1 January 1961. His father, a doctor, had died at sea when he was very young, and he had helped his mother to bring up her other younger children on very little money. At school he excelled at classics, languages, and mathematics. He was also a considerable athlete, played hockey for Scotland in the 1908 Olympics and was playing tennis and golf, with a single figure handicap, almost till his death. His professional career in secret intelligence began in November 1914 when he was 33, and it continued uninterrupted until 1 May 1945 - a period of over thirty years during which the significance of British signals intelligence attracted the close attention of most modern historians.

He was not only at the centre of these changes but was himself intimately involved in implementing them. He was recruited as an expert in the German language, having earlier studied both language and literature at Bonn University and taught it at Merchiston Castle, the Edinburgh public school, and at the pre-Dartmouth naval preparatory school, Osborne on the Isle of Wight. It was from here that Sir Alfred Ewing summoned him to the Admiralty at the outbreak of the First World War.

His skills as a German linguist caused his entry into the world of wireless interception and cryptanalysis, but it very soon became apparent that other skills were needed, and he and his colleagues were quick to learn them too. He was one of the original group of German linguists who, on the job with the radio hams and other brilliant and unorthodox personalities learnt the difficult techniques of cryptanalysis, together with attendant lady helpers - one of whom he married and re-employed in Hut 3 at Bletchley Park in 1939 - worked in Room 40 Old Buildings in Whitehall. It was a close-knit group and worked in watches - a practice which continued through both world wars - so that inevitably its members came to know each other very well, and to develop strong camaraderie which, by 1922, involved a closing of ranks and a paranoid suspicion of those politicians who misused the intercepted decrypts.

Signals intelligence, born in the early years of the twentieth century due to the exploitation of Marconi's great invention of wireless, started in the UK with the interception of radio messages - in morse or via other methods - through a series of intercept stations scattered round the eastern coastline of Britain. These were brought by landline or by motorcycle messenger to Room 40. There was also the increasingly expert analysis of wireless traffic (T.A.) intercepted to indicate where increasing volume might indicate imminent enemy activities; the decrypting and translation of the material; and finally a much more subjective, intuitive assessment of what these messages might

mean to the person or department to whom they would then be passed. This in turn required an assessment of the potential recipients, which in due course involved a form of interactional educational process. It also involved a close knowledge of the day-by-day progress of the war, and an understanding of the diplomatic and political sensitivities into which this processed material - its origins completely concealed - might percolate. Churchill was the chief user of signals intelligence thus obtained from 1915 (as 1st Lord of the Admiralty) to 1945, VE and VJ day.

The Zimmermann telegram, received and decoded overnight on 16 January 1917 by a close colleague of Denniston, Nigel de Grey, and William Montgomerie, an Irish Presbyterian German linguist, proved a watershed. It did indeed ensure the entry of the United States into the war on the allied side. But it could not be fully used until a second copy of it had been identified so that the sources of the discovery of the first copy could be protected. Much has been written about the Zimmermann telegram, not only as a classic example of the successful implementation of the total service which a cryptanalytic unit should provide, but also for its historical importance. Recent correspondence has come to light in the files of the National Security Agency at Fort Meade between Denniston and William Friedman, the head of American cryptology, in which as late as 1958 Friedman finally established authentic details of the transaction from Denniston's memories of the crucial days in which the telegram was decoded and processed. There was never any doubt that the Room 40 group was fully aware of the importance of what they had done and the success which attended Sir Reginald Hall's handling of it.

Hall himself recalled the moment, at 10.30am when de Grey came in and asked him 'd'you want to bring America into the war?' 'Yes, my boy,' I answered, 'Why?' The deciphered telegram revealed the German decision to wage unrestricted submarine warfare. It was all that was needed to bring America in, and US-UK signal intelligence co-operation in war began. The Friedman-Denniston correspondence further reveals some cryptanalytical successes which would never have seen the light of day but for the mutual regard and trust established in 1941 between the two secret servants.

The camaraderie of the members of Room 40, all of whose names are inscribed on a silver salver which was given to Denniston and his bride on the occasion of their wedding in 1917, was borne out at the end of the war by a now famous pantomime, sung by all present, which was written by Frank Birch, himself one of the original cryptographers who left the secret service for the stage and King's College after the war. It is a witty and rather moving account of their work; and the statement that clearly emerged from it was that whatever else

the other members would do after the war, and whatever happened to the unit which might be broken up, Denniston would go on for ever; he would never give up. And he never did.

After the acceptance of his paper on the importance of continuing his work, he was appointed head of what came to be called the Government Code and Cipher School in 1919, soon after the conclusion of hostilities. The unit, which had been divided into two sections - the naval and the non-naval - was brought together in 1919 under the aegis of the Foreign Office to monitor incoming diplomatic codes and ciphers by means of GPO interception. AGD and his wife went to Versailles for the 1919 conference, quite clearly to spy on friends and former enemies alike - as did experts from France and America. Shortly before he had been sent as official interpreter to Lord Beatty to receive the surrender of the German Fleet at Scapa Flow, where he expressed himself appalled at the indiscretions of the Admiral of the Fleet on that occasion. He was, as we have seen, both shocked at the conditions under which German naval officers and ratings had to live and impressed at their dignified and sailorly behaviour at a time of humiliation and stress. They scuttled their fleet.

AGD's inter-war career is closely tied up with the varying fortunes of the newly formed GC&CS. The unit itself was underfunded and misunderstood by the Treasury and the Foreign Office, to which it reported, but not to the Admiralty, as the following letter from the First Sea Lord (Winston Churchill) makes clear:

Private and confidential

March 28, 1919,

Dear Lord Drogheda,

I had a few minutes conversation with Lord Curzon yesterday on the subject of the new Cypher Department which it is proposed to establish, and concerning which a memorandum is now in his hands, containing the views of the Admiralty and the War Office.

Lord Curzon told me that he hoped to summon a conference at the Foreign Office one day next week to consider the matter, when I should have an opportunity of stating my opinions, and he asked me to send you in advance a memorandum of the points I wished to raise. I therefore send you herewith the following notes of matters which the Admiralty consider essential in any scheme that may be adopted.

(1) We have in the Section of the Naval Intelligence Department which has dealt with enemy wireless during the war, a great deal of material, some of which is worked out and filed for reference or historical purposes and some of which still requires further study. We have also a small remaining nucleus of the expert staff which has done this work during the war. If the Admiralty is to join the new Department, we regard it as essential that this material and staff should be kept together.

(2) Wherever the new Department may be located in peace time, we should have to stipulate that on the outbreak of war the naval portion of its staff should immediately be mobilised and take up their work in the Admiralty. Our experience has proved that in war the deciphering staff must be in the closest possible proximity to the War Staff. We have had to work day and night all the year round, and as immediate action has often had to be taken in consequence of the information which we have supplied, no avoidable delay in transmitting the information to the Operations Division can be allowed.

(3) *We should only consent to pool our staff with that of the War Office on condition that Commander A. G. Denniston is placed in charge of the new Department.* I do not say this on account of any jealousy of the War Office, or any reluctance to accept a War Office man, but because no one who has not been trained in the conditions under which we have had to work could meet the requirements of the Admiralty in time of war. Our work has been done in face of the enemy and always against time. The messages we have had to decipher were from ships at sea, engaged in actual operations, or from airships also operating. We have had to master a new key every morning before we could begin to read the messages, and sometimes we have had to grapple with two or three keys in one day!

(4) This has of necessity developed a particular kind of aptitude for the work, which depends for its success more on a study of the psychology of the persons sending out the messages and a sort of instinctive 'flair' for the kind of things they are saying, than upon careful study and analysis for which there is no time.

In the War Office they have dealt with cables which are far more accurate than wireless, and have never had to work against time, and the aptitude they have developed is different from - I do not for a moment suggest it is inferior to that which the conditions of our work have produced.

Denniston is not only the best man we have had, but he is the only one we have left with special genius for this work. We shall not be able to retain him in a subordinate capacity, and no advantages of concentration and co-operation with the War Office would compensate us for the loss of his services. If the War Office people are not willing to accept this condition, we should prefer to retain our staff in the Admiralty, but should of course co-operate with them in every other way that is possible.

RECORD OF A MEETING HELD AT THE ADMIRALTY ON 8 May 1919

TO CONSIDER THE FORMATION OF A CODE & CYPHER SCHOOL

Present.

Commodore H. P. Sinclair C.B., R.N. – Director of Naval Intelligence
Earl of Drogheda - Foreign Of f ice.
Captain R. L. Nicholson D.S.O., R.N. - Director of Signal Division
Captain W. M. James C.B., R.N. - Deputy Director of Naval Intelligence
Lt. Colonel W. E. Wynn O.B.E. - Air Intelligence.
Commander B. Buxton D.S.O. - Admiralty.
Mr. A. P. Waterfield - Treasury. .
Major M. V. Hay, Reserve of Officers.
Major H. E. Franklin, D.S.O., M.C.

The meeting considered the proposals contained in the report of the first meeting of the committee held on 2nd May.

Major Hay stated that in regard to the proposed organisation he did not consider that an Assistant Head was necessary for the Code & Cypher School, first because he did not think there would be enough work for him to do and secondly because of the difficulties in regard to the personnel that such an appointment would give rise to. Commodore Sinclair pointed out that it was not desired to discuss the question of personnel at the present juncture. Captain Nicholson stated that in his opinion an Assistant Head of the organisation was necessary because he did not think any one man could efficiently supervise the work of both the constructive and destructive sides, and also that an Assistant Head would be necessary to supervise the instructional work that it was proposed, to carry out in connection with the organisation and also to keep the research side in close touch with the constructive side.

After some discussion it was proposed that an Assistant Head should not be appointed but that the Head of the Construction side should act as the Assistant or Deputy Head of the Code & Cypher School and that a suitable officer should be selected accordingly with a slightly increased salary to that of the first class officials.

It was decided that the nomenclature of the officials to be employed should be altered from 1st, 2nd, 3rd and 4th class to that of:-

Senior Assistants,
Junior Assistants,
Translators,
Clerks.

Mr. Waterfield raised the question of the salary of £1,200 for the Head of the organisation. It was pointed out that this officer would in fact correspond to the head of a division at the Admiralty and as such would be entitled to a salary of £1,200.

It was recommended that the salaries of the Senior Assistants (late 1st class officials) should be £600 to £800 + War bonus, that of the Junior Assistants to be £200 to £500. Those with four years' service and over to commence at the maximum.

The salaries of the translators to be £200 to £300 and that of the clerks to be in accordance with the ordinary gradings.

All these to be considered as civilians for civilian pensions.

Mr. Waterfield requested that an official letter embodying these proposals should be written to the Treasury.

Some slight amendments in detail were made to the organization previously proposed, and the amended organisation is now shown on the attached sheet.

Minutes of a Conference held at the Foreign Office on the 28th April, 1919, to consider the question of the proposed new Code & Cypher School

Present.

The Right Hon. Earl Curzon of Kedleston, K.G. … Chairman
The First Lord of the Admiralty.
The Secretary of State for War.
The D. N. I., Admiralty.
The D. D. M. I., War Office.
Captain W. M. James, D.D. N. I.
Captain R. L. Nicholson, Director of Signals Division.
Major H. E. Franklin D.S.O., M.C.
Secretary: The Earl of Drogheda, Foreign Office.

The Chairman summarized briefly the recommendations of the Inter-departmental conference which recently met to consider the matter, and said that the main question now before the meeting was the housing of the new department, with the establishment of which everyone in principle agreed. In his opinion the arguments in favour of housing the new department in the Admiralty in time of war were unanswerable, but we were providing for its establishment under peace conditions, and in time of peace he thought that the fact that the interest of the intercepted telegrams was practically entirely political indicated that the new department should be housed in the Foreign Office.

Mr. Long said he adhered to the view that the Department should be housed in the Admiralty.

Mr. Churchill explained that he was quite impartial, as he did not in any case want the new Department in the War Office. What was principally required was adequate "cover" for it, and in his opinion this could only be properly provided in the Admiralty. It would be very difficult to hide the Department in the Foreign Office.

After the matter had been thoroughly discussed it was finally agreed that the department should be housed in the Admiralty, and that a small committee consisting of an Admiralty, War Office, Foreign Office and Treasury representative should meet to work out the details of the financial arrangements, it being understood that whoever was director of Naval Intelligence should always be the head of both sections (constructive and destructive) of the department.

Mr. Churchill raised the question of the distribution of the intercepted telegrams, and it was decided that they should be sent to the Secretary of State for Foreign Affairs who would be responsible for passing them on to the Prime Minister or other Cabinet Ministers concerned when they were of sufficient importance.

It was pointed out that, as soon as the censorship ceased, no foreign messages would be received from the cable XXX*, unless Section 7 of the amending Bill to the Official Secrets Act of 1v11 were passed. This Bill, which is in the care of the Home Secretary, has not yet come before the House of Commons, and it was decided that the Foreign Office should write to the War Cabinet Secretariat, and point out the importance of XXX* to the Bill being brought before Parliament at the earliest possible date.

Copy to the First Lord of the Admiralty.
Secretary of State for War.
D.N.I.
D.M.I.

---

* Censored

SECRET. 24 October 1919

Sir,

I am commanded by My Lords Commissioners of the Admiralty to acquaint you for the information of -

1. The Army Council.
2. The Air Council.
3. The Secretary of State for Foreign Affairs.
4. The Secretary of State for India.
5. The Secretary of State for the Colonies.
6. The Minister of Munitions.
7. The Minister of Food.
8. The Minister of Transport.
9. The Postmaster-General

that the War Cabinet has now given approval for the formation of a Government Code & Cypher School under the control of the Director of Naval Intelligence, and that it is proposed that it should commence its duties on the 1st November, 1919.

2. *It has been decided to appoint Commander A.G. Denniston, O.B.E., R.N.V.R. as Head of the Government Code & Cypher School, which will be accommodated in Watergate House, Adelphi, W.C.I.*

3. The duties of the Code & Cypher School will be as follows:-

(a). To compile and be responsible for printing all codes and cyphers used by the British Government Departments, with the sole exception of those mentioned in paragraph 5 below.

(b). To examine all the British Government Codes and cyphers now in force and the purpose for which they are used, mainly with a view to ascertaining and, where necessary, increasing their degree of security; but also so as to ensure that messages shall be free from ambiguity and undue delay ensuing from mutilation in transit, and that they shall be coded in the most economical manner possible.

(c). To maintain the closest liaison with all British Government Departments using codes and cyphers, and to advise them generally in matters relating thereto.

(d). To instruct as large a proportion of Officers as possible who may be employed at any time in coding or cyphering.

(e). To assist in the preparation of any hand-hooks or instructions relating to coding or cyphering, or of those concerning the handling of code and cypher messages in general.

4. I am therefore to suggest that each Department concerned should appoint a "Liaison Officer", whose duties will be, approximately, as follows:-
(i). To keep in touch with the requirements of his Department as regards codes and cyphers and all matters in connection therewith, and to ensure that these requirements are met by the Government Code & Cypher School.
(ii). To be responsible for the suitability of the "Dictionary" (or "Vocabulary") of the codes and cyphers compiled for his Department.
(iii). To advise the Head of his Department on:-
(a). The institution of additional books to meet new developments.
(b). "Departmental Codes" before and during their construction.
(iv). To maintain a watch over his Departmental messages for faults in coding or cyphering, or any other defects, which might prejudice the security of the code or cypher used in this connection he will work in close co-operation with the Head of the Coding and Cyphering Section of his Department.
(v). To assist in the instruction of the Officers of his own Service who may be employed at any time in coding and cyphering.

5. The preparation, etc., of the "Signal Books" and purely "Departmental Codes" of the three fighting Services will remain in the hands of the Services concerned. The Government Code & Cypher School, however, will advise on the general principles of their construction and the limitation of their "life". The decision as to what books are to be classed as "Departmental Codes" will be made by the Government Code and Cypher School after consultation with the Departments concerned,

6. In the case of Departments which require large numbers of codes and cyphers, it will be necessary to accommodate their "Liaison Officers" in the Government Code & Cypher School but where the requirements are small, this should not be necessary.

7. If no objection is seen to these proposals, I am to request that arrangements may be made to bring the foregoing scheme into force, so far as your Department is concerned, and that a Liaison Officer for the

(1) War Office
(2) Air Ministry
(S) Foreign Office
(4) India Office
(5) Colonial Office
(6) Ministry of Munitions
(7) Ministry of Food
(8) Ministry of Transport
(9) General Post Office

may be appointed.

I am, Sir,
Your obedient Servant
(Sgd) R. R. SCOTT.

Letters to:-
The Secretary, War Office.
The Secretary, Air Ministry,
The Under Secretary of State for Foreign Affairs, Foreign Office.
The Under Secretary of State for India, India Office.
The Secretary, Ministry of Munitions
The Secretary, Ministry of Food.
The Secretary, Ministry of Transport.
The Secretary, General Post Office.
The Under Secretary of State for the Colonies, Colonial Office.

F.O. File. Chief Clerk
Z/6700/G 12.7.1922

To the First Lord from the head of GC&CS.

I am having considerable difficulty with the Treasury in connection with the salaries of the officers of the Code and Cypher School.

At the verbal discussions with representatives of the Treasury, which took place prior to the formation of the Code and Cypher School under D. N. I., certain figures were mentioned as salaries which, I understood were to be exclusive of War Bonus.

The treasury are now endeavouring to force upon these officers salaries which are considerably below the figure they were led to expect inclusive of War Bonus.

These officers are experts. They are men who cannot be picked up in the street and if, as I believe, their services are of real value to the State, I consider they should be paid accordingly.

They have behaved in a perfectly loyal manner, but have protested at the Treasury decisions in regard to their salaries, and I consider that their protests are perfectly justified. Should you think fit, it would perhaps help matters if you would write personally to the Chancellor of the Exchequer and ask him to direct his subordinates to moderate their enthusiasm with regard to economy in the matter of cutting down salaries of the officers of the Code and Cypher School.

Even if they were to grant the maximum salaries possible that have been asked for the total amount would still be modest.

War Office Scheme
Code and Cipher School.

Head
(Retired Officer under some Minister)

Secret Branch

Head
(1st Class)

Central Information

Sections

France Germany Scandinavia Spain Japan N. America Balkans Turkey Italy S. America
(in each section one 2nd class and one 3rd class)

Code Construction.

	Army	Navy	Other offices
	Clerical		Research
	3 3rd cl.		1st cl.
			1st cl.
			2nd cl.
			3rd cl.
			3rd cl.

4 first	class.	£600 - £900	..... £2400 - £3600
9 second	"	£500 - £650	..... £4500 - £5850
14 third	"	£150 - £250	..... £2100 - £3500
			£9000 -£12950

II

Whether the Cabinet was fully aware of it and its potential is far from clear, but certainly Cabinet ministers were prepared to prejudice its security, which they did as a way of exposing the dangers of Comintern infiltration. And it was not just the politicians but the head of the secret service himself, Admiral Sinclair, who felt that GC&CS would be well sacrificed if the horrors of the red menace might thereby be exposed. It was this loose security which led to AGD's obsessive secretiveness and defensiveness, which in turn led to considerable misunderstanding on the part of the authorities as to the nature and activities of GC&CS, both then and later. His management skills were not up to his cryptanalytical abilities.

How could the cryptanalytic achievements of World War I be brought to bear on the barren political and diplomatic scene of the 1920s and early 1930s? This was the question to which my father and his colleagues addressed themselves. Here we have only guesses. But the guesses are by no means wholly without interest, in their own right as well as in the context of the 1938-39 move to Bletchley Park, the importation of Enigma, the invention of the Bombe, and the operation of Ultra.

By 1939, the GC&CS was able to read - even if it did not always do so for lack of staff, money and incentive - the secret traffic of all countries, friend, foe and neutral alike, with the sole exceptions of Germany and the Soviet Union. For instance the British cryptanalysts intercepted and cracked the Comintern's worldwide network of secret communications in the 1930s; they penetrated Japanese diplomatic and naval traffic; they read all Middle East communications from the War Office's busy intercepting station at Sarafand in Palestine; and from a station in north-west India they helped to preserve the frontiers of the Empire.

Though the main interception station was at Sarafand in the Middle East, the London-based embassies of such foreign nations as attracted suspicion were carefully monitored. The Palmer Street station in London may well have been used early on, strategically placed as it was to monitor the diplomatic traffic of all the main nations. The arrival of Ernst Fetterlein was clearly of crucial importance. He was Russia's chief cryptologist during the latter years of the Czarist regime. He escaped to the West, a small, bespectacled, discreet Government servant, with his wife (who could speak little English) in the early 1920s. They became family friends and Denniston's diary records his death in 1944. The successes of GC&CS against the Russians in the pre-war period was largely due to Fetterlein.

A strange mixture of high governmental secrecy with close ties of family and friendship dominates the professional life of government cryptographers. Two examples may suffice. Denniston was a devoted parent and amazed the Poles at the Enigma conference outside Warsaw in July 1939 by suggesting that Mayer, the Polish chief, and he should exchange daughters during long school holidays for language study: 'I [Mayer] would send my daughter to England to his family, and his daughter would come to Poland to stay with my family. Of course the outbreak of The War thwarted ... any ... such ... arrangement.' The same suggestion - the swap of daughters for educational purposes - was made many years later to William Friedman, but this also could not be followed up.

It seems surprising that AGD should be concerned to improve his daughter's education at a time when he was the first government employee to have his hand on an Enigma machine, and an opportunity to assist in altering the course of war history. Those working in secret intelligence carry their private lives into their work as a necessary element in their total concentration; in these cases it was an excellent way of establishing rapport. It sounds dangerous, eccentric, or self-indulgent, at least highly *ad hominem*. It is certainly mirrored in Denniston's pocket-diaries of the years between 1939 and 1945. In them names and events of undoubted importance appear *pari passu* not only with his modest social life and the minor ailments and achievements of his children, but with his personal finances, always meticulously noted. He also notes his monthly salary which increased varied from £80 in 1939 to £161 in 1942, declining after his relegation to £100 from 1943.

Much of the inter-war period is the subject of a 21-page memorandum which AGD wrote for the authorities at the end of 1944, shortly before his retirement. Surprising in one so loyal and discreet, he kept a copy, which is now in the archives at Churchill College, Cambridge. Christopher Andrew, professor of modern history at Cambridge, published it in full in the first number of the Journal Intelligence & National Security, since when it has been widely cited. (see Chap. 6)

In charge of the Secret Service during the whole inter-war period was Admiral Sinclair. GC&CS was, though small, on a par with SIS and there was a considerable interchange, at formal and informal levels, of information, knowledge and friendship between the various arms of the secret services. For people working in secret, relations with colleagues and with family are a very important part of life because such work cannot be shared. Remembering the dangers of penetration by enemy interception, it is remarkable that total security was maintained concerning the work of the GC&CS despite the fact

that its chiefs were all on terms of friendship of quite a strong kind with several colleagues now known to have been working for the Soviets. To AGD, Donald Maclean and Kim Philby were well-known before their defection. The Foreign Office was still a cosy enclave and the office politics continued to play their part.

The secret Cabinet directive for the new body was 'To study the methods of cypher communications used by foreign powers'. This was achieved by a clause in the new Official Secrets Act instructing all cable companies operating in the UK to hand over for scrutiny copies of all cable traffic passing over their systems within ten days of despatch or receipt. This secured sufficient volume of throughput without which cryptanalysis is impossible. A great deal of traffic is needed to provide sufficient material for the appropriate distribution of the resulting decodes and (as important) to establish the other side's priorities. A flurry of activity between two nations not normally on speaking terms may herald the approach of an important new diplomatic initiative as well as provide the raw material out of which their cyphers can be broken.

GC&CS was a poor relation of SIS, which took most of the available funds for straightforward spying and counter-espionage. GC&CS had 25 officers and a similar number of clerical staff. Pay was exiguous, but as early as 1925 recruitment from the universities began. Classicists, linguists, papyrologists were most suitable, but after AGD's Polish visit in July 1939, the importance of mathematicians became more important. AGD himself recruited Alan Turing and Gordon Welchman. By 1939 he had realized the vital importance of GC&CS's product to the armed forces. The most important aspect of this was the Army in the form of Brigadier Tiltman, who worked at GC&CS for a while in the 1920s and continuously from the early 1930s to the end of the war. He died in 1983 after a long career in secret intelligence, a man of great achievement and probity, a firm friend of AGD. The Air Force involvement was signalled by the appointment of another man of great brilliance and achievement, Josh Cooper, who continued in cryptanalytical work through the Spycatcher era and became head of research at GCHQ. Commander (later Sir Edward) Travis was AGD's deputy. He gradually took over the administration of the service traffic in 1941; in 1942 the job was divided in two and he took all the service work (Denniston took the Diplomatic and Commercial traffic) and remained head of Bletchley Park till 1944.

Later historians separate off the solvers of cryptanalysis from the administrators of the work, the specific problem-solvers from those with an overall view. During the inter-war years there was no such division; indeed, very little administration was necessary. Several individuals, including AGD, received

modest monetary rewards for specific cryptographic achievements. Key men included Fetterlein, Knox, Strachey, and Cooper. Hobart Hampden worked alone on the vital Japanese traffic: 'With his knowledge of the habits of the Japanese he soon acquired an uncanny skill in never missing the important.' That phrase alone establishes the width as well as the depth of skills needed to provide a total cryptological service - to identify and concentrate on the important and the relevant. An understanding of the psychology and thought-processes of the sender and the recipient in Whitehall was as vital as the discernment of patterns in letter frequency.

Parallel with these developments the Americans were meeting similar problems rather differently. What might have been achieved had the two efforts been co-ordinated earlier, as they were to be from 1941 onwards, it is fruitless to speculate upon. The American effort was funded more generously and had greater access to experts, from engineers to linguists and mathematicians, of whom William Friedman was already a recognized high-profile world-class cryptoanalyst who combined remarkable intellectual concentration over long periods with a cosmopolitan's view of world priorities. The British effort was much more modest by contrast; the British employed a few ex-Consuls who were Japanologists to provide valuable decodes of Japanese naval intercepts. Denniston's memorandum notes:

> Yardley's Black Chamber tells of the American success at the Washington Conference in 1919 - a revelation which of course deeply embarrassed the US government. No one will ever tell how much more accurate and reliable information (on Japanese as well as European influence) was made available to our Foreign Office and service departments during those critical years.

The other main diplomatic achievements of GC&CS in the early inter-war period include much work on the German machine systems and Russian ciphers. Italian territorial ambitions in Abyssinia and the Eastern Mediterranean brought Italian experts to GC&CS; and a valuable basis for future German work was established when that country had re-emerged from the humiliations of Trianon to become the Number One enemy. Austria was too weak after Versailles to produce enough traffic to be worked on, Hungary was successfully attacked by Dilwyn Knox, but without much of use emerging. Summing up, Denniston writes:

> We started in 1919 at the period of bows-and-arrows methods - i.e. alphabetical books: we followed the various developments of security measures adopted in every country: we reached 1939 with a full knowledge

of all the methods evolved, and with the ability to read all the diplomatic communications of all powers except those who had been forced, like Germany and Russia, to adopt OTP.

What was translated and submitted for circulation was up to the discretion of AGD and his team. In addition to the daily issue there was a regular summary of telegrams decoded but not circulated for the benefit of the SIS and some ministries, but this was not greatly drawn upon. GC&CS successfully fulfilled its allotted function, with exiguous numbers and with an absence of publicity which greatly enhanced the value of its work.

Included in his memorandum is an interesting section on 'clandestine activities', in fact a nest of spies at work in a London suburb, in direct touch with a Comintern network operating from near Moscow. Italian codes were broken with considerable success thanks 'to their habit of enciphering long political leaders from the daily press'. Via the Italians, GC&CS was introduced to the commercial Enigma and this led to the exploration of machine encipherment. This was tackled by Knox, aided by younger men such as Bodsworth and Peter Twinn. Yet another experience was acquired in traffic analysis, a process which enabled the operator to continue plotting the movement of troops or ships even when the ciphers themselves were not legible, to establish a quantitative volume indicative of activity or otherwise. This indicates the wide scope of GC&CS' activities. Ultimately, most secret-service activities were monitored and controlled from Bletchley Park as only the seniors there had access to the total picture of clandestine activity against which each individual detail becomes significant or otherwise. In the inter-war period Malta was the focal point for all traffic between Europe and the East, and access to this traffic enabled GC&CS to watch the growth of the Axis combination at first hand - yet, paradoxically, with little ability to influence the course of events.

* * *

III

AGD's career at this time involved attention to the 'how' of interception, the establishment of the Y committee, and the university recruiting drives of 1937 onwards. The memorandum ends:

> From August 15th 1939 onwards when the diplomatic and commercial sections moved to BP the university recruits began to join, so that by September 1st GC&CS was in action at its war station, already in process of growth towards that vast and successful body whose full story will perhaps never be told.

What is certain is that a very minor operation, underfunded to such an extent that a major bureaucratic operation had to be mounted in the mid-1930s to recruit half a dozen war veterans who had an entitlement to only half of their proper disability pension (all this is attested in the National Archives files), became in 1938-39 an important but unrecognized unit which would serve the Allies through the war with invaluable material, acknowledged by Eisenhower and used by all top military commanders, including Montgomery. It was understood by none better than Churchill himself, who knew the value of the naval intercepts from his experiences as First Lord of the Admiralty in World War I. He made visits to Bletchley Park, charted the daily results of the intercepts on his war maps, and eventually brought success to the British war effort and created, inexpertly, the ensuing peace.

Two events of historic importance appear in the pocket-diary for 1939. They both concern the developing interest of the French and the British in the intermittently successful attempts by a group of Polish government cryptoanalysts working near Warsaw to solve the secrets of the Enigma machine. Much has been written about this, of course, including a whole appendix in Vol. 1 of Hinsley *et al, British Intelligence in the Second World War* (HMSO 1979) pp. 487-495. At first the French had taken a more positive view of the Polish achievement than the British, and a conference of the three cryptographic establishments (Denniston was assigned the code-name Crypto) in January 1939 was generally regarded as only a modest success. The obsessive secrecy of GC&CS following the political disclosures of the early 1920s had not abated, and it was a not unnatural reluctance to share Dilly Knox's theoretical attacks on the Enigma problems coupled with doubts about the genuineness of the Polish achievements and (I would guess) an ancestral suspicion of the French that caused both Poles and French to register something like contempt for the British contribution to that conference, whose dates, whereabouts, and main participants duly appear along with

some exiguous expenses in the Denniston diary for the week. In fact, all three nations kept their secrets to themselves.

However little that conference achieved, events later in the year brought the Poles to the heroic point of handing over their complete work to both French and British. This took place in July 1939, and there are various accounts of what happened. The Britons were AGD as head of GC&CS, Knox as the Enigma expert, and a naval communications officer, Commander Sandwith. AGD's account of the visit, with subsequent additions, is now to be found in the National Archives and in chapter 7.

Much has now been written about the trip to Poland, to discuss with the French and the Poles the solving of the Enigma, the making of the Bombe, and the receipt by the British and French not only of the Poles' vital findings but of specimens of the machine itself. The party went from Dover to Ostend or Calais and by train across Europe. The passport, issued the previous year (possibly because they had expected to make this contact earlier), shows arrival at Calais on 24 July and Lille on the same day, passing back through Germany from Poland on the 28 July. On 14 August Bertrand brought the Enigma machine to Menzies, who handed it over to Denniston.

In December of that year, the phony war now in progress, there was a conference chaired by AGD in London. The French were represented by Bertrand and the Poles by Langer. 'During this conference', writes T. Lisciki, a graduate of the Warsaw Polytechnic who commanded a Polish signals unit and has recently set the record straight regarding the Polish contribution to cryptanalytical matters in this period, 'it was decided to establish this direct link and the question of which cypher to use arose. As the British Typex machine was super secret and the French did not have any, your father had a brilliant idea to use the German machine. This machine was used until the collapse of France and I doubt if the Germans ever had any suspicion of such "affront"'.

The admiral, that is to say Admiral Hugh Sinclair, Menzies' predecessor as head of the British SIS, bought Bletchley Park. After a successful 1938 dummy run those in control were more than ready, with Enigma in their hands and war declared on 3 September 1939, to crack the German codes which had eluded them for so long. And the university recruits came, 'the Professor types', mostly from Cambridge. They were paid £600 a year. In August Professors Waterhouse, Gore Brown, Vincent, and Boase joined and others, including the WWI veteran Nigel de Grey, rejoined. In September Gordon Welchman and Alan Turing joined and Frank Birch, Frank Adcock, and William Hope rejoined. Lord Dacre, in charge of the radio security service, told me how

he and AGD had got across each other during the war and had made it up at dinner at Christ Church afterwards; and he told a mutual acquaintance that in his view the state of friendly informality verging on apparent anarchy, which was such a feature of the early years at Bletchley, was AGD's particular contribution, that diminished with his departure to Berkeley Street with the diplomatic and commercial sections from BP. Travis was a more dictatorial supremo, probably what BP needed, but some Huts 3 and 6 veterans missed the former collegial atmosphere.

Many others came, mostly women. Some early reminiscences of their reception at BP are circulated. One published one, by Aileen Clayton, *The Enemy Is Listening* (Hutchinson, 1980), recalls:

> 'Station X . . . then under the control of Alastair Denniston, a quiet middle-aged man who seemed more like a professor than a naval officer. It was to him that I had to report, and I was immediately impressed by his kindness and by the courtesy with which he greeted me.'

The author goes on to give a vivid picture of Y intelligence at work in her first interview with Josh Cooper.

George Steiner wrote in the *Sunday Times* (23 October 1983) that increasingly 'it looks as if Bletchley Park is the single greatest achievement of Britain during 1939-45, perhaps during this century as a whole'. I am also indebted to Neil Webster for the following passage from his unpublished paper on intelligence:

> The cryptographic organisation at Bletchley was highly efficient. Indeed it was the most efficient working organisation I have met, perhaps because there were no trade unions and little or no financial control and because it was run mainly neither by business men nor career civil servants but by mathematicians and chess players, who brought detached and decisive minds to the solution of cryptographic, organisational and human problems. Contributory factors were the devotion, high morale, and esprit de corps of the picked band of workers. Gifted people were willing to work on boring and repetitive tasks if it was important that these should be done by people capable of spotting the occasional small nugget, which might turn up in the sieve.

Some photographs at the time bear out the informality and also the tension - AGD watching a game of rounders with his hand characteristically over his mouth, his double-breasted suit. Because of his small stature he and my

mother always took particular care of his appearance. In addition to his interest in technical matters, he devoted much time and thought to the building programme round BP, necessitated by the exponentially growing numbers.

His diary records on 18 April 1940: 'Birch to have copies of all naval traffic so that Hope can consult.' On the same day: 'esquimaux traffic: Stern not wanted: Falconer not wanted majority of RR material is by post; however TP's necessary'. This was the setting up of Hut 3 under Frank Birch, handling all the naval traffic. Meanwhile Enigma work, assigned to Travis, was concentrated in Hut 6 with Welchman, Turing, Babbage, Milner Barry and de Grey. And this is where office politics become inextricably tied up with winning, or trying not to lose, a world war.

IV

When we holidayed at Loch Striven in south Argyllshire in 1937 – one of several summer holidays cut short for my father by the exigencies of GC&CS as war approached - we included Ian Schiller in the party. Uncle Ian was a German who had come to adopt our family and made Y his honorary god-daughter. Despite infantile paralysis which left him partially lame he was adept at messing about in boats and since all our chattels had to be rowed the mile along the coast north from where the shepherd lived to our holiday cottage his skills were vital. My father loved boats and the sea, having been brought up near them in Dunoon, and I got the urge - He taught me the rudimentary skills of managing a dinghy. When war came my father's gift for friendship extended to the Americans who came to liaise with BP and Berkeley Street, chief among them Telford Taylor and his successor Major Bancroft Littlefield. Both men used to weekend at Ashtead in 1944 during the V1 and 2 bombing. Bancroft picked and ate our soft fruit while watching these lethal machines whizz overhead to do serious damage to more western parts of Surrey, while Telford played the piano (including duets with me), and tennis at which he was far better than us. In the evenings he and my father used to drink the whisky he always brought with him, and then no doubt my father opened up and told him more of the truth of his 30 years in signals intelligence.

My father's ability to make friends with his close colleagues was a major factor in his management style, and ultimately in the success of his undertakings. As an example, recent releases to the National Archives at Kew throw light on the early days of Bletchley Park, from the first arrival of Captain Ridley's hunting party to the autumn of 1939 when Knox and my father had returned from Poland with the Enigma machine. HW 14/1 discloses AGD submitting to Admiral Sinclair, his friend and boss and a tower of strength to him 'that the whole of GC&CS stays at Bletchley.... The large schoolroom is practically empty and it is proposed to put the commercial (i.e. diplomatic) section there. There is now under consideration a plan for the erection of huts just outside the grounds of BP to house the Service sections, including their necessary expansion, thereby facilitating the necessary expansion of various sections of SIS.' Sinclair envisaged the whole of MI6 stationed at BP, a scheme which would have been abhorrent to his successor, Stewart Menzies (minghis) who preferred clubland, whereas Sinclair, though he valued his creature comforts too, brought his own chef to Bletchley with him on his exploratory survey of BP's amenities, had more strategic plans. Unfortunately by Christmas both the chief of SIS since 1919 and his chef had died, the latter having committed suicide.

By now my father had trusted colleagues to share the load, chief among them Josh Cooper who recalled in 1975, 'At first our living conditions at Bletchley were very similar to what they had been in the Munich Crisis (of 1939).... There was as yet no pneumatic tube system at Bletchley, and very few messengers to get texts (i.e. deciphered GAF Enigma intercepts) from the teleprinter room to Air Section (Cooper's responsibility) and vice versa, so we used a contraption in which messages were put into holes drilled through large wooden balls, and rolled down an inclined gutter'. Cooper, whom I remember as a kindly, deaf man eager to help me rehabilitate my father, had worked at GC&CS before the war and eventually became head of research and development in GCHQ in Cheltenham, as Peter Wright revealed in his *Spycatcher*, a long and valuable career in signals intelligence.

This was only equalled by that of Brigadier **John Tiltman**, my father's other most valued colleague and lifetime friend till their deaths, who at BP headed the military section. Tiltman's remarkable career in signals intelligence - he could be said to have all but invented the modern science of deciphering British diplomatic and military intercepts - has already been set out in Ralph Erskine's fine monograph on his work and has thus had his rehabilitation. Tiltman wrote to me about my father and their friendship in 1981, remembering their years together and deploring the manner in which he had been rejected in February 1942.

Tiltman had the same gift of friendship as AGD but tended to go his own way and did not enjoy collegiate life. Equally non-collegiate - surprising for a Cambridge don - was **Frank Birch**. He was an experienced cipherbreaker of long standing, and had worked at GC&CS before the war, and of course was one of the Room 40 OB veterans of WW1. It was he who wrote the musical for Room 40 staff, *ID 25 in Wonderland,* in which many of his colleagues there, including my father and Dilly Knox, took part. He certainly had a vein of mercurial humour, but less innocent and childish than Knox's. Between the wars, when not teaching and lecturing at King's College, Cambridge, he came to London during the pantomime season where he was in much in demand to play Widow Twankey, a cross-dressing character that somehow suited him. We saw him at more than one winter pantomime.

By 1939 when he rejoined GC&CS, his secret career blossomed and by early 1941 my father directed that all naval Enigma material was to be sent to him. Now naval Enigma was Britain's key to not losing the U-Boat war, so that Frank Birch's achievements proved of national importance. What part he played in my father's leadership crisis of early 1942 I do not know, but since everyone except Josh Cooper and John Tiltman supported the move, he must

have been in the majority party. He remained within the high command at BP and after the war was one of the chief authors of the official secret history. His prose style was rather leaden compared to de Grey's but his factual account of naval enigma is at Kew and available to diligent researchers. For some reason he and I did not like each other, though my mother and sister liked him, and he was always respectful to my father. He invited us all to go swimming at Ranelagh where he was a member, and I remember watching his heavy, lumpish torso surmounted by a jowlish face and thinking 'he's up to no good'. Later I cast him as one of the great Cambridge nest of spies - say no.7 - but there is no evidence in the record or anecdotally of his playing that part. He was married to a Russian aristocrat and they were childless.

Dilly Knox, the most brilliant of all of them had not the same collegiate attitude to management but, despite that, spearheaded nearly all of BP's early crypt-analytical successes, and though difficult to manage, was as upset as any when my father left Bletchley in 1942.

Gordon Welchman, a Cambridge mathematician interviewed and accepted for BP by my father who struck up friendly relations with several senior BP mandarins, brought valuable organisational skills to bear on both technical and managerial problems as well as his teeming mathematical brain - he could think not just laterally but three-dimensionally, one veteran recalled, thus quickly inventing the diagonal plugboard which speeded up the 'research' (cryptanalytical) process at a time when speed was vital to get the messages to the service ministries in time for serving officers to use them in their daily tactics as well as their strategic planning. He dedicated *The Hut 6 Story* to Rejewski, Knox, Denniston and Travis.

Nigel de Grey was the oldest, though perhaps not the closest, of my father's friends and colleagues. The co-breaker of the Zimmerman telegram in 1917, he became a publisher in the interwar period but remained in touch with GC&CS, and he befriended my sister and me by giving us Medici prints of impressionists like Monet at Christmas time. He was first to hear of my success at the Challenge - the Westminster scholarship without which I would not be able to go to the school - from my mother whom I rang when the welcome greetings telegram from Downsend told them the news, and de Grey told both parents that that was the biggest intellectual hurdle, and that a glowing future in academia was thereby assured. He was quite wrong.

At BP de Grey's contribution from 1939 towards the breaking of Enigma was equal to Knox's or Cooper's or Tiltman's. He broke the Abwehr code which supplied us with daily information about Nazi atrocities against German and

Eastern European Jewry, but he was also the colleague who ungently thrust my father from his job as BP's supreme in February 1942. Their friendship did not survive this, and de Grey's own later account of GC&CS before the war seems to have been the product of the anti-Denniston attitudes that had developed by 1944-45, to counter which my father wrote 'The GC&CS between the Wars' which appears at Chapter 5.

Another cryptographer who appears in the literature of signals intelligence was **Hugh Foss** who accompanied my father on their abortive secret conference to Paris in 1938 with the French and Poles. Foss had worked at GC&CS since the 1920's and was a skilled cryptanalyst who played only a small part, according to the record, at BP. Another friend who visited us at Stapleford Mill Farm was a Cambridge don called F. L. Lucas whom I remember but can find no record of his BP work. Finally, not from GC&CS but from the top of MI6, Valentine Vivian (deputy to Menzies, 'C') and his wife became family friends of my parents since he retired as a colonel from the Indian army and lived at Ashtead to be near us. Vivian is largely a figure of fun, unfortunately, and Philby treats him mercilessly in his memoir *My Silent War*, but he alone came to my father's funeral in the New Forest in 1961 and told me what great work my father had down for his country and for the free world.

Ernst Fetterlein was a refugee from the Bolshevik revolution of October 1918. He and his wife escaped from Petrograd via a Swedish steamer, and landed at Tilbury to be interviewed by Sinclair who knew at once he had struck gold because Fetterlein had been the Tsar's chief cryptographer, and sported a large ruby ring his master had presented to him shortly before his murder. His breaking of the diplomatic ciphers of the new Soviet diplomats, Krassin and Kamanev, proved the greatest achievement of GC&CS in the early 1920s when British ministers revealed Broadway Buildings' successes at deciphering, interpreting and distributing evidence of Soviet revolutionary perfidy, much to my father's disgust. Thereafter the Fetterleins became friends of my parents and spent each Christmas Day with us at 48, Tedworth Square, bringing more expensive presents for us children than our parents could afford. Fetterlein did not go to Bletchley in 1939 with the rest of the diplomatic and service team, perhaps because Russia was deemed less important, as a neutral till 1938, and only became an ally (so ineligible for message interception) in the summer of 1941. Fetterlein's death in 1944 was noted in my father's diary for that year, as was Knox's.

Less important than his gift of friendship but not without significance throughout his life was the fact that my father was a keen sportsman, and became such a star hockey player at left half that he played for Scotland in the

1908 Olympics. He went on playing hockey, later tennis and squash and golf through middle to old age and since he was a kindly father taught me to play tennis and squash - though not hockey - and golf: for in 1937 we spent our summer holiday in Scotland and the pro at North Berwick - one of the sacred cities of that game - he showed me how to aim for the 'sixpence beneath the ball' and to swing so that in my teens I was a single figure handicap player and on a good day could beat my father - who was so pleased about this that he wrote to his friend and colleague William Friedman about it in the mid-1950s. In 1939 we spent several golf weekends at Barton-on-Sea (we had sold the bungalow in Fairfield Road by that time) and enjoyed the modest luxury of a seaside hotel. Between rounds we spoke little about non-golfing matters as neither of us was good at smalltalk, or conversation in general when not on pre-arranged topics. He must have known war was close since a few weeks after our last golfing weekend he went to Warsaw to collect an Enigma machine, but we did not discuss politics. He continued to play tennis and squash on return to Ashtead in 1942, and even after his retirement from the FO when he worked for a few months as foreign language teacher at Downsend school near Leatherhead, where I had been a pupil and whence I won my Westminster scholarship. But coaching cricket in your 60's is too strenuous and he retired properly to the New Forest where golf continued to be his passion and his pastime. He also grew vegetables with great care and attention.

* * *

V

Four separate factors had a profound effect on my father's career from mid-1940 onwards.

The first was the unexpected success achieved at Bletchley under his control and afterwards.

The second was his temperamental inability to exploit these for his own advantage and the consequent missed opportunities that others later identified for the enhancement of the work itself.

The third is a severe illness which struck him down and nearly killed him in 1941, but from which he was later to make a full recovery; indeed, he concluded his professional career on a high note of success which remained known to few and with which a later section of this monograph deals.

The fourth was the American involvement.

The success of Ultra in World War II is now history, though some war historians differ as to the extent of its influence in shortening the duration of hostilities. The success was due to a number of factors, for which the long pre-war preparatory years of interception, cryptanalysis, and distribution - integrated but secret - provided an invaluable base. Enigma could not have been broken in Britain in 1940 without Knox's theoretical work in the 1930s and without the mathematical genius of Turing and the technological solutions of Welchman. But the information provided still needed processing in a secure fashion, and this task, given the parlous state of the British war effort, the contrasting requirements and temperaments of commanders in the field and at GHQ, and the lack of an integrated hierarchy of leadership below the War Cabinet, was at least as taxing as the others. In all these AGD played a part. Perhaps the most crucial was the first, where he alone had the lifelong experience of and commitment to a total service of secret intelligence provision from cryptanalysis. Others came and went and came again. Newcomers were quick to learn. But the main instructor and implementer was AGD.

He was also at the heart of Y intelligence (interception of morse messages), vital to the GC&CS output, though increasingly overshadowed by Ultra. Oliver Strachey and Dilwyn Knox were both running important self-standing cipher-breaking units. The secret Abwehr codes – which revealed Nazi atrocities in Eastern Europe - were being read for some time before Enigma came on stream. Traffic between Madrid and Berlin was being read early on.

Bletchley Park had become an organization producing signals intelligence vital to the daily conduct of the war in Europe, and this both gives a context for the early days at Bletchley Park and illustrates some of the pressures created by the very successes of its cryptanalysis. AGD was not, however, a man who found leadership easy. He lacked self-confidence. He was a highly intelligent self-made Scot who found it difficult to play a commanding role amongst the bureaucrats and politicians with whom he had to deal. He doubted the discretion of most people outside the secret service, including his own superiors. He was no delegator. In essence he ran a one-man operation months long after it should have become a management structure. This had advantages as well as disadvantages. Professional recruits, as we have seen, appreciated the informal atmosphere in which much of their best work was accomplished. Security was maintained on the basis of highly individual commitment. But access to funds for expansion was badly hampered and it was not long before some of the new arrivals came together with some veterans, including de Grey and Birch and particularly Edward Travis who deputized for AGD during his 1941 hospitalization. They eventually decided to recommend to Menzies the replacement of Denniston by Travis. AGD was not cut out for high-profile leadership and his previous experience was no help in his predicament.

The organization of office life at Bletchley from 1939 to 1941 and the palace revolution that ensued is not available to the ordinary researcher and one has to rely on memories. P. W. Filby* remembers:

> Travis was deputy to Denniston and a crony of de Grey. They had endless talks in the crucial days and although they were held next door the walls were wooden and since we were almost always working in complete silence I couldn't help hearing the conversation sometimes. De Grey's voice was that of an actor and I knew ages before it happened that they didn't feel Denniston could cope with the enormous increase demanded of Ultra and other problems. AGD was headstrong and didn't like criticism; after all, he had carried the group throughout the 1930s, against criticism quite often, and now that war had actually occurred he wanted to be at the helm, in charge of the organization he had created. Travis and de Grey were perfectly right.

Other accounts of the February 1942 bouleversement at BP include Gordon Welchman's account in his *Hut 6 Story*. It is difficult, of course, to be impartial. To a brilliant young mathematician like Turing it must have seemed inexplicable, and culpable, that sufficient resources were still not available as late as the end of 1941 to carry out the tasks described in his famous letter

* No relation to Kim Philby

to Churchill. In Whitehall the prime objective remained to draft the best people into the armed forces: Bletchley Park then carried no cachet. Turing remained amazed at the authorities' inability to convince both Menzies and the War Cabinet of the importance of what was going on. Yet my father had spent years building the operation to its present size and shape, with Treasury parsimony and Foreign Office indifference as a constant companion. And it was AGD who had had the foresight to recruit Turing the day war broke out.

* * *

VI

The year of crisis for AGD would be 1941, the year in which he had to spend precious weeks and months in hospital at a time when Bletchley Park was growing exponentially with the early successes of Ultra, when the American involvement, as a prospective wartime ally and as sharer of the secret, was becoming ever closer, and when the new scale and nature of the organization he headed made the eccentric nature of his leadership particularly vulnerable. His diary entries for the early weeks of the year show regular meetings of the Y committee and with the DNI, the DMI, and Menzies, and visits from Americans, French, and Poles. But on 27 February a stone in his bladder was diagnosed (and a five-guinea bill for X-rays was noted). On 10 March he left Bletchley and three days later was operated on. Hospital bills ate up most of his net salary of £104 for that and subsequent months. He was discharged on 14 April but immediately contracted orchitis and was hospitalized at Ashridge until early May. A period of convalescence followed. He returned to the office on 9 June after nearly three months. Edward Travis, his number two, was in day-to-day command and by early August 1941 AGD had received authorization to make two arduous, and as it turned out vitally important personal visits to Canada and the USA. He left for the United States, flying via Newfoundland on 11 August, and his diary noted the questions he had for his American hosts. He dined with William Friedman on the 18th and returned to England on the 23 August. Expenses included a hotel bill of £41.

The friendship established between the legendary cryptanalyst William Friedman and my father was to give a strong base of trust and understanding to what was to become an Anglo-American joint enterprise handling of all signals intelligence. It was already well established when Friedman and his colleagues Colonel McCormack and Brigadier Telford Taylor arrived in England on 25 April 1943. By September, and despite setbacks, the agreement on complete cooperation between the two countries 'in all matters pertaining to Special Intelligence' had borne fruit. His own friendship with Friedman was also to last until his death in 1961. Many years later, in 1961, Friedman wrote to my sister:

> Dear 'Y'
> .... *Your father was a great man, in whose debt all English-speaking people will remain for a very long time, if not for ever. That so very few of them should know exactly what he did towards achievement of victory in World War I and II is the sad part of the untold story of his life and of his great contribution to that victory.* His devotion to the supremely important activities to which he gave so much of himself unstintingly, and with no thought to his own

> frail strength and physical welfare will never be forgotten by those of us who had the pleasure of knowing, admiring and loving him....
>
> William F. Friedman

In 1941 he was still an ill man (his diary records 'neuritis begins' on 26 August). Yet only a week after his return he was flying westwards again, this time to Canada. The expenses of that journey included a bill for £283, which was not deducted from salary, but the doctor's bill exceeded his net salary. On his second trip AGD flew to Toronto to brief the Canadians about British cryptographic achievements against the Japanese and warned that British material would not be made available unless the US cipher brain Herbert Yardley was removed. AGD's diary notes with rare circumstantiality that 'Montreal could train up to at least 100 W/T operators every three months'. That and the following week's expenses amounted to £400, all recouped from a float of £500 issued to him in two separate amounts. His purchases included unusually lavish presents for his family. He flew back from Ottawa via Gander. The flight took 15 hours. He was the only passenger and was put in the bomb rack, where he wore an oxygen mask which he removed only to eat chocolate, which was all that sustained him. He got to Ayr at 11.30am on 13 September, travelling thence to Hendon and home to the isolated farmhouse near Bletchley that he had rented for the duration. On the previous and subsequent nights, RAF planes were shot down. His survival was regarded by his family as a miracle.

It is surprising that at the height of this crisis year at BP in 1941 my father should have made these trips. The circumstances of the visits are still unclear, given that the United States was not yet in the war and matters at Bletchley must have needed his full attention. The files are silent on the matter of authorization. Yet the outcome of these trips caused him the greatest satisfaction, amply justified by history. He returned with the outline of the plan for American involvement in Bletchley Park and Berkeley Street, and in due course a succession of American officers were seconded to work with GCHQ in the UK. This may have been a factor in determining the American decision to enter the war on the Allied side in December 1941, though Pearl Harbor made that decision inevitable.

By August all seemed to return to normal in Denniston's professional life. America would not become our wartime ally for several more months. Without American involvement, despite Churchill's brave words, Britain remained a hostage to Hitler's master plan, or at least would find itself in desperate need of another Zimmermann telegram, another trigger to force American public opinion towards war. In 1941 few apart from Denniston knew about the management of the Zimmermann telegram, but no one of the

calibre of Sir Reginald Hall was around to exploit it, though there were a few Anglo-American intelligence entrepreneurs like Sir William Stephenson who had influence but insufficient discretion.

Before August 1941 America was uninformed about Enigma. Denniston saw that the British could do for the Americans what the Poles had done for the British and French - make total unilateral disclosure; but to whom, and in return for what? It could only be the entrance of America into the war, by playing the Enigma card so skilfully that a result comparable to that of 1916 could be achieved. Denniston himself was unqualified for the work but he recognized its crucial importance. Menzies had neither the background nor the influence so it was to identify who should be the American recipient of the information that AGD flew to Washington in July 1941. In establishing friendly contacts with Friedman and the others he played the Enigma card - less spectacularly than Blinker Hall with the Zimmermann telegram because it took another six months and Pearl Harbor to achieve the objective – but as well as he could. And, as further evidence of the importance of the World War I precedent, Friedman and Denniston continued to correspond on the minutiae of the Zimmermann episode, till close to the latter's death in 1961. In 1941 AGD had a similar opportunity to influence the course of a world war, recognize the opportunity, and play a modest part in turning defeat into victory.

On 19 September he saw Menzies. Later he met Vivian, de Grey, the DNI, and other friends, old and new. He continued to serve on the Y Committee. He had check-ups but had returned to reasonable health. We moved from the farmhouse to a small semi-detached house called Friedenheim just outside the gates of Bletchley Park, which now was renamed not GC&CS but GCHQ. Christmas dinner was celebrated *en famille* with 'The Profs.' - Boase, Last, and Adcock at Newton Longueville where the mother of a family friend, Rhoda Welsford, had rented the old rectory a mile from the gates of Bletchley Park. But pressures inside the gates were mounting. He remained as Director until 30 January 1942, when he was moved sideways to become DD(C) (Deputy Director in charge of commercial and diplomatic traffic) a fact that was duly noted without comment in his diary. The move to the gates of Bletchley Park was followed by a further move back to our house in Ashtead, Surrey (since he was to work in London), where he had lived before the war and whence a number of ultimately distinguished cryptographers had been recruited by him into GC&CS.

Ronald Lewin writes of AGD as a man of great charm and integrity, and a skilled and experienced cryptologist:

> 'He could also no doubt have become a technical expert in breaking Enigma's machine ciphers, but he carried the heavy administrative load involved in expanding his peacetime GC&CS into a wartime organization. His health was poor ... he needed the support of a practical specialist, but the brightest star at his side, the scintillating Dilly Knox, was a man very specifically, of letters ... Denniston's personal contribution to the success of Ultra has not yet been properly appreciated.

What is certainly true is that Knox had mastered some of the theory behind Enigma even before the encounters with the French and the Poles, that the two of them so impressed the other parties when they met that, despite the official British Government passivity referred to by Bertrand, they were allotted crucial tasks in the undermining of Enigma's secrets, and that Knox, even before the arrival of Welchman and Turing, had proceeded far into theoretical solutions. Thus, Knox was upset and irritated when these brilliant young mathematicians took over, Welchman developed the Bombe without which daily decrypts would have been impossible to achieve, and computers began to see the light of day. Welchman's own account of this crucial and moving moment carries the sound of truth as well as innocence. So Knox perhaps deserves the credit for Enigma, and Denniston for Ultra.

Denniston's relegation caused a tremendous rumpus, out of all proportion, one might think, to the actual event. The knighthood which was his due, in the view of a whole generation of veterans of the secret service, was not to be his. Charles Whiting believes that mutual dislike between Denniston and Menzies was the cause of the decision, with Menzies paying off old scores, demoting and finally retiring him on a pittance. F. W. Winterbotham more charitably reported: 'It had been considered advisable to put all the departments at Bletchley under one director, Commander Travis, who was put in to replace Commander Denniston, the real founder of Ultra, now posted back to London on other cryptographic duties'.

Since the event signalled the beginning of his most successful years as a 'total-service' cryptanalyst, it is worth trying to find out what happened and why. AGD facilitated the arrival of the mathematicians and their solutions of machine decipherment, but he remained deeply worried about security. This was his obsession. All would be lost if Germany knew what we were reading. However difficult it would have been for the High Command to switch from Enigma they would certainly have done so, or at least made access many times more difficult, had they seriously suspected that they had been compromised. Elderly German ex-cryptographers still cannot believe the Bletchley achievement. That Denniston felt this so strongly was due to

his length of service, which gave him a perspective and an understanding of the need for a total service, which was not available either to newcomers or to pure specialists, for whom problem-solving was the whole story. He was particularly worried about the arrival of Menzies. He had similar misgivings about Vivian's arrival. My father had become paranoid about security, and hence a poor delegator and communicator. To Admiral Sinclair he could always talk, but his successor was very different. Menzies was a WWI hero and conducted most of his secret MI6 business at White's Club in St. James's and BP's intellectual feats were simply beyond him. Also, as a manager of difficult and clever men he was almost useless.

The ill health which was the ostensible cause of my father's removal was soon overcome, and once established at the Berkeley Street office 'above Peggy Carter's hat shop' he never missed a day's work until retirement. He accepted demotion and settled down to make the new job work. The embassy-listening post at Palmer Street was still active and provided plenty of material, as we shall see.

Confirmation of the quality and importance of the work of DD(C) and his team at Berkeley Street is not easy to come by. This is not only because of the official embargo, but also because of the office politics and personalities involved. The more successful the work the more some individuals wished to take it back to Bletchley Park and reincorporate it there. The only published story is a tantalizing one in Kim Philby's *My Silent War* which is given some further context in Andrew Boyle's *The Climate of Treason*. Given the scepticism (not always justified) with which Philby's revelations have been received, it may be better to rely on the painstaking Boyle. It is clear from both accounts that the successful playing off of Berkeley Street and BP was a watershed in Philby's career as a double agent.

In the autumn of 1943 Philby was in charge of the Italian, African, French, and Iberian counter-espionage sections, working from Ryder Street. His boss was Felix Cowgill and his current undercover job was to replace Cowgill by himself - a vital step in his own double career both in MI6 and in Russian intelligence. Several of their colleagues, American and British, knew what was going on. With Cowgill absent in America, Philby, promoted to be his deputy, raided his filing system and memorized a file of German Foreign Office material opened by the Americans and validated by Allen Dulles of OSS, despite rejection by the British. Dansey received copies and took the official British view of their authenticity: so Philby sent samples of the Dulles material to AGD, who quickly proved that the Americans were right and the British wrong. Philby sent more samples, which proved identical to some

AGD's wartime passport photograph

AGD (left) with Professor E.R.P. Vincent, one of the Hut 4 Italian experts (centre), and Colonel John Tiltman, the brilliant codebreaker.

AGD's 1939 passport, now on display at Bletchley Park

AUGUST **MEMS** **1941**

17 Sun—10th after Trinity

Richmond 4 1938
Rowlett Sclarke

18 Mon

Annual Test 7/..
8.30 Navy 1621

19 Tues

8 3.. Grey 37.41

Whitehouse :

20 Wed

Ka 78/30
Sat 83/(32)

21 Thur

2 1001 ... 1
for C. de Grey

22 Fri—● New Moon, 7.34 p.m.

New York - Brant
Pictures

23 Sat

Return
Lance

The entries in AGD's in August 1941 when he flew to the USA for a meeting with codebreakers there.

HW 19/45 13

COMMANDER DENNISTON.

Following are my observations on your comments in connection with your forthcoming trip to U.S.A.:

Para. 1. I am not clear what Ottawa is trying to solve, but if it is merely French Messages, I see no harm in your visiting Commander Brand to find out the position, and then judging the advisability of meeting members of the National Research Council. I am confident, however, that the Americans will not play so long as Yardley is at Ottawa.

Para. 2. This, though delicate, should not be insoluble, as it would seem essential that the F.B.I. should work on the groups, but clearly should not concern themselves with diplomatic traffic.

Para. 3. I agree generally with your note, but I am a little uneasy about the proposal for young mathematicians to come over here prior to their entry into the War. If they disliked the work they would be in a position to resign, and what hold would there be over them? In other words, it would have to be understood that once they came, they should remain here so long as America had not entered the War. Could the American Authorities take steps to ensure that they would, either now or in the future, never publish anything of what they had learned? Would the individuals be regular members of the American G.C.& C.S., or merely be young scientists, owing little allegiance to this specialised Service.

I should feel inclined not to mention the Hollerith machinery, as this might be used as an argument for entrusting the American firm with the construction of the Bombe, not that I would be prepared to give way, and I am glad to know that you are talking of 36 as being our goal.

Para. 4. If Hastings could be made the liaison for both parties, that would eliminate the necessity for nominating an American Officer in London.

Para. 5. I agree with this paragraph.

5th August, 1941.

Memo to AGD prior to USA visit, 5 August 1941 (author unknown)

1444 — 57 29-9-41

Mr. Smith
Capt. Hanley } to see & ret. me. 2919.

he Director

HW 14/45

The American Section.

Since my return from Washington the question of continuing to decypher so far as possible American diplomatic telegrams has been raised in various quarters, and I am asked if it is worth the effort as the co-operation between the various departments of the two countries is now so intimate.

If you and the Foreign Office should decide that such work is unnecessary, I feel that perhaps in view of ultimate peace negotiations when we might wish to know American views fairly accurately, it might be advisable to keep Miss Curtis as observer of the traffic passing so as to watch all cryptographic developments and where necessary ask the Research Section to investigate new systems which might occur.

When in Washington, I was told that the State Department had had little advice from the War and Navy Departments on the subject of their cyphers, which the two latter departments knew to be insecure but that early in this year the State Department had formed a committee including Friedman, chief adviser in the War Department and Safford of the Navy Department to advise on their cyphers and I therefore anticipate changes before so very long.

I should be grateful for an early ruling on this problem as among other questions, the censors abroad from time to time ask if it is necessary to recable American Government messages and I am inclined to answer in the negative.

A. G. D.

29th September, 1941.

AGD memo, 29 September 1941, following his visit to USA

Bletchley Park staff c1940/41: seated (left to right), E. M. Smith, Edmund Green, Barbara Abernethy, Patrick Wilkinson and Alan Bradshaw; standing (left to right), Philip Howse, Stephen Wills, Captain Ridley, John Barns, George McVittie, Marjorie de Haan and A.G. Denniston, head of GC&CS.

ing the Foreign Office for permission. If Denniston is right about the difficulty of solving the Iraq system, what sense does all this make? Some of these Britishers, I think perhaps including Denniston, think we in Washington are a little bit at loose ends, and what do you suppose I would think, if my thoughts made any difference, when I get three cables in short succession, one of which says that cables were omitted because nobody asked for them, the second says there were omitted because the parties were exchanging them through censorship, and the third says there were omitted by common consent. Jesus. Taylor has been talking to Denniston about the Iraq matter and

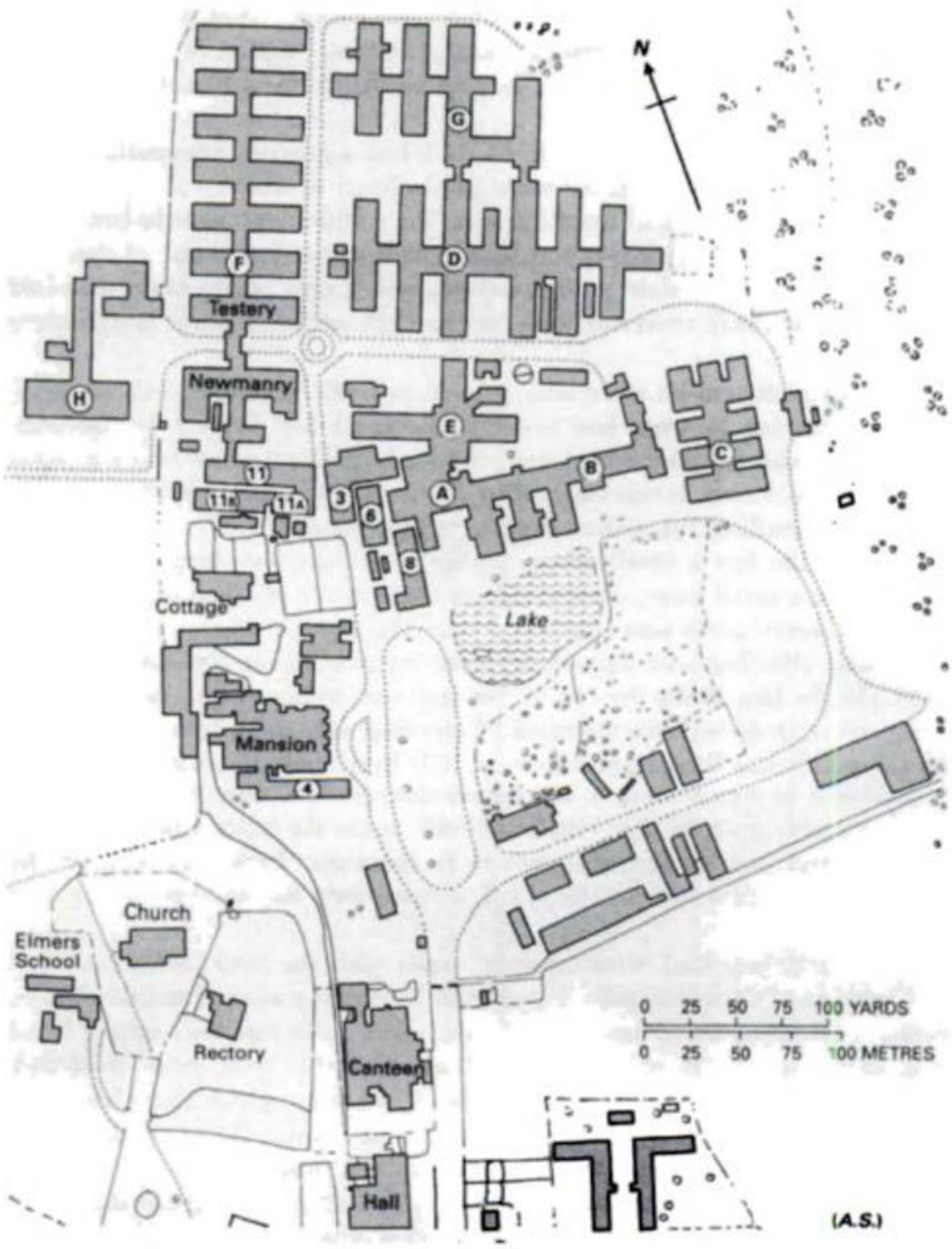
TOP SECRET

SECRET

ULTRA

Extract from US Embassy, London, memo June 6 1943 concerning Arlington Hall's liaison with Berkeley Street

Bletchley Park (above, and below, plan of the grounds)



FOR WASHINGTON thw 14/45 19 CXG 139.

Personal from DENNISTON.

In a telegram from War Department A.16 of 18th December they raise the question of investigating the German Air-Army cypher. During my visit it was agreed that we should be responsible for this investigation and that when U.S.A. were in real need of this work we should invite their party to join ours.

Could you find *out* if their views on this procedure have changed and if they wish to begin their own investigations now? It is devoutly hoped by all here that any such investigations will not interfere with their progress on Japanese work for which we count on them.

We could send by bag two days of traffic and certain keys (all information on this being sent in cypher) but bag communication is very slow.

Could you also find out if they are intercepting any of this material?

I am sending by bag material for German air to ground traffic.

23.12.41.

AGD memo to Washington, 23 December 1941.

of Berkeley Street's recent diplomatic intercepts with which they now hoped at last to crack the German diplomatic code, Floradora. Philby successfully exploited the animosities not only between Cowgill and the rest of the British establishment, but also between Bletchley and Berkeley Street, to further his career and international aims.

Berkeley Street was clearly no backwater, and this is confirmed by the fact that the Americans assigned a senior officer, Brigadier Telford Taylor, to work with the British on diplomatic traffic and later, Major Bancroft Littlefield. Harder evidence is adduced by Denniston's official Number Two, Bill Filby, who writes that Denniston took with him the German, Japanese, Middle East, Portuguese, and Spanish groups, and

> on seven floors we worked like beavers - for our hero, AGD. He was in every day, visited the sections almost daily, and encouraged all of us by the intimacy he had with the janitor to the heads of the sections. Obviously he was disappointed and extremely bitter, but whenever I went to stay with him and with Dorothy he was relaxed. The villain of the piece was really a man named Freeborn, leader of the machine group from Letchworth. He was power hungry and realized with AGD out of the way he could manipulate to his heart's content. Even Travis would generally address Freeborn: 'Mr Freeborn, we have a particularly difficult time in front of us. Do you think you could spare a few machines?' Freeborn would look at a board and ruminate, and would finally state that if he cut A and B he could accommodate Travis. Having got his way he attacked AGD unmercifully, and because his Hollerith machines were now all powerful he virtually controlled all but Ultra. AGD was given the sop at Berkeley Street but to the horror of Freeborn it turned into a gigantic success for AGD. We used to work 18 hours a day, seven days a week as if to prove that AGD could control and direct. 'C' was always on good terms with AGD and one day in 1943 he was able to turn to AGD and congratulate him on a great success, with more to come. Freeborn called me in his office and he asked me to come back to Bletchley with my team. 'Travis will OK it if you wish.' I declined and he promised to stop further promotion.

Robert Cecil, one of Menzie's senior staff, adds the following memoir:

> Looking back, forty years on, I ask myself why I did not know him better. Part of the answer is to be found in the age gap. AD had made his reputation as a cryptanalyst in the first World War. But part of the answer must lie in the character of AD himself. He seemed a very self-contained Scot, perhaps a little dour. I think his long and sometimes discouraging

experiences of GC&CS had etched in this characteristic more deeply. Between the wars, his work had suffered both the neglect of politicians, who had not provided enough resources, and the levity of politicians who, in a moment of loud-mouthed indignation, had given away to the Russians the hard-won insight into their cyphers.

When World War II came, money began to flow again and the huts rose up rapidly at Bletchley; but by then there were less scrupulous and more ambitious men on hand to skim off much of the credit. Denniston left Bletchley and came back to London to escape the back-biting and get on with the job; he disliked the in-fighting more than he feared the Luftwaffe.

These characteristics stood out in the period 1943-5, when I knew him. I was one of the personal assistants of 'C', Menzies. Heads of sections, each armed with a choice tit-bit of intelligence, used to carry it in to 'C' as if it was all their own work, in the hope of basking in the sunshine of vicarious success. Not so AD. He would make a careful selection of the most telling diplomatic intercepts (in the FO we used to call them 'BJs'); but these were always sent to 'C' in a locked box by hand of messenger.

The diplomatic section has not achieved as much celebrity as the military section, which produced Enigma. We never read the top German diplomatic cypher, but we read all the Japanese and enough of the neutrals' in the difficult days when most of them thought we should lose the war. When it was Hitler who was losing, the Germans were telling the Japanese everything that would keep them fighting in a lost cause. For example, they were telling the Japanese Embassy in Berlin all about the wonder-weapons V-one and V-two. They were telling us, too, though they did not know it.

Denniston always kept his ship on an even keel and his staff, who included a number of brilliant eccentrics, liked and respected him. One of them, whom I remember, had come down from Oxford with a First in Egyptology and had then become an astrologer; when his eccentricities began to affect his colleagues, Denniston just sent him on sick-leave and welcomed him back, when he was restored.

My father retained the special relationship of mutual trust and disclosure with the Americans. This is confirmed by letters from two American veteran cryptanalysts, Abraham Sinkov and Frank Rowlett:

January 20, 1991

Dear Mr Denniston,

... I came to B.P. in early 1941 with a small team of Americans whose mission was to initiate collaboration in signal intelligence with the UK. We were greeted on our arrival by Cdr. Denniston who graciously welcomed us to our task and indicated how we would be accommodated and would function in our mission. ... I remember that he was highly considered by the Bletchley personnel ...

Abe Sinkov

30 April 1991

Dear Mr. Denniston

.... I remember well your father's visit to Washington in August 1941. It was his visit which laid the foundations for the collaboration between the cryptologic activities of the US and the UK which produced intelligence vital to the successful prosecution of World War II. We spent considerable time together discussing the technical activities undertaken by both countries and worked out some of the details of our early collaborative efforts. Some months later I spent several days, at his installation in London where I was treated most graciously by your father and his staff. ....

Frank B. Rowlett

CHAPTER FIVE

Diplomatic Eavesdropping 1922-44

Based on an article published in Intelligence & National Security

I

Diplomatic eavesdropping in 1922 was not a new or recent practice, but the coming of wireless telegraphy (WAT) at the turn of the century gave access, via interception and decryption, to greatly increased volumes of traffic. Much of this would have been worthless, emanating from chancellories without power or influence to affect the course of European affairs. But not all. For the victors in World War I and from the signing of the Treaty of Versailles, British, French, Italian and American codebreaking departments were re-instated or established. The use and abuse of the material thus provided has been tacitly acknowledged but rarely studied. In Britain the history of signals intelligence, known as sigint, has concentrated on the Admiralty codebreaking department in Room 40 OB (Old Building) during 1914-18, and the interwar abuse of Russian cipher insecurity, fuelling the anti-Bolshevik scares of the 1920s and precipitating a Soviet change to a more secure cipher system. 1939 brought not only a new world war but a new dimension of cryptanalysis involving breaking machine-enciphered messages. The Enigma breakthrough and what followed therefrom has been well documented. This chapter is about non-service - that is diplomatic - traffic, much of which was enciphered by systems which predated machine encipherment.

The new source disclosed is the diplomatic component of the files that came to Churchill from MI6 from late 1941 to VJ Day. It is called DIR/C, and in the Public Record Office system it is known as HW1. The value of this material (described by retired government officials as 'the intercepts') can now be assessed, because Churchill proved to have been a prime user of diplomatic sigint, and his daily files of intercepts have now been released, though some items are still witheld. Their release is the first and almost only indication that

diplomatic eavesdropping – on friends, neutrals and enemies - was a part, and as it turns out a major part, of the British cryptanalytical effort in wartime.

Recent researchers have discovered much about British Sigint efforts of the interwar period. These reveal that as a source of reliable and relevant secret information, human intelligence, or spying, was less useful than the decryption of intercepted messages - Sigint. This applies as much to diplomatic as to wartime sigint. The leading neutral was Turkey. Turkish foreign policy was conducted by no more than three high government officials - the Prime Minister, the Secretary for Foreign Affairs and above all the State President General Ismet Inonu - and these all relied heavily on the reports of Turkish ambassadors to Europe in London, Rome, Berlin, Tokyo, Washington, Stockholm, Kuibyshev/Moscow, Madrid, Lisbon, Berne, Vichy; in South America, Buenos Aires and Santiago; in East Asia, Bangkok and Tokyo. These same reports, encoded and cabled to Ankara where they were reprocessed into their original French, were consistently intercepted and monitored by the British and German foreign office decryption departments. Thus they were available to, and used by, both Hitler. It is possible now to construct a hidden dialogue between Churchill and Inonu on whether and how Turkey should join the war.

This would have been impossible without the release of DIR/C, for then there would be no BJs to read and little evidence that they ever existed. Prior to this the very existence of a government department involved in the interception and decryption of foreign diplomatic telegrams has been unacknowledged. In releasing them, Government Communications Headquarters (GCHQ) revealed that neutrals' signals were being read.

* * *

II

In order to understand the use the FO and other departments made of BJs the prewar methods of interception, decryption, assessment, translation and distribution by GC&CS require some further explanation. The DIR/C (1941-5) files contain a surprisingly high proportion of BJ material, and this calls for comment, since Churchill's daily intercept reading was hitherto thought to be largely if not completely devoted to Enigma/Ultra – 'high-grade' intercepts arising from the North African and Eastern Front campaigns, the war at sea and the Far East. In fact about one quarter of DIR/C is BJ-related. And of this a significant proportion related to or emanated from Ankara's determined efforts to stay neutral.

Each file contains up to 5 items:
(1) The crucial component is 'special messages' - highgrade sigint, Enigma/Ultra. Nothing in the discovery of BJs takes away from the primacy of this material, given its uniqueness and authority as a source. Victories in North Africa and the Mediterranean, victory in the U-Boat war, victory against the Italians and eventually the Germans were all notably advanced by Enigma/Ultra.
(2) 'Naval Headlines' from Hut 1 at Bletchley Park (BP),
(3) Intercepts of *Abwehr* traffic.
(4) Internal correspondence generated by the PM's queries.
(5) BJs.

(1) The '*special messages*' so designated by the head of the Secret Intelligence Services, Major-General Sir Stewart Menzies, universally known as 'C', have rightly provided the main focus for historical research into the conduct of the war. A fiction that these were not intercepts but reports from well-placed agents survived till 1945 by the use of the codename 'Boniface' to describe them. Boniface appears and reappears throughout the series: also 'source glimpsed' or 'source caught sight of a partially burnt message', etc. - indicated some groups were corrupt.

Notes and comments, separated off from the messages themselves, are often supplied by the sending department at BP, which maintained war maps and backup to ensure the accuracy of the material and its contextual relevance. So places identified are so indicated, and references to people and events that appeared in earlier messages are given. A growing professionalism in the use of service jargon (Hut 3 employed only civilians at this stage) may have been expedited by Churchill who as a former serving officer knew the vocabulary of war and sometimes corrected the messages that came to him. Additionally he

annotated them, in the form of exclamation marks, circles on figures of Axis service and even civilian casualties, queries to the Chiefs of Staff, the Foreign Secretary, complaints to 'C', some late night doodles: and occasionally a delphic comment. 'Fear', he writes on one sheet, 'it does not prevent, it may even provoke action. But it is there all the same.'

Distribution is indicated by initials, most of them unidentifiable except WO (War Office), ADM (Admiralty) AM (Air Ministry) and BB (Broadway Buildings - where MI6 was located.)

(2) *Naval Headlines.* These are numbered, presumably from 1, sometime in 1940, to 1479 on 4 June 1945. They itemise the movements of the German and Italian navies and the miniscule Spanish Navy, and include messages from the Spanish Blue Legion of volunteers who served on the Eastern Front. At a later stage this division by origin changed to a division by war zone - Home Waters and the Atlantic; the Mediterranean and Black Sea; and the Far East.

The Italian material came on stream early due to GC&CS's monitoring of Italian naval and diplomatic traffic which started in 1936 with the Abyssinian crisis and the Spanish Civil War. Thanks to BP breaking the Italian cipher the British severely damaged the Italian Fleet off Cape Matapan on 28 March 1941. Thereafter shipping movements in the Mediterranean were monitored so comprehensively that loss of transport for men and materiel brought an earlier than expected defeat for the Axis in North Africa in 1942.

Naval headlines were only distributed internally, and to 'Director' (C). Churchill rarely annotated Naval Headlines; i.e. he circled tonnages of Axis ships sunk.

(3) *Abwehr intercepts.* These appear due to an early breaking of the Abwehr codes, used by Himmler for orders to his henchmen who reported killings of Jews (until they were ordered not to). At Hut 3 Nigel de Grey, a veteran cryptographer of 1914-18 and the breaker of the German diplomatic cipher which produced the Zimmermann telegram, asked whether reports of this 'butchery' had to be continued. However, evidence that reporting continued until December 1942 is suggested by Sir Anthony Eden's parliamentary reference on that day to 'receiving reliable information of the barbarous and inhuman treatment to which Jews were being subjected'.

(4) *Internal correspondence* generated by Churchill's comments and queries, including questions to FSL (First Sea Lord, Admiral Sir Dudley Pound, later Admiral Sir Andrew Cunningham) about whether to close the Straits to Axis

shipping, queries to CAS (Chief of Air Staff, Air Chief Marshal Sir Charles Portal) on bombing results, aircraft shot down - Axis and Allied - casualties and damage achieved, comments to CIGS (Chief of the Imperial General Staff, General Sir Alan Brooke) criticising generals, complaints to 'C' for not getting the gist of this or that Enigma message to commanders in the field - despite the fact that a sophisticated system of Special Liaison Units (SLUs) had been set up to do just this. Menzies and Churchill regularly discussed cipher insecurity. Churchill used DIR/C on an almost daily basis in his direction of the war effort and foreign policy initiatives centred on non-belligerents until D-Day began in June 1944.

(5) *BJs.* BJ telegrams did not just drop from heaven to become Churchill's daily wartime reading. What they were, where they came from, how they evolved from the routines of Room 40 OB in World War I, who got them and what they thought of them, and what was done with them, then and afterwards, all throw light on Churchill's wartime use of them.

They became part of Whitehall life as early as 1922. Before that, Great War interception and decryption of naval, military and diplomatic messages were handled respectively by Room 40 and MI1b. In 1919 decisions were made to maintain an interception and decryption operation based on two methods. One was cable censorship, whereby diplomatic messages from and to foreign embassies in London were sorted by the Post Office and scrutinized by GC&CS. The other was listening posts maintained by the RAF at sites on the Norfolk Coast.

The British were not alone in identifying the importance of the new Morse-based signals intelligence which became available with the development of Wireless Telegraphy (WT). Similar work was undertaken by most major powers, including Britain, by Germany, France, Russia, Italy and the USSR. The results, for Germany, produced by several large and efficient decryption bureaux, surpassed anything achieved by the other major powers, for it was by exploiting diplomatic eavesdropping that Hitler drove German foreign policy in the mid-1930s. The British targeted the USA, France, Turkey, Germany (without success) the USSR and Japan. Japan proved of particular importance, given her aggressive tendencies in the 1930s and her conservatism over cipher policy. So was Turkey. Between 1919 and 1939 GC&CS obtained knowledge of the cryptographic methods used by all powers except those which had been forced, like Russia, to use One Time Pads or who like Germany had moved to machine encipherment, or those with contiguous European land boundaries who could use landlines to ensure cipher security.

The Abyssinian Crisis and the Spanish Civil War (1935-39) provided sufficient volume of machine-enciphered messages, diplomatic and military, to explore machine encipherment. The Far East yielded valuable intercepts to and from military attachés in Europe. Quantities of Italian naval and military traffic came in as a result of Italian imperialism in Africa and Spain: and diplomatic messages had been read before that. What was produced was valued at the time, and proved invaluable as the basis for greater decryption later on.

From the early months of WW1 the whole operation depended on successful interception. Without interception there could be no intercepts and no clandestine eavesdropping. The British seem to have been alone in adding cable interference as an additional means of reading messages - though telephone tapping became standard practice by other European chancellories in the 1930s, and tapping into landlines used by others has also received a passing mention. The operation of censorship is impossible to track, for lack of any references in the files. But the building of intercept stations in the interwar period in England, Scotland, Iraq and India, was on a substantial scale, whose funding has only recently been identified. GC&CS may have thought it was a Cinderella operation but the backup resources which enabled it to function at all were expensive, elaborate and efficient. Each intercept station had between 16 and 23 men, including cryptanalysts. About 1,400 men worked in these stations, most of which were managed by the RAF, though the Foreign Office maintained its own, run by the Post Office. Additionally by 1925 5 officers and 4 other ranks worked in cryptography in Baghdad while up to 1935 the Royal Navy had formed a separate unit composed of 5 officers. Between 1920 and 1939 the Indian Army's HQ maintained a cryptanalytical section of 5 officers. So the services probably had 20-30 cryptanalysts between 1925 and 1934 and perhaps 40-50 by the later 1930s. Brigadier John H. Tiltman was their chief, before he was seconded to GC&CS where he served throughout the war. Costs averaged £5,000 per station. By 1939 it cost £15,600 to build a new interception station in Britain. The extent and sophistication of the interception network is demonstrated by a 1942 summary of intercept stations - chief of them at Cheadle, Chicksands, Waddington (RN), Kingsdown and Brora - which lists the countries targeted, the volume of traffic and the callsigns and frequencies.

The work of GC&CS in the interwar period was undertaken by a small group of 'Senior Assistants' and a slightly larger group of 'Junior Assistants'. GC&CS was well equipped to handle the great wartime expansion required by the continuous breaking of Enigma, Shark, the Abwehr machine and hand ciphers, and other medium-grade signals intelligence deployed against diplomatic as well as service traffic before and during the war.

At the end of 1919 GC&CS employed 66 staff. This number went up to 94 in 1924 but of these 65 were support staff, leaving only 29. By 1935 there were 104 on the payroll, of which 67 were support staff. The Abyssinian War produced a temporary need for Italian experts, who were laid off when the emergency receded, but later supplied a firm basis for Bletchley's outstanding Italian section. A few stayed on anyhow, because other and larger war shadows were looming. In 1939 there were 125, but 88 were support staff, the experts remaining at 35. Of these an impressive roll call - Ernst Fetterlein, John Hitman, Henry Maine, Oliver Strachey, Dilwyn Knox, 'Josh' Cooper, Hugh Foss, Thomas Kendrick - testifies to the success of the early recruiting procedures. Qualifications for working at GC&CS included fluency in at least one language other than English. Most were German and French speakers, a few were multi-lingual, in particular Knox. Two (Ernest Hobart-Hampden and Kennedy) were Japanologists: Fetterlein was in earlier years the head cryptologist of the Tsarist foreign service. Linguistic skills not only gave a beginner immediate entrance into intercepts by way of translation, but the skills of a linguist include a facility in guessing meanings from context, word-frequency, letter patterns, the spotting of cipher errors, and the identification of special vocabularies. Ability at mathematics was also highly rated.

Little is said in my father's account of GC&CS between the wars about training, which tells its own story. On training the Foreign Office early on took the view that 'the only way a man can learn to be a cryptographer is by devilling for an expert. A training programme would be an impossibility'. The six or so senior assistants were all proven cryptographers with a track-record of achievement and expertise stretching back in some cases to the beginning of wireless interception. Cryptography or crypt-analysis has a history which goes back to ancient Egypt, and in the USA formal cryptanalytical training, including the history of the subject, was promoted energetically by the Head of Army Signals Intelligence, William Friedman. He was a scholar of the subject as well as a leading practitioner. But there is no evidence of similar training for interwar GC&CS recruits; training was mostly 'on the job', and this is confirmed in the memoirs of recruits to Bletchley Park between 1940 and 1943. By then the techniques were changing so fast, and the work to be done was so urgent, that formal training may well have been impossible. In the prewar GC&CS the Head and his Deputy and the Senior Assistants had together considerable cryptographic experience behind them, but regarded their job as too hush-hush even to give it a name, much less a pedigree and academic respectability. They referred to 'special work' as opposed to 'administrative duties'.

In fact the difference in training methods between Britain and the USA seems to have been one of degree rather than kind. However by 1941 the British were well ahead of the Americans in the application of cryptanalysis for the day to day problems of peace and war.

The age and previous experience of most recruits, until the arrival of Oxbridge graduates in the mid-1930s, would indicate that a career structure within GC&CS would have been impossible anyhow. Within the Civil Service as a whole there was, of course, a clear structure involving promotion after 15 years, change of job description and status, increasing salary and the prospect of a decoration of some sort towards retirement. GC&CS's staff, both senior and junior, were explicitly bound out of the civil service establishment structure and the pensions which went with it. Yet to achieve what they undoubtedly did required intelligence, dedication, discretion, flair, self-discipline and self-motivation of an uncommonly high order. These qualities did not grow naturally in the culture of the prewar civil service. The dichotomy between what was needed and the lack of incentives, both for recruits and experienced staff, was well known to my father from 1922 to 1944. 'It must be remembered that beyond a salary and accommodation vote GC&CS had no financial status; it became in fact an adopted child of the Foreign Office with no family rights, and the poor relation of SIS (Secret Intelligence Service) whose peacetime activities left little cash to spare'. While its relation to the Foreign Office is well documented, its closer relation to SIS, whose interwar head Rear-Admiral Hugh Sinclair acquired responsibility not only for GC&CS but also Interception and Direction Finding, remains totally secret. Anecdotal evidence suggests that while the FO hand was a dead one, Sinclair saw to it that GC&CS had the freedom and resources which made possible its expansion and move to Bletchley Park in 1939.

My father's account of GC&CS between the wars deserves a chapter to itself.

CHAPTER SIX

The Government Code and Cypher School Between the Wars

This was the seminal report by my father, published in the first issue of Intelligence & National Security *on which many historians of signals intelligence have relied He wrote it shortly after his retirement and my mother typed it on her ancient typewriter.*

I

In paragraph 10 of 'Post-War Intelligence', a memorandum by Group-Captain Jones, occurs the remark in large type:

> It would indeed be a tragic and retrograde step for intelligence as a whole, and therefore – this is not putting it too high -- for the future of the country, if GC&CS were to sink back into its pre-war position.

I think I am right in taking these words *not* as a general scathing criticism of the pre-war activities of GC&CS but as a warm tribute to the efficiency of the wartime development in GC&CS of its new function of 'Intelligence' at the source, a tribute with which, I am sure, none of the service departments will quarrel.

But in justice to the late Admiral and to the members of the peace re-organization of GC&CS who, for 20 years fulfilled their allotted task and reached 1939 with a solid foundation on which to build, I propose to state quite briefly for the information of those now about to build a new GC&CS:

A The origin and purpose of the 1919 GC&CS;
B Its establishment under Treasury control;
C Its development.

Files and records sent to safety in 1940 are not available to me, therefore I write from memory and cannot claim complete accuracy in dates and numbers. But the main facts can be substantiated by the evidence of others who took part during those 20 years.

II

A [THE ORIGIN AND PURPOSE OF THE 1919 GC&CS]

1. During the 1914-18 war cryptography was practised in two sections:
(a) *40 OB*, principally German naval, latterly a certain amount of diplomatic enemy and neutral, only using material obtained by interception of W/T by stations under Admiralty control, and
(b) *MI 1B*, principally German military and (currently) some neutral and later even Allied diplomatic, the raw material for the latter being obtained from Cable Censorship under War Office control. Only from 1917 was there any exchange between (a) and (b) and then principally of results.

2. Early in 1919 the Cabinet decided that the results obtained by these two sections justified the formation of a permanent section to keep alive the study of this work which had such an important effect on the prosecution of the war, both naval and military.

3. Admiral Sinclair (then DNI) was given the task of forming a section from the remnants of 40 OB and MI IB, to be established under the civil administration in the Admiralty. Negotiations between Admiralty, War Office and Treasury continued through spring and summer of 1919 and in November or December the new organisation was set up in Watergate House (staff details under B).

4. The present [1944] Ambassador to Peru (Courtenay Forbes), then in the Communications Department of the Foreign Office, invented the title Government Code and Cypher School.

5. The public function was 'to advise as to the security of codes and cyphers used by all Government departments and to assist in their provision'.

6. The secret directive was 'to study the methods of cypher communications used by foreign powers'.

7. Nothing in this constitution indicated how raw material was to be obtained. But DNI, being in charge, was able to retain a small party, both in the Admiralty and War Office, drawn from their rapidly diminishing war time intercepting stations. Pressure from DNI and others procured the inclusion in the New Official Secrets Act of a clause instructing all cable companies operating in UK to hand over for scrutiny copies of all cable traffic passing over their systems within 10 days of despatch or receipt.

8. Nothing in the constitution indicated that it was desirable that successful results of the study should be made available to government departments who might be interested, though in actual practice there was a circulation of 'unprocessed' decodes from the day of our birth, which has continued until today without interruption.

9. In 1921 the Geddes axe fell on us and we moved to Queen's Gate where we were more comfortable but rather remote from other departments. But we were nearer Melbury Road, and when the Admiral took over in 1923 he, as our founder, at once took steps to bring the two organisations into closer touch; this process culminated in 1925, when both moved to the third and fourth floors of Broadway Buildings.

10. About 1922 after two or three years' work and circulation in which results showed that *there was no service traffic ever worth circulating*, the late Lord Curzon, then Foreign Secretary, claimed that GC&CS was doing work solely for the Foreign Office and should therefore be transferred from the Admiralty to the Chief Clerk's Department of the Foreign Office for administrative purposes. The Admiralty, at that time in process of cutting down, willingly assented and thenceforward GC&CS estimates appeared in the Foreign Office vote.

11. It must be remembered that beyond a salary and accommodation vote GC&CS had no financial status; it became in fact an adopted child of the Foreign Office with no family rights, and the poor relation of the SIS, whose peacetime activities left little cash to spare.

* * *

III

B [ESTABLISHMENT OF GC&CS UNDER TREASURY CONTROL]

1. GC&CS began with a sanctioned establishment of 25 pensionable officers as follows:

1 head
6 senior assistants
18 junior assistants

A clerical staff (unpensionable) was also sanctioned, amounting to approximately:

6 typists
12 clerks (for code construction)
10 traffic sorters and slipreaders

2. The pay of the senior staff was based on that of the Administrative Class in the Civil Service, that is:

senior assistants = principals
junior assistants = assistant principals

In due course members of our staff were considered to be eligible for membership of the Association of First Division Civil Servants as are the senior staff in the museums, but there has never been any question of precise equality of pay.

3. On the other hand, when we had to recruit new staff through the Civil Service Commission our candidates did not have to sit for the Administrative Class examination but were selected on interview and record by the Committee of the Commission in which GC&CS was represented.

4. The original selection in 1919 for all classes was made from volunteers who had served in the Admiralty or War Office. Where the needs of the work required special qualifications such as Japanese (Mr Hobart-Hampden) or a highly experienced but already elderly man (Mr Fetterlein) who could not be made pensionable, they were granted equal pay with the others and blocked posts in the establishment. The Chief Clerk had difficulty more than once in explaining to the PAC why two very senior ex-Foreign Office officials were now graded as junior assistants of the GC&CS.

5. In 1925 when we first recruited young staff direct from the university, the establishment was increased to 10 seniors and 20 juniors. But promotion was slow. Naturally there was little or no difference in the work of good juniors and seniors. Therefore during the early 1930s the proportion was altered to 15 seniors and 15 juniors.

6. But promotion was still too slow, principally because no seniors died nor were superannuated. Therefore in 1937 the Treasury agreed to promotion of junior to senior after 10 years' service and the scales were slightly altered and fixed at:

junior assistants £250 - 25 - £500
senior assistants £700 - 30 - £1,000
chief assistants £1,000 - £1,100

while the head and deputy head were given the position and pay of assistant secretaries.

7. The above paragraphs (B, 1-6) have concerned the civil staff established under the Foreign Office. It might be fitting now briefly to account for the contribution made by the Services (Admiralty, War Office and [later] Air Ministry).

8. Their main effort was in the interception of foreign government W/T messages, a subject outside the scope of this paper. But the Admiralty and the War Office did make some staff contribution to the GC&CS until the time when the War Office and Air Ministry did maintain their own section within the framework of GC&CS.

9. From 1923 onwards the Admiralty evinced special interest in the Japanese diplomatic and naval attaché traffic and always provided one officer (Japanese interpreter) to work in the section. When a small party in the Far East was being formed, a system of rotation arose. Ultimately when in 1934 Admiralty started a bureau in Hongkong, sufficient officers had been trained to man it and Paymaster-Captain Shaw (then retired) was taken on the Foreign Office Establishment to act as the first head of the bureau. Further Admiralty assistance in the matter of staff is described in part C.

But the Admiralty, unlike the other two services, never maintained their own section in GC&CS.

10. The War Office, at the time of the Armistice, had in addition to MI IB, certain small sections overseas of which the one in Constantinople continued to function after 1918 until its staff were transferred (about 1922) to form the original nucleus of the War Office station at Sarafand which still exists today as an intercepting and crypto-graphic unit dealing almost entirely with local problems. A close liaison between GC&CS and Sarafand has always been a satisfactory feature. During the twenties the War Office did send military officers to GC&CS for some training before proceeding abroad. Among others, Captain Tiltman, spent some months in 1920 at Watergate House on

his way to the Middle East. But it was not until the early troublous thirties that Captain Tiltman, having returned from a long tour of duty in India, rejoined us, and before long started, himself as a civilian under the War Office, the Military Section to which were attached an increasing number of military officers. Their activities will be described more fully in [part] C.

11. For at least 15 years of our life the Air Ministry, while considerably interested in some of our results, contented themselves with the provision of valuable intercepting facilities. But about 1936 their Intelligence authorities felt the need of a technical expert of their own. They therefore set up the RAF Section within the framework of GC&CS and Mr J.E.S. Cooper was transferred from the Foreign Office to the Air Ministry civil establishment. The early development of this section will also be dealt with more fully in [part] C.

12. During 1937 the Admiral, convinced of the inevitability of war, gave instructions for the earmarking of the right type of recruit to reinforce GC&CS immediately on the outbreak of war.

Through the Chief Clerk's Department we obtained Treasury sanction for 56 seniors, men or women, with the right background and training (salary £600 a year) and 30 girls with a graduate's knowledge of at least two of the languages required (£3 a week).

To obtain such men and women I got in touch with all the universities. It was naturally at that time impossible to give details of the work, nor was it always advisable to insist too much in these circles on the imminence of war.

At certain universities, however, there were men now in senior positions who had worked in our ranks during 1914-18. These men knew the type required. Thus it fell out that our most successful recruiting occurred from these universities. During 1937 and 1938 we were able to arrange a series of courses to which we invited our recruits to give them even a dim idea of what would be required of them. This enabled our recruits to know the type of man and mind best fitted and they in turn could and did earmark, if only mentally, further suitable candidates. These men joined up in September 1939.

Thus very early in the war GC&CS had collected a large body of suitable men and women quite apart from recruitment of service personnel by the two service sections, of which the Military was now on an entirely military footing.

13. With regard to the clerical and typing staff which grew gradually during those years, involving us in prolonged discussions with the Treasury, the Tomlin Civil Service Commission of 1929 widened the basis of establishment, consequently we did obtain sanction for the establishment of two higher clerical, some six to ten clerical officers, about a dozen clerical assistants and half a dozen typists.

By this means we were able to retain with prospects of pension some of those girls and women who had proved their value to us in both our functions.

* * *

IV

TOP SECRET

C [DEVELOPMENT 1919-1939]

1. In A.5 I stated that the ostensible function of GC&CS was 'to advise as to the security of codes and cyphers used by all government departments and to assist in their provision'.

This duty was carried out exclusively by Travis who came to us fresh from this type of work in the Admiralty, together with a clerical party whom he had trained. He alone is in a position to tell the story of its development.

Suffice it to say that each of the big departments nominated officers in the Communications Branch to act in liaison with us. The Admiralty alone appointed an officer to work in GC&CS (later increased to two officers). Out of this has now grown the section known as CSA with far wider responsibility and power.

2. The secret side of GC&CS had as its task 'to study communications of foreign governments'.

The development of this work I propose to outline under the headings Diplomatic, Clandestine, Services and Commercial in the order of their appearance as vital issues during the period 1919-1939.

3. *Diplomatic*

As stated in A, 1 and 2, some diplomatic work was undertaken in both sections during the 1914-18 war. But it must be emphasised that this work was from a cryptographer's standpoint most elementary. Of the countries then tackled and read, only the German Foreign Office was using 'hat' books and reciphering methods: all the others read had an alphabetical basis. Sir George Young invented a method of reading German hat books (for which he received a monetary reward) which included an elaborate card index manned by some ten graduate women. Within a year of the start of GC&CS, the solution of a hat book was the task of one good linguist working on the method used Mr Fetterlein for many years in this work in Russia. I myself, working with Young, also received a monetary reward for solving the first additive key we had ever seen as used by the Germans. When I say that this key varied from 7-13 digits, I must consider myself lucky to have been rewarded for a job which nowadays any young cryptographer would take in his stride.

Fetterlein's previous training enabled us to read the fairly complex Austrian keys and rebuild their hatted books.

It might perhaps be noted here that I took a small Admiralty party over to Paris, in April 1919, to work with the French on the *German* material passing during the Peace Conference. We remained until the signing of the Peace of Versailles and I have always thought that our visit was useless though pleasant. Although Germany was a beaten nation, nothing appeared in the terms of Armistice concerning their diplomatic cyphers. Consequently their mission came to Paris provided with entirely new books and methods. We obtained all the traffic between Paris and Berlin but failed to produce anything of any value. How could we? Germany knew well we had read her diplomatic traffic for the last three years (e.g. Zimmerman Letter), and no one prevented Germany from replacing her compromised codes by the safest methods she could devise. I believe that at that time Germany made use of OTP for the first time. I am certain she used the method ultimately solved in 1942 and then only thanks to an amazing scrap of physical compromise. In any case there was no GC&CS at that date and such was the lack of co-ordination that the party in Paris never saw results obtained in London of American and Japanese work, while French and Italian had then never been attempted.

All other powers which were read in wartime, including American, Japanese, Greek, Spanish and Scandinavian, were using alphabetical books. Norwegian was alphabetical; the first Danish and Swedish solved were hatted but some 'cribs' were available.

Thus it came about that in 1919 only those who had worked on the enemy countries, who were driven to recyphering processes, had had any real experience in cryptography. The majority of the party were linguists. Ultimately the reconstruction of code books used and the translation and emendation of the resultant texts was our productive function. Fetterlein, Strachey and Knox were our original key men while Turner had the role of master-linguist with Hobart-Hampden in charge of Japanese.

The first effort of the early years was devoted to breaking into the hitherto untouched material from various governments.

a. The Americans celebrated the advent of peace by introducing a new hatted diplomatic code recyphered with tables changing quarterly. The solution of the first of these tables was a year's work and thereafter the American Section had to be expanded for the increased task of breaking the tables and reconstructing the code. Good progress was made, and the section was able to be of some assistance during the Washington Naval Conference in 1922.

b. The second really big task was to make a concentrated attack on French diplomatic cyphers, which had received no attention during the war.

A large number of hatted books of 10,000 groups were used and with the constant practice of reconstruction of such books they never presented any difficulty. Given sufficient traffic, legibility appeared within a month of birth.

Many recyphered books also appeared and after the initial struggle to obtain the general system, the constant change of tables presented little difficulty. Only about 1935 did the French introduce any system which defied solution. This was a development of the bigrammatic substitution and it was felt that even this would not be insoluble if only there were enough traffic. The Quai d'Orsay is conservative and we never observed anything of the OTP type.

The reading of this traffic during the years of peace and intrigue did from time to time produce very interesting if not invaluable intelligence. But the proximity of the two capitals did mean that a great deal passed by bag.

c. The only real operational intelligence came from our work on the Soviet traffic. We were able to attack their systems step by step with success from the days of Litvinov's first visit to Copenhagen, of Kamenev as their first representative in London followed by Krassin, until the famous Arcos Raid in 1927 (?) when HMG found it necessary to compromise our work beyond any question. From that time the Soviet government introduced OTP for their diplomatic and commercial traffic to all capitals where they had diplomatic representatives.

The revolutionary government in 1919 had no codes and did not risk using the Czarist codes which they must have inherited. They began with simple transposition of plain Russian and gradually developed systems of increasing difficulty. The presence of Fetterlein as a senior member of the staff and two very competent girls, refugees from Russia, with a perfect knowledge of the language, who subsequently became permanent members of the staff, enabled us to succeed in this work. We were also able to borrow certain British Consuls who could not return to Russia.

d. The fourth big productive effort was on the Japanese. Here the cryptographic task was for the first ten years almost non-existent so far as diplomatic work was concerned. For the language, which was the main difficulty, we were lucky enough to have recruited Hobart-Hampden just retired from 30 years' service in the East. But for a long time he was virtually alone, but with his knowledge of the habits of the Japanese he soon acquired an uncanny skill

in never missing the important. Probably not more than 20 per cent of the traffic received was circulated, but throughout the period down to 1931 no big conference was held in Washington, London or Geneva in which he did not contribute all the views of the Japanese government and of their too verbose representatives. Sir Harold Parlett, another distinguished officer from the Japanese service, joined him in 1926 and ably seconded him with an equal sense of the essential. Yardley's 'Black Chamber' tells of the American success at the Washington Conference. No one will ever tell how much accurate and reliable information was made available to our Foreign Office and Service Departments during those critical years.

Of the building up of the Japanese naval work, in which both these officers played a part, I will be speaking briefly later.

e. A continued watch was kept on the ex-enemy countries, but here there was little development. Germany was allowed to introduce her new methods, and we soon knew that she was using OTP for all she wished to keep secret. In course of time we knew her method of using pads and how she made them up. We also knew of her second method and diagnosed it as unbreakable.

This second method, nicknamed Floradora, was finally broken in 1942 thanks to three chances:

1. The basic book fell into our hands;
2. Close co-operation with USA;
3. SS work by an able ally who obtained first-hand information and one page of figures from a German cypher officer.

We had in fact reconstructed the basic book during the period 1932-39, but the effort was never profitable as German security rules forbade its use unrecyphered, except for purely administrative telegrams which proved of little interest or value.

The Austrian government had always used reasonably secure methods of recypherment and never used their books plain. Thanks to assistance from Fetterlein we did read them in 1918 and 1919, as there was sufficient traffic. But Trianon produced a small poor country whose communications grew less and less, and ultimately we failed for lack of telegrams.

Austria, Hungary, and the Balkan countries rarely produced sufficient material to justify an attack. The greater part of their telegrams probably passed on the continental landlines which were never available to use in peace.

Hungarian was successfully tackled by Knox, but it is doubtful if the results obtained at that time justified the enormous effort on his part.

Later an increase in the use of W/T and the troublous political situation did enable us to read some of the traffic of these countries but never have we been able to report full legibility, a regular flow of traffic and valuable results.

f. Some of the other powers had already been started in MI 1B or 40 OB, notably Greek, Spanish, Italian, Scandinavian and Persian and where purely alphabetical books were used, telegrams had been read and circulated.

Sections were therefore formed in the new GC&CS to carry on this work. Early in our career the Foreign Office disclaimed any interest in Scandinavian, so this subject was dropped.

Passage of time and changes in the political situation opened up new lines. The various South American republics, Portuguese, Brazilian, were tackled. The Balkans were watched, though little traffic was available as European landlines carried most of it. A Near East Section was envisaged, working in close co-operation with the military station at Sarafand, of which I will write later.

To sum up the cryptographic effort of 20 years on diplomatic traffic: we started in 1919 at the period of bow-and-arrow methods, i.e., alphabetic books; we followed the various developments of security measures adopted in every country; we reached 1939 with a full knowledge of all the methods evolved, and with the ability to read all diplomatic communications of all powers except those which had been forced, like Germany and Russia, to adopt OTP.

The authority who sanctioned our establishment in 1919 clearly never envisaged a complete reading, translation and issue of every telegram received by us.

Such was a physical impossibility for the 30 specialists who composed the main body of the staff employed on the work.

Hence from the outset sections did exercise their own discretion as to what they translated and submitted for circulation. They got guidance from the D and R who in turn received intelligence directives from the Foreign Office, the circulating sections of SIS and the officers who used our material in the Service and other large departments.

During the thirties we did supplement our daily issue by a daily 'Summary of telegrams decoded but not circulated', for the benefit of SIS, Admiralty and War Office (occasionally the Foreign Office) and it is noteworthy that it was only a very small percentage that were ever asked for in complete form.

With personal satisfaction I maintain that GC&CS did during those 20 years fulfil its allotted function with success, with exiguous numbers and with an absence of publicity which greatly enhanced the value of its work.

4. *Clandestine*

Peacetime GC&CS did have one experience of successful work on clandestine traffic. This, unlike the diplomatic, necessitated close cooperation between interception, T/A and cryptography before the final results were made available only to a small select intelligence section of SIS.

Some time around 1930 our stations picked up a mass of unusual and unknown transmissions, all in cypher except for the 'operators' chat', which was all of the international amateur type. The analysis of this traffic was studied closely, and from it emerged a worldwide network of clandestine stations controlled by a station near Moscow. It turned out to be the Comintern network. Brigadier Tiltman has written up the story of the cryptography attack which met with complete success. Control of interception, including D/F, was left to Kenworthy and Lambert, and their successful effort to locate a room in a house in a terrace in a suburb of London was perhaps the earliest example of this type of work, and proved in the early days the value of co-operation between interception, T/A and cryptography.

I can imagine that there was a considerable amount of clandestine wireless from 1935 onwards, during the Abyssinian and Spanish wars, and various episodes of Hitler's aggression, but lack of technical facilities prevented any attempt at interception.

One other clandestine network was observed and studied by us in the prewar days, namely that organised by the German Foreign Office. As we were aware that already our own Foreign Office and SIS were taking steps to ensure communications with our embassies and posts abroad in the event of a breakdown of the normal routes, we were not surprised when Denmark Hill in 1937 and 1938 obtained obvious German diplomatic traffic broadcast from an unlisted station in Germany to unknown recipient call-signs as well as obvious replies from unknown stations.

As previously stated, we could not read the traffic, but it could not be mistaken:

it was not disguised. Interception, T/A and direction finding enabled us, even in those days, to be certain that every German embassy and legation and many German consulates were equipped with W/T gear for reception and transmission. Denmark Hill was able to make preliminary studies of all the methods of changing frequencies, call-signs, etc, used to disguise as far as possible the originators and the services, so as to avoid interception and identification. When later during the war it became necessary to obtain all this material, these early studies by Denmark Hill proved of very great help.

5. *Services*

GC&CS, as an office, had no means of obtaining W/T traffic. Admiralty and War Office had set up a large number of intercepting stations during the war, from which DNI (Admiral Sinclair) persuaded the Signal Department to retain two, Scarborough and Pembroke, and the Military Directorate in the War Office to retain one at Chatham. Naturally the first duty of these stations was to watch the service traffic of other powers, but they also undertook to spend part of their time watching the big commercial transmitters in foreign countries with a view to obtaining such government cypher traffic as they heard. I propose to go more fully into this question in section D. But it had to be mentioned here as one reason for the creation of a Naval Section.

Admiralty. The beginning of the Naval Section is obscure in my memory. Clarke, who became the head of the section, did not join until 1921 as he was engaged in writing up the naval history of the Great War. But the Admiralty did lend certain officers, first German, then Italian linguists. There was of course very little German naval material in the early years: there was no German navy to speak of. There was a small amount, but it was soon apparent that we could not read it. The Armistice Commission and the Peace Treaty had made no demands. So far as I remember we concluded that a machine recypher had been applied to the 4-letter code book with which the German navy finished the war, but at that time we knew nothing of the German development of the Enigma machine. It is possible that in 1923-25 they were already using it.

In any case there was no navy, and consequently little traffic, and so interception was dropped.

The Italian navy was also watched, and here we were lucky. There was a navy and consequently a fair amount of traffic, and in early days we did reconstruct the main naval code book because of the delightful Italian habit of encyphering long political leaders from the daily press. As can be imagined in those years and with such habits, the Intelligence value of the effort was slight, but we did build a foundation which proved of value from 1934 onwards.

But even in the early twenties the Admiralty did evince an interest in Japan. But GC&CS only obtained diplomatic and attaché material - no Japanese naval traffic could be intercepted in this country. We knew the Japanese cryptographic methods to be low-grade - the language was the difficulty and linguists were hard to find. The Admiralty, however, had a certain number of interpreters, some of whom were for one reason or another no longer essential for active service. From 1922 onwards we had always one naval officer working in the Japanese Section, reading the diplomatic and naval attaché telegrams. By 1925 we even had officers still on the active list and a scheme was arranged whereby such came to us for two years and then joined the China Squadron in a ship where there were facilities for local interception. Thus a first start was made on Japanese naval traffic.

From then onwards there was a flow of traffic by bag to London where the various codes were segregated and broken as far as possible, and a return flow of officers with skeleton books to carry on the work locally. I believe that by 1930 they were able to be of definite use to the C-in-C, China. Finally the Admiralty sent out Captain Tail (then DDNI) to study the Far East question, and in consequence of his report, set up a small bureau for interception and cryptography at Hongkong (moved to Singapore in September 1939) where Captain Shaw, now retired, headed the first party to exploit Japanese naval signals, to which was added the beginning of Japanese military. The Diplomatic Section had followed the diplomatic and attaché developments, including the introduction of mechanical devices, successfully, and thus it can be maintained that in early 1939, GC&CS had full control of diplomatic and attaché traffic, were reasonably fluent in their reading of all the main naval cyphers and knew quite a lot about Japanese army cyphers as used in China.

To revert to European affairs, the period of dull slackness of naval affairs and traffic, noted in the opening paragraphs of this section, continued with slight alarms and excursions consequent upon naval reviews and visits until around about 1934, when the Italian governments probably began to plan the Abyssinian Campaign. From then onwards, Italian naval traffic was obtained in increasing quantity with increased security measures. The section kept pace with it all, though by 1935 increased numbers and more room had to be provided. Throughout the campaign and in the tenser moments aroused by the threat of sanctions, the section was able to keep DNI fully informed of the strength and activities of the Italian navy. When in the Spanish war the Italians, not content with their own reasonably secure hand methods, introduced the commercial Enigma machine for all their secret naval communications, this proved a heaven-sent opportunity for us to explore machine encypherment. Knox led the party and younger men, such as Bodsworth and Twinn, had their first experience with him, a fact which proved invaluable after 1939.

It was not until the summer of 1936 that any interest was taken in the German navy. But when they appeared that year in the Mediterranean, all our stations were inundated with frequent repetitions of their naval broadcasts. Work began at once under Knox and by this time we were quite aware that the Enigma machine, with the special attachment known as the 'Stecker', was the basis of their service signals. Strong efforts were also made by our naval stations to supplement the broadcasts by ship signals and local coast stations in Germany to try to find lower grade traffic. Lack of gear and men prevented this. Knox made considerable progress in his diagnosis until April 1937, when the Germans introduced the new method of indication [4 bigrams] to which he had to admit defeat. Captures in the spring of 1940 showed the correctness of this diagnosis. In 1937 we had no access to mechanical devices which alone enabled this system of indication to be overcome.

But correct diagnosis does not read messages, so the German naval signals were submitted to another process which we called W/T from which we hoped to learn something of German naval activities. Even in the Great War during 1917 and 1918, when new books were introduced and the cryptographers of 40 OB were not in production, the 'plotting' section, with the unread signals before them, did continue to produce daily a reasonably accurate situation report. But no German naval signals had been read for 20 years, and it was hardly to be hoped that the Nazi German navy had preserved the habits and routines of the imperial navy. Nevertheless, from 1937 onwards, such an effort was made by officers lent to GC&CS by the Admiralty, reinforced by available members of GC&CS. We had no accurate checks by the cyphers becoming legible; but out of this effort grew the art now called, I think, T/A, which from 1940 onwards has proved a most valuable adjunct to cryptography, quite capable of acting as a trustworthy substitute when the cryptographer is temporarily unproductive.

To sum up the situation of the Naval Section in 1939, including the Japanese branch in Hongkong: they exercised a very fair measure of control of all Italian and Japanese naval cyphers; they had only seen German signals by the Enigma machine and this they could not read; they had started an intensive professional study of raw German traffic with a view to extracting any available intelligence.

Military. Unlike the NID, MI *1 always maintained a personal interest, not only in interception and result but also in cryptography.* Before there was any question of a Military Section, officers were sent to us with the definite object of training, while the Admiralty lent officers to assist us in producing results. As stated above, the War Office had, during the war, maintained posts abroad,

and early in the twenties decided to set up a permanent intercepting station in the Middle East, and about 1923 Sarafand in Palestine was selected and started to function. In addition to interception, they also intended to read the traffic which affected the area. Therefore at Sarafand Arabic was a primary concern, while French and later Italian were also exploited. I visited there in 1925 and am glad to think that the liaison between GC&CS and Sarafand has been maintained for 20 years. Many army officers worked in both places. MI 1 was also our liaison with a bureau which the Indian army had founded during the war to handle the problems (Persian, Afghan, Russian) which affected India.

Throughout the twenties the military officers who joined us went to sections where their language was used or in which the War Office was interested, because there was *no purely military* traffic. But very early in the thirties the War Office decided to regularise this somewhat haphazard form of training, and the Military Section was formed to which all army officers with us were attached. Tiltman was made the head of the section, receiving the position of senior assistant on the War Office civil establishment. Members of the Military Section conformed to the routine and discipline of the GC&CS, but MI 1 had the right to dictate their requirements as to training and type of work. At a later date the War Office also recruited civilians on the same lines as GC&CS. Thus was laid the foundation of the very large Military Wing of the war period. Originally the Military Section took over certain of the normal commitments of GC&CS, but with the increasing threat of war, gradually the subject and the traffic on which the sections worked became more definitely military. The Far East began to send back bags of Japanese military material, the Japanese military attachés in Europe began to assume importance. Then the Abyssinian and Spanish wars produced large quantities of Italian military material. All of this latter was tackled successfully, and consequently the section became well trained to face their operational task in 1940.

Naturally the Military Section worked in close co-operation with the military intercepting station at Chatham, and it was thanks to this that the section, and GC&CS as a whole, had, in 1937, their first glimpse of German army and air force material, and of German police transmissions. Knox failed in his effort on the naval enigma, led the team which started to investigate this new problem. Tiltman, deep in other problems, broke in to contribute one vital link. An ever closer liaison with the French, and through them with the Poles, stimulated the attack. Fresh ideas flowed, even from those selected from a university as recruits in the event of war. *I think it may be rightly held that this effort of 1938 and 1939 enabled the party at B/P to read the current traffic of the GAF within five months of the outbreak of war.*

RAF Section The Air Ministry had, since 1922, contributed to our need for traffic by maintaining a very good intercepting station at Waddington. There was no real air traffic, so we profited. As the Intelligence Division of the Air Ministry was never so politically minded as in the other two services, our diplomatic result could not have had the same value to them.

Our debt to them was therefore the larger. But with the threat of war, about 1935 the Air Ministry decided to form an Air Section to work in GC&CS on the lines of the Military Section. They had no trained experts of their own. They asked, therefore, to have a member of GC&CS transferred to their civil establishment. So Cooper became the first head of the RAF Section and I am sure that the Air Ministry will agree that GC&CS repaid their earlier debt to the full, and with interest. In 1938 further civilians were recruited direct into the section.

From then onwards, Cheadle, whither Waddington had transferred, began to look out for foreign air traffic.

The war in Spain and aggression in Europe gave them ample scope. Italians, Spanish and German operational air-to-ground was collected and worked on with success. So the section had first-hand knowledge of some of the methods used by the Germans when war began.

6 *Commercial*

For 20 years, during which cable companies submitted all their traffic to the GC&CS, a vast number of telegrams of a purely commercial nature were seen but never copied. Similarly, the operators at the intercepting stations had to hear and pass over far more than they recorded. We only worked on foreign government traffic. Once or twice perhaps we may have looked out for individuals. Once most certainly we did investigate the telegrams of certain oil companies. But this was not our function. In those days of peace, all companies of any repute had their private codes or at least private encypherments of standard commercial codes. Apart from secrecy, it is cheaper to use code for telegrams. The majority of these commercial codes can be purchased in the open market, whatever their nationality. Therefore the reading of such telegrams presents no difficulty, and where encyphered, GC&CS should be able to break it down.

But with the few exceptions noted above, commercial work was not in our mandate and we had not the necessary staff.

Sometime in 1938 the Admiral and the newly appointed DNI formed that

opinion that in the events of a troublous political situation in the Far East, the Japanese might take steps to render their diplomatic and service material illegible, and that the communications of the big Japanese firms, particularly as to shipping, might be the only available source of intelligence.

Further, Major Desmond Morton had now organised a section known as IIC for the study of commercial and financial intelligence out of which grew MEW in the latter half of 1939. He was on our circulating list and was always anxious to extend the bases of his intelligence.

Therefore, in 1938, Hope started a very small section to investigate commercial traffic, more especially the telegrams of the big Japanese firms. A library of all the known commercial codes in various languages was assembled as a necessary foundation. But his task was definitely cryptographic.

About this time the Cable Censorship were engaged in drafting their final plans. They naturally intended to stop the use of code for all terminal traffic (except of course for neutral and allied governments whose representatives enjoy cipher privilege). Consequently the Censors themselves would circulate the intelligence derived from terminal plain language. But they did not propose to interfere with traffic transit at censorship points, and they agreed to provide our commercial section with all the commercial code telegrams of this nature. Our intercepting stations were now, in late 1938, asked to record commercial traffic where possible, and as much of this was taken on high speed automatic gear, our slipreading party had even then to be reinforced. The Commercial Section did have 12 months' experience of a variety of the codes used by all nations, including Japanese, and of the type and mass of plain language commercial telegrams. Above all they began to learn the very necessary discriminations. Never more than 10 per cent of the very large numbers of telegrams received really justified translation and circulation and *the accurate selection of this 16 per cent required training and close liaison with the users.*

V

SUPPLEMENT: TRAFFIC

The Cabinet authority establishing GC&CS gave no directive as to raw material, without which little could be done. But the authorities controlling the new body were fully alive to the necessity and supported to the best of their power all suggestions we put forward. We only had the experience of four years of war, when such a question was simple, because our results were valued.

Full cable censorship provided copies of all cable traffic. The development of the scientific methods of intercepting W/T traffic, service or commercial, dated only from 1914 but was now practised on a considerable scale by stations controlled by Admiralty, War Office and GPO. It was necessary to ensure that the provision both of cable and W/T traffic should continue under peace conditions.

1. *Cables*

The conclusion of the Treaty meant the suspension of censorship. Temporary unofficial arrangements were made with the moribund censors which provided the cable traffic for some further months. But legislation in the form of the Official Secrets Act gave the government the right to obtain cable traffic for scrutiny purposes *not* for censorship. A clause was inserted authorising a secretary of state to issue a warrant to cable companies operating in the UK requiring these companies to hand over all traffic passing over their systems in the UK within ten days of receipt or despatch to a named department, for the purpose of scrutiny, the secretary of state alleging that a general state of unrest and world emergency required him to make this demand.

I believe the Secretary of State for Home Affairs signed the original warrant and named the Admiralty. I believe occasional questions were asked in the House but we continued to receive all cable traffic from all the companies until September 1939, when cable censorship was again instituted, and once again the Censors provided us through the war with copies of the traffic we asked for.

Throughout the 20 years (1919-39) it was our aim to make this procedure work smoothly with the companies (British and foreign). It was undoubtedly a nuisance for them to have to send all their traffic in sacks to an outside department, and I have always considered that the credit for smooth working and no questioning should go to Maine. To carry out the work of sorting and

copying we took over a comparatively small body of GPO lower grade staff who were accustomed to this work. Our aim was to inconvenience the companies as little as possible, and throughout we tried to let them have their traffic back within 24 hours. *We only had to sort out and copy government traffic and occasional suspicious characters in whom our security authorities were interested.* I believe we never failed to return all the traffic, though many million telegrams must have passed through our hands.

Another very valuable job carried out by Maine was to obtain traffic from stations abroad where, during the war, there had been a censorship point, e.g. Malta, Hongkong, Bermuda. Traffic at these points was *not* required under the warrant.

Malta, above all, the focal point for traffic between Europe and all the East, was of the highest importance. Maine was able to arrange with Messrs Cable and Wireless, who operated the stations, that they should have all the slip transmitting Malta sent back by bag to London, ostensibly for accountancy purposes. We received it, engaged slipreaders, and had this valuable material read regularly, though of course with a considerable delay. For instance, the Japanese traffic to France and Germany always went via Malta. All Italian cable traffic passed there. *Thus we were, throughout, enabled to watch the growth of the Axis combination.*

In a similar way we were able to watch other old censorship points and, finding the traffic of little value, to give them up again.

It is probable that once again after this war, Malta traffic will be essential.

Also, with the CTO, Maine's excellent liaison proved of the greatest help at times when foreign embassies during big conferences requested and obtained private lines from their embassy to their capital. The Germans, the French and other great powers adopted this procedure on occasions. Of course these private lines had to pass through the CTO, and Maine was always able to arrange for measures to be taken there whereby copies became available to us.

Finally, when the state of unrest in the world became intense, from 1935 onwards, it was found that the 10 days' delay granted by the warrant became intolerable. Maine was able to cut it down to 24-48 hours in the case of foreign companies, and to instant service, where necessary, in the case of the CTO and Cable and Wireless.

Between us and the companies there has never been any question as to why we wanted the traffic and what we did with it. The warrant merely said scrutiny, and the traffic arrived back apparently untouched within a few hours. I have no doubt that the managers and senior officials must have guessed the true answer, but I have never heard of any indiscretions through all these years with so many people involved.

In short, barring the delay, we always had as good service of cables when we dealt direct with the companies as in the periods of censorship.

2. *W/T*

We started the peace regime with two Admiralty stations, Pembroke and Scarborough, gradually decreasing their naval work owing to absence of targets and increasing their watch of the big foreign commercial stations, and thereby producing foreign government cipher traffic, and (in the early days) a good deal of foreign government P/L, especially from Moscow.

Our director was at that time the DNI, Admiral Sinclair, who was obviously able to obtain the willing assistance of the Signal Department who owned the stations and the gear, and of ACR who provided the operators. Further, a Cabinet committee for postwar planning with General Romer as chairman had apparently planned for further interception and had appointed Admiral Sinclair as Co-ordinator of W/T interception. Before the Admiral left (in 1921) to take up the post of OC Submarines, naval interception by these stations was on a firm, if modest, footing, complicated only by the fact that ACR controlled the staff, DSD was responsible for station and sets, and DNI had to indicate the programme of work.

About this time (1921) the WO also set up a station at Chatham under MI IB, who were also prepared to produce material for us. The GSO2 or 3 of MI IB became a liaison officer to GC&CS, and we worked out a plan of interception with him. Later (about 1923,1 think) the Air Ministry joined up also and founded a station at Waddington under AII, who also nominated a liaison officer to us. So, when the Admiral returned in 1924 as Director, there did exist a means of co-ordination on a low level, that is, such sets and operators as existed were used to our best advantage but any expansion was out of the question. He resumed his function as Chairman of the Co-ordinating Committee and held an annual meeting of the Directors of Intelligence at which on each occasion the Head of GC&CS and the liaison officers assisted. At the early meetings little could be done beyond allotting priorities of work as still no expansion could be hoped for.

One of the first major actions the Admiral undertook was to arrange with the Police Commissioner for the loan of a small body of constables whom the Commissioner had used as a police W/T unit, I think, for interception of illicit transmissions in this country and for control of the police W/T network in London. These constables (10 to 12) had a small station at Denmark Hill, where their work was directed by a civilian engineer on the staff of the Receiver, Kenworthy by name. The Admiral undertook to pay for these men and the upkeep of the station while the Commissioner agreed to ask no questions about their work. This was the first station which undertook purely diplomatic work over which GC&CS had full control. *It was soon apparent that Kenworthy possessed a flair for this work which amounted to genius.* To him the FO and the Service intercepting authorities owe a very great debt, not only as a technical W/T engineer designing and constructing suitable gear, but also as the instructor in the matter of interception of difficult transmissions, and as a pioneer in the interception of non-Morse transmissions.

About 1929 the Admiralty began to take the Far East situation more seriously. The Committee of Co-ordination was able, not only to advise, but also to use the prestige of its members to force necessary expansion through the various departments. The Committee became known as the 'Y' Committee, and they formed a 'Y Sub-Committee', consisting of the head of GC&CS and the liaison officers. This sub-committee from then onwards met once a fortnight in the GC&CS. Its terms of reference were: to study the work of the various stations, to co-ordinate the programmes allotted, to avoid waste of effort and to investigate new lines of traffic and new means of transmission. Thus policy and expansion were the functions of the 'Y' Committee, while the sub-committee formed the executive, each member reporting if need be, to his own director.

This continued smoothly until about 1935. Certain other departments were asked to appoint liaison officers who sat on the sub-committee, notably the GPO with whom we had hitherto little contact, the chairman of the W/T board, and later Gambier Parry (then Captain) who had been appointed as Section VIII of SIS.

From the beginning of the Abyssinian war the sub-committee began to take a far more active part, and co-ordination of programmes became a more difficult problem, because there was now service material to be intercepted and new service sections to study the traffic. Consequently, fewer sets were now available for diplomatic traffic at a time when the contents were of more vital interest.

With the best will in the world, the service officers could hardly make a case for expansion on behalf of diplomatic traffic. It was possible for the Admiral to persuade the Commissioner to increase the staff at Denmark Hill, but with the increase of world unrest, it became clear that the FO would have to take its share in interception. Protracted negotiations resulted in success, but it was not until 11 September 1939 that the first station was opened at Sandridge. It had been planned and erected by the GPO. All the gear was designed and provided by the GPO engineering branch and the operators were all GPO staff. The FO footed the bill and GC&CS directed the various programmes of work. This very important development was one of the major actions of the sub-committee.

Another was the introduction of teleprinter links between the stations and GC&CS. Hitherto all traffic arrived by registered post creating an average delay of twelve hours. During the anxious days of the Spanish war it had become obvious that all delays must be cut down, and the service members were able to use the value of the results to induce their authorities to sanction the installation of the T/P links between GC&CS and the naval stations (Flowerdown and Scarborough), the WO station (Chatham) and the RAF station (Cheadle). *Of course, not only service material but also diplomatic was passed over these links. Thus we had two years' experience of rapid and efficient communication.*

In the spring of 1938 the Admiral bought the property at Bletchley Park, and the GPO set to work to equip it with suitable lines of communications. In the autumn of that year the service sections of GC&CS spent a month at the Park simulating, as far as possible, wartime conditions and direct communication. Thus it fell out that our work could definitely begin on 1 August 1939, when the Admiral ordered the service sections to take up their war stations. The diplomatic and commercial sections were ordered to move on 15 August.

From then onwards the university recruits began to join, so that by 1 September when war was declared, GC&CS was in action at its war station, already in process of growth towards that vast and successful body whose full story will perhaps never be told.

2 December 1944

CHAPTER SEVEN

How News was bought from Warsaw at the end of July 1939

My father always reported on his visits – to Scapa Flow in 1919, about Room 40, and GC&CS 1919-1942, about his Polish visit in 1939, about his American visits in 1941. His words speak for themselves.

Before attempting from memory a description of the visit of July 24-27 it is necessary to outline previous events which led up to the visit. The hero or mystery man or deus ex machina was undoubtedly the French officer Bertrand alias Godefroi. I never really grasped how G.C. & C.S. came to be involved in this liaison.

From 1937 onward it was obviously desirable that our Naval, Military and Air intelligence sources should get in very close touch with their French colleagues for political and military reasons. The Admiral had always wished and worked for a close liaison between S.S. and G.C. & C.S. but 1 had always thought that Dunderdale, then in Paris was the man who brought Bertrand into the English organisations. Menzies, it is true, had a close liaison with Rivet under whom Bertrand worked but I think it was Dunderdale who, entirely ignorant of the method of cryptographers, urged this liaison on the technical level. Bertrand was his man in the French military branch. The French had no interservice organisation. In fact they all four, (including Quai d'Orsay) thoroughly disliked and distrusted each other. Bertrand was no cryptographer and never pretended that he was. Any technical staff under him must have been very second rate but he had a genius for making use of others. By July 1939 he certainly was obtaining cryptographic results from us and from the Poles and he also salvaged five Spanish republicans who had worked at Barcelona and installed them in Paris as his party working on Spanish and Italian material.

Bertrand was, no doubt, inter alia a peddler and purchaser of foreign government codes and I think that as he never had an opportunity in his own

organisation of obtaining results from crypt, he had decided to concentrate on careful purchase as the surest method. I would say he did not have access to very much cash and frequently asked us to go 50-50 in a possible deal. We were averse to this as we already read most telegrams except the Russian and German neither of whom was among Bertrand's customers. But the Admiral thought that occasionally it was well spent money to keep in with Bertrand. He must have been useful to SIS in other ways and I well remember an official lunch in '38 or '39 at which Menzies presented Bertrand with a gold cigarette case engraved with the Royal Arms.

It should be noted as of some ultimate importance that in the course of some of his visits to us in Broadway we arranged for Bertrand to have conferences with certain sections such as the Spanish and Italian. He heard explanations of our methods and saw results and with the Admiral's permission received a regular supply of certain results.

I think he was impressed by our success and by the ability of certain officers and it might well be that this had an important bearing on his subsequent action.

The Spanish war had rekindled our interest in the German Enigma as, at last, we were intercepting a considerable volume of German Naval material and a little military or air traffic. Knox was working on the naval material with intermittent assistance from Foss. Tiltman was in the background but was really fully occupied with the military sections and the solution of the Japanese military ciphers. In addition to this *we had found that the Italian Navy were using the commercial Enigma*. This was cracked by Knox and a small section was formed with Bedworth in virtual charge to handle the current traffic leaving Knox clear for the German machine.

So far as I can remember this was the position in January 1939 when Bertrand asked me to come over to Paris as he wanted us to meet certain Polish experts. We assumed that such a meeting could only concern German and Russian work on both of-which we were so weak that we felt we might well profit by such a meeting. So I went over with (I think) Tiltman, Knox and Foss, We met in an atmosphere of secrecy and mystery. One of the Poles, a Major Ceski *(sic)*, gave us the alleged results of their research into the Enigma machine as used by the German services. He had no English and his French and German were only fair but it was clear that he was describing the results of his work on the 'message setting' which at that period appeared as the first group in all messages in all services. (It was only in May 39 that the German Navy adopted the bigrammatic indicator which Knox quickly diagnosed and found himself

forced to drop the Naval and concentrate on the Military/Air). The Pole gave us a prolonged and pedantic description of what Tiltman had spotted and learnt in an hour namely that the message setting was soluble because no letter could be ciphered by itself and the German operators were simple souls with childish habits. The Pole finished by saying they were obtaining a lot of material and pursuing their research and would keep us informed of any results. At that time we had to regard the meeting as a flop and that the Poles were no great find. Since then I have thought that it was our party who were being vetted by the Poles who were at that time reading the traffic and only wanted to know what progress we had made. Bertrand himself let it be understood on this occasion and always when the question was raised that he was himself ignorant of the ability of the Poles or of what they could read. He was aware, he said, that they obtained some results. Later he admitted that he had to visit Warsaw once a month at least to exchange raw material and results and further he considered them exceptionally well-placed to do 'business', as he understood it, with treacherous Germans and Russians.

For the next six months we heard nothing more from the Poles probably because they felt they did not require any help from us. In the middle of July however we received an invitation, through Bertrand, to pay them a visit in Warsaw. The international situation was now clear. England was pledged to go to the assistance of Poland if attacked by Hitler. Each party now knew that the other had an active cryptographic organisation. So it appeared quite natural that the Poles should invite us. But it must not be forgotten that the German Navy had changed in May. The Polish invitation specifically included Knox who was known both by the French and the Poles to be working on this subject. I do not think though now I cannot be sure that they were aware of our success on the commercial Enigma as used by the Italian Navy.

However the Admiral instructed me to take Knox with me. I could well wish now that I had added others of our party but everyone was fully occupied and could ill spare the time to travel to another flop as in January. D.N.I., in close touch with the Admiral, suggested that Sandwich should go also. Why I don't know as Sandwich was not a cryptographer and the Poles had so many. Bertrand was, of course, of the party. Knox and I went by train as we wished to see Germany probably for the last time, the other two separately by air. We left on the 24th and were met by the Poles and Bertrand and lodged at the Bristol. We were there for work on 26th and 27th and leaving on 28th. I was back in London by Sunday 30th. Knox, whose passport had been wrongly stamped for his return transit through Germany, had to go back from the frontier to Poznan and get the visa from the British Consul in that town. The 26 (Wednesday) was THE day. The Poles called for us at 7am and we

were driven out to a clearing in a forest about 20 kilometres from Warsaw. Here we found a new, strongly built and strongly guarded office with some underground accommodation and here we met the Polish cryptographers some of whom luckily spoke some French or German.

A prolonged full dress conference with the Polish senior officer in the chair (I have forgotten his name). Colonel Lange was in charge of the organisation in the forest. Major Ceski with the steckered Enigma now described in full detail the steps they had taken to break down the cypher and obtain the wheel order and to read the messages. We followed him each to the best of our ability. Knox, as our expert, was alongside Ceski and in the best position to follow his explanation. He, however, reacted very badly to the explanation which took about three hours with a break for a cup of tea. I confess I was unable to understand completely the lines of reasoning but when, as seemed part of the conference, we were taken down to an underground room full of electric equipment and introduced to the 'bombs' I did then grasp the results of their reasoning and their method of solving the daily key. Knox accompanied us throughout but maintained a stony silence and was obviously extremely angry about something. It was only when we got back into a car to drive away that he suddenly let himself go and, assuming that no one understood any English, raged and raved that they were lying to us now as in Paris. The whole thing was a fraud he kept on repeating. They never worked it out. They pinched it years ago and have followed developments as anyone could but they must have bought it or pinched it.

Our position became increasingly difficult as even Bertrand, who knew no English, was aware that Knox had a grudge against the Poles who, so far as Bertrand knew, had only been successful where Knox had failed. I assume that he did not believe that they had constructed the order on the wheels and he may have been correct in his surmise. Ceski's explanation was very lengthy and involved and in a language which he knew only fairly well and I was not competent to judge of the possibility of complete success. So far as I was concerned they were reading messages up to the previous May and were now quite sanguine as to the reading of current messages again by means of their 'bombs'. I have since thought that they were finding considerable difficulty especially with the naval and, knowing Knox's reputation and ability, felt it was a good moment to come clean and gain his assistance especially in view of the political situation.

The rest of that day remains a nightmare to me. Knox remained aloof and alone. Bertrand, Sandwich and I discussed the situation at length and decided to get away as soon as possible. The next day had been allotted to personal

contacts with their technical and intelligence officers, Knox had cooled down considerably and spent a long morning with their technical staff examining the machine and their methods. Language was of course still a difficulty but he now seemed to understand their reasoning and in his conversations with me never referred to his outburst after the disclosures.

I was shown the mass of telegrams they had read, the naval traffic being practically only between Berlin and their fleet in Spanish waters, which formed the bulk of their material. They undertook to send us copies and a model of the machine through Bertrand, as we, of course, had no line of communication with them. The machine did arrive during August but I doubt if any messages arrived. *As the situation was now clearly war and the service sections had already gone to Bletchley we were not interested in back material but were naturally concentrating on current air/army traffic.*

I should add that on that second day Knox was really his own bright self and won the hearts and admiration of the young men with whom he was in touch. If only that first day of disclosures could have been avoided and pompous declarations by senior officers had been omitted, Knox's mind and personality in touch with men who really knew their job would have made that visit a very real success. They were all simple and straightforward. To me Bertrand's attitude remains a mystery. I still believe that he knew all about their work and feigned the surprise which he manifested at the Polish success.

* * *

Two years later my father tried to explain to Knox the difference between information and intelligence!

11.11.41.

Dear Dilly,

Thank you for your letter. I am glad that you are frank and open with me. I know you disagree fundamentally as to how this show should be run but I am still convinced that my way is better than yours and likely to have wider and more effective results.

If you do design a super Rolls Royce that is no reason why you should yourself drive the thing up to the house of a possible buyer, more especially if you are not a very good driver. I lost any confidence you had in me when I disagreed with you in Dec. 1939 and said that you could not exploit your own success and run huts 6 and 3. I was right

- you broke new ground while the building in your foundation was carried on by Travis etc. who, I say, were better adapted to this process than you.

Your next big show was K. You alone among us found the way but the full value of <u>your</u> work could only be obtained by fitting results into the full picture in the Naval Section.

And now comes your latest effort which only proves again that you are the right man in the right place. You told me of a side-line in Intelligence that you wanted to develop. I agreed but begged you to remember your real metier. So you produced this result which none other of our party could have done.

You say you did it because you are a scholar who proceeds from his raw material to his finished text, well - who is preventing you - you have access to all past material and copies of all new.

What are my grocer's window dressing. Eric Smith offers all productions in neat form to those who need them. Birch ties up information from every naval source and tells the story. Hut 3 collects and reports accurate information derived from the source you invented.

Do you want to be the inventor and the car-driver? Do you want to be Eric Smith, Strachey, Birch and Wing-Commander Humphreys and De Grey wrapt into one which will include Knox who is the source? If so I don't agree and don't mind at all what steps you take.

You are Knox, a scholar with a European reputation, who knows more about the inside of a machine than anyone else. The exigencies of war need that latter gift of yours though few people are aware of it.

The exploitation of your results can be left to others so long as there are new fields for you to explore.

I do disagree with you.

Yours ever,

A. G. D.

AGD and ADK remained friends of this frank sort till Knox died in 1944.

CHAPTER EIGHT

Berkeley Street crypto activities in 1943

On 30 January 1942 my father admitted to his diary that he was no longer director of GC&CS but Deputy Director (C). This, coming after the acknowledged successes of 1941 was a heavy blow, but my father - though privately bitter - took it well. We left Bletchley for Ashtead, from where he commuted daily to Berkeley Street. At this point his diary and the official file remain silent for the next 15 months. All the family knew was that we now had a smaller car and my mother had to learn to cook. I was beginning my second year as a scholar at Westminster School, evacuated to the Hereford/Worcester borders, and my fees were accordingly paid by the bounty of previous Westminster benefactors. My sister, 18 months older, left school and went to a secretarial college.

My mind is a blank on those 15 months, but hindsight reminds us that they were the months which started so badly for Britain and ended, despite remaining unsolved problems, better. The fall of Singapore in February 1942 was traumatic even for a schoolboy. The war at sea was still being won on a monthly basis by Admiral Doenitz, but there were British successes in North Africa. Above all, we no longer stood alone - for Hitler had overreached himself in the summer of 1941 and invaded the Soviet Union, and by December the USA had joined the Allies after Japanese aggression at Pearl Harbor. We were still downhearted for Germany was still the strongest nation on earth and it was to be another two years before the Allies invaded mainland Europe at Normandy on 6 June 1944 and over another year before VE day.

Just over a year before, the files suddenly gave a detailed rundown, in May 1943, on my father's 200-strong operation on diplomatic and commercial signals intelligence in Berkeley Street and Park Lane. The McCormack report, released to the National Archives in Washington, is here reproduced in full. Some thriller readers may find it too circumstantial but I hope they will persevere.

Colonel McCormack (US army) to:

ARLINGTON HALL STATION*
MESSAGE CENTER

Date Filed May 21 1943
Time Filed 1212Z

Incoming Message
FROM: AMEMBASSY LONDON
TO: MILID WASHINGTON
NR; 4832

Denniston's show, commonly called Berkeley Street, has none of the hectic atmosphere of Park but rather gives impression of well established operation that goes along through wars and peace. General impression is typified by the two ladies who receive and sort incoming traffic. (They started as telegraph clerks in Post Office in reign of Queen Victoria and were fully familiar with general field when they joined present organisation in 1919.) These little birdlike old ladies receive and register all incoming material and they have acquired such great familiarity with it that can do everything except actually decipher it. Whole organization is very simple and they seem to accomplish a great deal with quite limited personnel. Whole outfit consists of two hundred.

TO STRONG FOR CLARK AND CORDERMAN FROM McCORMACK

38 bodies divided, subject to some doubling up, as follows:
Deputy Director and administrative staff – 5;
Distribution and reference section – 5
Sorting section – 2
Typing – 14
Teleprinter clerks – 2
Geographical sections – 155
Commercial section – 50
Research section 5

Geographical sections are divided into enemy countries, neutral countries and allies.

---

* Arlington Hall Station was the headquarters of the US Army's Signal Intelligence Service (SIS) cryptography activity during World War II

Personnel in enemy country sections are:
German - 26; Italian and Vatican -19; Japanese - 36; French (which now overlaps enemy and allied groups -14; Siamese - 1 (who in off moment doubles up on Irish); Bulgarian - 2; Roumanian and Hungarian - 1; Finnish is now being worked on in Research Section.

Neutral countries are divided up as follows:
Spanish – 6 bodies; Portugese - 10; Swiss – 4; Irish - (see above)
Latin America, Spanish language – 5; Near East (which covers Turkey, Saudi Arabia, Iraq, Iran, Afghanistan, Egypt, Palestine and Syria - 17
All Scandinavia is handled in off moments by Rees, who is Chief Administrative Officer.

Allied countries account for full time personnel of 11, of whom eight work on Chinese, two on Belgian and one on Greek. Dutch is done by people who work in Near East section, Brazilian by Portugese section, Polish, Jugoslav and Czeck by the man who handles, with a clerk assistant, Bulgarian material, and Mexican of course is done by Latin American section.

Taylor will report later on composition of commercial section subdivisions. Principal sources of material, other than by exchange with United States, are censorships at London, Ottawa, Mauritius, Barbados, Gibraltar and Middle East. (Where there are joint censorships at Cairo, Baghdad, Teheran and possibly elsewhere.) Foreign Office intercepts stations in United Kingdom (Denmark Hill, Sandridge, Saint Albans, Whitchurch, Cupar and Brora) and, through BP, other intercept stations at Ottawa, New Delhi, West Africa (recently discontinued), Melbourne, Cape Town, Simonstown, Suez, Malta and Mauritius. You will observe what extensive coverage this adds up to. Other source of material is secret intelligence service in neutral capitals. General outline of workings of outfit follows: sorting clerks route material to proper geographical section, where it is registered in appropriate book in which notations are made under following headings:

first serial number,
second cipher,
third signature,
fourth reference (that is, to cipher keys),
fifth subject (briefly indicated),
sixth remarks and distribution number (this is inserted if material is distributed, so that by looking at any page you can tell what has been distributed and what not),
seventh source (that is, intercept station or other point which it was picked up).

Traffic then goes to crypt people and if successfully processed results are passed to Head of Section, who sets aside what he thinks not important enough to give to anybody and sends the rest to distribution and reference section, which is heart of organization and which I will report on in more detail in another message. This section decides whether material is worth circulating and if so gives each item to be circulated its proper serial number and sends uncirculated items back to geographical sections for filing or destruction. Up to this point everything is done in longhand. Only what is going outside is typed up. Note that commercial material does not go to this section but processes along another routing which Taylor will describe.

Everything that is circulated goes to Foreign Office and Director, that is C, and except in very special cases everything goes to War Office and Admiralty (will have to check further what goes to Air Ministry). The very special cases that service ministries do not get are such cases as where material shows that some British diplomat abroad has 'dropped a brick'. Policy is to recognise that especially in time of war service ministries have their own views on matters of foreign policy and are entitled to be kept fully informed on all diplomatic developments. *In case of Berkeley Street as in case of Park, what impressed us was the pains that are taken to see that all information gets out to those who can make use of it.*

There are liaison officers from various governmental offices who are assigned to Berkeley Street and have access to its material, although this is not full time job and most of them are high personages. In this manner the following are directly represented in Berkeley Street operation:

C's office; BP; Winnie himself; Foreign Office; all three services; Ministry of Economic Warfare; Treasury; War Cabinet; Colonial office; Military Intelligence Five, which is counter espionage; India Office and Secret Intelligence Service, which is Charlie in another form but this last named liaison officer does not serve C but serves other branches of the government, including Board of Trade; Department of Overseas Trade; Petroleum Board; Home Office and Minister of War Transport. There is some form of liaison to everybody who might be able to act on information coming in.

Through BP liaison is maintained with Washington, New Delhi, Melbourne and African Force Headquarters. Please make following correction at beginning of message: Elderly ladies do not register and record all incoming material, but only material from certain sources, when there is some reason to keep such records in order to evaluate source or keep track of source for some

reason. At present they are keeping register of incoming traffic only from Mauritius, Port Sudan, Cairo, Gibraltar, Khartoum and Jerusalem. Khartoum is not mentioned above and I believe this is censorship point. Note however that complete register of all traffic by nationalities is kept by geographical sections.

ASNr 4191
Date Completed May 22 1943
Time Completed 20005Z

ARLINGTON HALL STATION
MESSAGE CENTER

Date Filed May 21 1943
Time Filed 1345Z

INCOMING MESSAGE
FROM: MX AMCEMBASSY LONDON
TO: MILID WASHINGTON
NR: 4834R

Records maintained at Berkeley Street do not include figures for total traffic and I did not ask them to go to geographical sections and add up all these figures, but they receive 'thousands' of messages per day. Their serial numbers of circulated diplomatic items crossed one hundred thousand early in 1942. Do not have present range of number.

TO: STRONG FOR CLARKE AND CORDERMAN
FROM McCORMACK

But monthly average has been running at from eight hundred to one thousand. Generally speaking I would say that their policy of what to distribute is same as Arlington's, the difference in numbers distributed being accounted for by fact Arlington covers wider field and that here they have been going for much longer and have learned over period of time what is new information and what is not; and they also have had much more guidance as to what to put through and what to discard than Arlington gets from its distributors, naturally in view of short time that operation has been going on present scale.

Basic principle is same however, namely, to distribute everything that might have any intelligence value, however small.

Great difference between BP operation and Berkeley Street is that BP is essentially an intelligence organization with important operational functions whereas Berkeley Street is production organization like Arlington. However they do seem to have the intelligence side of their operation, functioning as aid to crypt people, very well set up. It centers in the distribution and reference section, headed by Earnshaw Smith, a youngish looking man who nevertheless has been in this work since 1917. His assistant is Ore Jenkins, Professor of Medieval and Modern Greek at Cambridge, who has been in it since war started. They have three girls in theory but two in actuality, one of whom has been fourteen years at Berkeley Street and six years in this section.

The other has been in the section for five years. These people are in effect a reference bureau for crypt people, and in addition they determine what shall be circulated and to whom it shall go in cases of doubt, and they supervise mechanical operation of getting it out.

Nothing goes out by teletype, other than exceptional material for Chief, the four teletype connections being with BP, Chief's office and intercept stations at Denmark Hill and Sandridge. Earnshaw Smith's section has most simple filing system imaginable. Material is simply laid in folders in serial number order, unbound. There are three files - one is master file and another is spare file, both in straight serial number order. The third and important file is called 'Subject and Country' but in fact it is only country and not subject, since all material bearing on any particular country is laid in a folder in order of dates and there is no subdivision of country files by subjects. Most startling fact about this section is that it receives daily, shows to geographical sections where interesting to them and then puts in its files all incoming and outgoing communications of Foreign Office, Dominions Office, Colonial Office and India Office, and all but purely operational material of the three service ministries. More later.

ASNr 4194
Date Completed May 22 1943
Time Completed 1545Z

MOST SECRET.

13

TO BE KEPT UNDER LOCK AND KEY: NEVER TO BE REMOVED FROM THE OFFICE.

JAPANESE INTERPRETATION OF RENEWAL OF ANTI-COMINTERN PACT.

N.C.t. 100

No: 698360

Date: 30th November, 1941.

From: Foreign Minister, TOKYO.

To: Japanese Chargé, LONDON.

No: 2394 Circular.

Date: 25th November, 1941.

[In Chef de Mission cypher recyphered on the machine].

The prolongation of the validity of the Anti-Comintern Pact has probably attracted a good deal of attention, not only because six Powers signed the Protocol, but also because there was announced at the same time the adherence of CHINA, ROUMANIA, BULGARIA, SLOVAKIA, CROATIA, FINLAND and DENMARK. For our part, animated by a continued opposition to Communism, we did no more than prolong the period of validity of this Pact which was expiring, and this has no special political significance. Please make this clear to the Government of the country to which you are accredited if you find it necessary.

This means Nanking. Because.

This telegram is addressed to LONDON and WASHINGTON.

Foreign Secretary

Director (3).
F.O.(3).
P.I.D.
Admiralty.
War Office (3).
Air Ministry.
M.I.5.
Sir E.Bridges.

Fear!

Fear may not prevent, may even provoke, action. But it is a fact all the same.

WSC

PM 21

Intercepted cable from Japanese Foreign Minister to Japanese Embassy in London, dated 25 November, 1941. NB Churchill's annotated footnote: 'Fear! Fear may not prevent, may even provoke, action. But it is a fact all the same.'

Kim Philby at a press conference in 1955

AGD at his daughter's wedding in 1958

'D.G.' was Dorothy Gilliat, one of the five children of a successful Leeds businessman, Arthur Gilliat, himself the youngest of ten children. 'D' as she was known to her sisters, born in 1891, was the clever one and went up to read English at Lady Margaret Hall, Oxford. She was a beauty and had many admirers, most of whom died in the Great War. Her closest friend was my father's sister, Biddy Briggs. Through Biddy 'D' met my father. They were married in 1917. After the war, they lived in Chelsea, moved out of London to the outer suburbs because of my health in 1936, and lived near BP from 1939 till 1942. 'D', a linguist with good French and German and an excellent English writing style, worked as a watchkeeper at BP till my father's job required him to return to London. She was the soul of discretion, She sent a telegram in late 1957 to say she had a mammary tumour, from which she died a few months later. Her only obituary called her 'one of the quiet ones'. She was a wonderful mother. R.I.P.

ARLINGTON HALL STATION
MESSAGE CENTER

Date Filed May 22 1943
Time Filed 0920Z

INCOMING MESSAGE

FROM: AMCEMBASSY LONDON
TO: MILID WASHINGTON
NR: 4839

One of the most illuminating documents in Denniston's show is book showing net results of all British intercept activities in diplomatic field for second half of 1942. It consists of one sheet or set of sheets for each city in which traffic originated.
On each sheet:

The first column shows alphabetically the cities to which traffic was destined.

Column two further breaks down traffic for each city according to nationality, all subsequent columns following the breakdown of column two.

Columns three and four show by call signs the originating station and. station of destination.

TO: STRONG FOR CLARKE
FROM: McCORMACK

Column five shows station or stations which did Interception. Column six shows estimated number of messages sent. This is based on message numbers. In some cases exact number of messages is known; in others estimate is based on numbers intercepted up to late date in month; in others it may be guess based on small numbers of interceptions not running to end of month. In cases where senders do not number messages this column is left blank.

Column seven is number of messages intercepted

Column eight is number missed, being difference between column six and column seven, where six has been filled in.

Column nine is number of messages intercepted in cases of unnumbered series.

Column ten is the usual remarks. Remarks include information necessary to understand figures, such as note that traffic only started in June or that interception commenced in August or that diplomatic relations were broken in May and traffic discontinued. Remarks also include information to guide users of book, such as note that traffic is important and that further efforts should be made to get it, or that at actual places of interception it is hard to get legible copy, or that because only slow means of relaying are available it arrives too late to be used, etc.

Pages are thirteen plus by sixteen plus inches and triple spacing is used, leaving plenty of room for notes. Such a book would be of great use to us and over the past year if information of this kind had been available in this readily usable form it would have saved innumerable inquiries to Arlington and would have made answers to many inquiries more accurate. From such a book it is possible to take off totals of material by origin and destination, by nationalities etc, and *to see what intercept stations produce important material and in what volume, to determine at a glance what sources of information there are in each principal city and how many of them are being tapped and of course to see how much of each type of traffic is being brought in.*

Recommend that you and Corderman consider setting up this kind of a record and keeping it up month to month, which British are now starting to do.

It is impossible to exaggerate how many surprises you would get from looking at these records or how many subjects that we have discussed it would illuminate. To mention one, you will recall our discussion of possibility of stopping Axis traffic to and from Portugese African points. You may be surprised to learn that Portugal, which governs the colony, sent 122 messages to Lourenco Marques during second half of nineteen forty two whereas the Italian Embassy in Lisbon send 1295, and that figures in other direction are comparable. Had we had these figures in our mind at time of our discussion we would have seen this picture in very different light.

Pages for Tokyo give clear and extremely interesting picture of whole Japanese diplomatic communications picture. They reveal that 498 diplomatic circulars were intercepted out of 936 sent out, but unfortunately figures for interceptions does not in any instance include traffic received from United States and therefore that side of picture is incomplete.

Tokyo figures show that German communications to and from Berlin are much more numerous than Japanese (almost four times as large).

I cannot carry in mind all striking examples which I noted but one other is that Italian traffic to and from Bangkok is much larger than I had imagined and that much the largest item in Irish Government traffic was to and from Vichy. I give you these to illustrate how much information you can spot quicker from such a schedule and how useful it would be in various ways, including setting up of traffic priorities (Special Friedman System)

ASNr 4217
Date Completed May 25 1943
Time Completed 0145Z

ARLINGTON HALL STATION
MESSAGE CENTER

Date Filed May 22 1943
Time Filed 1620Z

INCOMING MESSAGE
FROM: AMCN EMBASSY LONDON
TO: MILID WASHINGTON
NR: 4847 Page #1

Japan Section of Berkeley Street is most impressive because of experience and ability of personnel. Traffic coming in is classified and registered by three girls who have had long experience and

TO STRONG FOR CLARKE FROM McCORMACK
is then passed to proper crypt people who number 14. Those who actually do crypt work at present are not prewar employees but have been in this work most of war.

One girl handles crypt side of purple while two men in middle thirties or thereabouts do all work of recovering JIC keys and are now complaining of lack of work. Head of Section was away when we visited and name escapes me.

One young man handles liaison with us and Australia and balance of section consists of decoders and clerks. This young man and two men handling JIG Nineteen keys are typical of selection methods here. Before war one was history teacher in public school, one was detective story writer and third was seller of odd books to American collectors. All were called up and all were selected for Intelligence Corps and after six months in Army sent to Tiltman's school. On finishing course they had privilege of taking commission or being returned to civil life in assignments in this work. Two took commissions and are now Captains, the third chose to serve as civilian. All wear civilian clothes.

You can see that these realistic British know that men working on JIG Nineteen are not really in Army and they do not have to pretend that they are unless they want to. JIG Translation Section is much higher form of animal life than Crypt Section and includes people who have done crypt work and might be doing JIG crypt now if it were not so easy. Head of Section is White, who at beginning of war was Consul General in Tientsin and had long service in Japan and China. All work coming from Crypt Section passes over his

desk and is examined by him or whoever is acting during his absences, in original language, and is marked with one to four symbols meaning high priority, priority, unimportant, or please look over to determine whether it is worth translating. High priorities must be translated at once, priorities must be translated when translators get around to them, unimportant ones are not translated. Result is that eighty per cent of color material and fifty percent of JIG Nineteen's are translated. Lousy Annie material is not normally translated. It is looked over in original language and watched for items referred to in higher class material, to circulars, for identifications OK persons etc, and in certain special cases, such as Kabul, where it has proved to be source of information, it is followed with more care.

This based upon study of Lousy Annie* material made last year.

Translation staff (working on DIP and not including those on Commercial) consists of retired Colonel (who was Military Attaché in JIG in twenties and has been in his present work since 1927, and seven civilians: Cunningham, formerly Consul in JIG, Roscoe, who was Consul in JIG during last war, thereafter lived and worked there and returned here for present work in nineteen thirty one after seventeen years of residence there, Hobart-Hampden who they say is probably world's leading JIG scholar and coeditor of Standard Dictionary recently reprinted in Washington, two recently retired Consuls, who were Consuls General at two JIG commercial cities, one Consul on active list, who when war started was serving at Taiwan and, finally, one Braithwaite, who was brought up in JIG, got his advance education there during last war, went into business and resided there up to present war. As White remarked, his section's standard of scholarship in JIG is very high.

We did not have chance to inspect closely the files of this section or aids used in its work. While general impression is of men steeped in knowledge of their special field, and who carry most of what they need in their heads, we did see a lot of dictionaries and reference books and two complete looking files, one of personal names and one of geographical names, the latter apparently considered very important in their work. They of course keep files of their own material, and I got impression that they more or less specialize, one man dealing with material relating to one part of world and another man another part, and that these men are not merely translators but are experts on the areas with which they deal, and that they are consulted by Foreign Office people for their opinions on information coming out or material.

* Los Angeles

All of which leads me to this suggestion: Arlington is plugging away at very difficult work which is largely for use of State Department: that Department must have JIG experts who are spending their time at much less important work than getting this JIG diplomatic material out when Army can very properly say that, with JAC material to handle, it cannot do State Department's job unless such people are furnished to handle DIP translation work.

This leads me to another thought: *when you get some idea of economic warfare picture that has been built up here from continental commercial material, by process of just getting every tiny item and putting them all together by most painstaking labor, you cannot fail to think that we ought to be doing same thing for areas involved in JIG material.* It would take many months of most intensive work to start building up picture, and no time ought to be lost in starting it, because at some point in this war important decisions in JIG area are going to be affected vitally by what we know and do not know about the details of economic matters in those areas.

Lord Farrar, who sits in Economic Warfare Ministry for purpose of handling most secret information in continental economic field and in fact for whole world, told us yesterday that 85% of all important information about South Central economic picture has been built up from Berkeley Street production, the contributions by censorship, foreign press, radio broadcasts and agents being trivial in comparison with our material.

There is evidence that people here, who already are reading and translating around a thousand JIG repeat JIG commercial items per day, are beginning to build up JIG economic picture.

Here is another case in which, unless we approach this problem with imagination and energy, they are going to steal the show.

Problem is principally one of translation, since large part of stuff comes in clear and code problems are either not serious or can be licked. When sure that with help of State Department, with vigorous efforts to find personnel without being scared by shadows (and security problem could be taken care of easily by putting this translation operation in place away from Arlington) and with MSVCL selling job that should be easy in light of evidence of what British have been able to do, this JIG commercial picture could be built up into one of best intelligence sources available. Whole job except decoding could be handled by Special Branch if translating talent were found, and translators of ability might be willing to participate in work that would involve *both translating and adding up the produced intelligence.* Strongly recommend

that you consider this in prayerful conference with powers, including Adolph Berle.

JIG commercial part of White's section describes itself also Translation Bureau and consists of six translators and two lady clerks. Principal translators are Captain Rayment and Captain Shaw, both of Navy, and a civilian who I believe is an ex-consul. When war began Shaw was serving as Chief Cryptographer at Singapore. Rayment was officer of Naval Intelligence and JIG expert and translator for Navy. Note quality of personnel assigned to this commercial field.

Believe their traffic comes from Point Grey and other west coast Canadian stations and is sent over every week or ten days by bomber. Great majority of items are in plain language. Material in four figure code thought to be mercantile marine code, in which page start with 111 or 110 are of interest to Park and are sent up there. Some of material is in NYK RPT or OSK RPT OSK codes, and occasionally there are items in one of the other MITS RPT MITS. Some messages are in public commercial codes. In cases of both MITS, both old and new books are used, old ones for Europe. I understood them to say that in both cases they have old books and have made progress in building up new ones.

Large part of traffic is inconsequential, such as small financial remittances and even greetings. Rest of it concerns mainly commercial transactions, mostly offers to buy or sell, conditions on obtaining licenses. There are however about ten or twelve items per day in ship material from Canada which are important enough to circulate. Examples of these as given were references to ships by name or routing, reports or large financial transactions or of specific completed commercial transaction, messages which give address of military or naval unit or ask for personnel for such purposes as building ships, putting up power house, or contain information or clues to progress of dock repairs, restoration work on mines, refineries or something of the kind. Their rough guess on volume of Canadian material is fifteen hundred items per week.

An important source of material is intercept station at Mauritius, which sends it only code or cipher material. Plain language stuff taken down at Mauritius is apparently translated there and sent directly to Economic Warfare Ministry. What Berkeley gets from Mauritius is mainly in commercial codes, and 80% of stuff of both MITS is picked up there. Much of it involves Indo Chinese peninsula but it covers all areas of interest to us, perhaps twenty five percent of material is worth circulating. The two Navy Captains were very vague of figures, but they finally produced traffic register covering the four syllable

MIT form, for periods from last August to this May 15, and I counted up four hundred fifty five recorded messages. Could not count number circulated, but my guess would be around one fourth.

Third source of JIG commercial is what is picked up in England, mainly stuff from Continental points. Output of JIG Commercial Section goes in longhand to Alford House, where 'Commercial Section' of Berkeley Street is housed.

The material is typed up and routed to consumers. Taylor will give you in later message important facts re Aldford House. Note that principal consumer, Economic Warfare Ministry, gets not only what is produced in White section but also what comes from New Delhi, where as you know considerable work is done on commercial stuff, and also whatever Mauritius turns out from its plain text interceptions. End of story re JIG at Berkeley Street.

Finally got two letters

Note to code clerk: after third, repeat, in part seven text should read 'output' of JIG Commercial Section goes in longhand to Aldford House, where 'Commercial Section' of Berkeley Street is housed etc.

(Special Friedman System)
4232
Date Completed May 24 1943
Time Completed 1545 Z

ARLINGTON HALL STATION
MESSAGE CENTER

Date Filed May 22 1943
Time Filed 1620Z

INCOMING MESSAGE
FROM: AMEMBASSY LONDON
TO: MILID WASHINGTON
NR: 4837

PART ONE
Continuing with Denniston's distribution and reference section: this section keeps indexes of all circulated material.

(TO STRONG FOR CLARKE signed McCORMACK)

This work is done in longhand, mainly by the two girls, but it may interest Huddleston to know that Foreign Office officials and Cambridge professors, unlike Harvard Law School graduates, are not above putting pen to paper in order to produce good indexes. I have examined a number of index cards and hereby pronounce that a good workable index can be maintained in longhand and that it would not be any great intellectual feat, though it would take time, to devise system under which what our girls do not now index could be indexed in our own geographical sections by men who follow the material and without occupying many of their minutes during any day.

AS Nr 4216
Date Completed May 25 1943
Time Completed
(ATTENTION DURANT)

One of the indexes is a name file of all name references in special material, in which important events in lives of senders of messages are noted and also all references in messages to individuals, on cards under their names. In cases like those of *our favorite oriental author** his trips and important interviews are noted. Collateral information is also noted, in much the way Durant's section..... job, though job is keyed on lower scale and they have advantage of working with file that goes back before last war. They now have 19,000 names in file, of course after eliminating those who are permanently dead. Subject indexes are kept, based not only on Berkeley Street material but also on cables

* Hirohashi, Japanese ambassador in Berlin and crony of Nazi high command.

of various government officers.

By far the largest subdivision in index is Treaties and under it, by countries, are set forth all details about treaties and negotiations for treaties among various governments.

By all details I mean dates and important subjects dealt with, but of course cards do not attempt to cover any whole subject further that is necessary to refer index user to underlying material. Index cards give references by dates and serial numbers to source material. Next to treaties the largest headings are 'Conventions – Economic' and conferences. While it may seem like going into too great detail I believe that it would be useful for our people to have exact idea of subjects considered important index headings, and I therefore set them forth:

> Air Associations and Federations; Banks; Budgets; Churches; Commissions and Committees; Communists; Anarchists; Espionage Plots Outrages etc (we were told confidentially that this elaborate heading is really designed to cover subject of enemy spy organizations in various countries); Concessions and Contracts; Conventions; Coups D'Etat; Ciphers; Debts; Delegations and Missions; Disarmament (including sub-headings for disarmament conferences); Economic (under which subject headings are almost all names of commodities, with oil comprising by far the largest amount of material, but with some non commodity subjects such as 'mergers'); Economic Number Two under which information is indexed by countries; Exhibitions; Expeditions; Finance; Frontiers and Frontier Incidents; Jews; League of Nations; Loans; Mandates; Military and Military Missions; Naval; Opium; Press; Propaganda; Railways; Refugees; Revolutions, Plots etc; Shipping; Slavery; Supply of Munitions; Tariffs and Customs; Telegraph, Telephone Lines and Wireless; Traffic in Arms and Trials.

Please have Huddleston meditate in more prayerful attitude than usual on lessons to be learned from these headings.

Note that under Treaties headings they put not only treaties and negotiations as such but also all relations between government not otherwise classifiable. Whole impression is that, like everything else that these very practical people do, index is designed to serve its purpose as neatly as can be achieved with minimum waste of effort. Note also that, while they try to keep track of all material for sake of whatever information readily available in indexes, their primary purpose is to supply crypt people with reference file in which they may locate quickly whatever information may be helpful to them in solution work.

Another important reference item is what they call the Cabinet Book. This is record of important officials in various governments throughout world, but it is very different thing mechanically from what Durant keeps. It is big ledger with subdivisions by countries in alphabetical order. When you turn to pages devoted to any particular country you find clippings and longhand notes giving names of cabinet officials and elected officers in order of dates, and you may trace through pages for any country and see very quickly what governments it has had for years covered by book. It is all somewhat disorderly in appearance, but when you examine it you find that, what with clippings from Times and Telegraph and longhand notations, there is a surprising amount of information in a form where it is quickly usable.

They also maintain a file of ships referred to in material, but here you may doff my hat to brother Snow, because this is the only thing I have seen in England in this general field where we have done a better job. One of the most interesting records that they keep, and from what they say one of most useful, is what they call the Diary. This is a very large bound book in which each day is assigned two opposite pages, on which notations are made in longhand of all the events of that day that might be interesting to one who is working with material that might involve such events. The important subjects are mainly country classifications, and for every day the information about any country or other subject classification is set down at the same place on either the left hand or right hand page. For instance everything about Turkey is always to be found, say, in column five on the left hand page, three quarters down the column, so that a crypt man who wanted to know what was going on in Turkey over a period of two weeks last year can see at a glance what was happening in Turkey everyday, as gleaned from intercept material, government communications, or news reports in London Times or Telegraph, which are the two newspaper sources that are relied on. Note that these two newspapers are clipped daily for all news of possible diplomatic importance for each country and the clippings put in country file with intercept material and government cables, all in order of dates.

Nothing is filed twice. If an item affects Russia and Japan it is filed under either Russia or Japan but not both. According to rules of thumb evolved over the years they decide which country; but if the same subject involves communications between the opposite Ambassador and his country, they file it under that country.

You can see how little they permit duplication of effort and building up of cumbersome files.

Incidentally, coming back to the Diary, let it also be noted that Diary contains after each item entered the reference to where full information may be found in the various sources on which it is based. Another file maintained is the Who's Who file, which appears to consist almost entirely of Foreign Office printed bulletins which identify diplomats in various parts of the world and other important personages. It seems that British diplomats report periodically to Foreign Office on all important diplomatic and local personalities in their respective countries, giving not what might be called official information but also whatever else may contribute to Foreign Officers store of useful knowledge. For example, of one diplomat it was stated that he had a youngish wife whose myopia required her to wear very thick glasses and of another it was intimated that his wife was on the frivolous side and "is not interested in the community problems on which her husband works so indefatigably". I mention all this as further evidence to the thoroughness with which these Britishers do their jobs.

Same section also keeps reference library for use of Berkeley Street personnel. Among books that they have published weekly which deserve note is a manual of current events, published weekly, known as Kensing's Contemporary Archives, subtitle Weekly Diary of Current Events. This is published in England and covers all events of note in the world. I understand that it is difficult to get a subscription to it now, but please ascertain whether Arlington and Gee Two get it, because 1 think they should if they do not now get it. There is a library of Who's Whos and various reference books of the sort that you would expect, and where they are out of date and more recent editions are now available the staff annotates the books as new information comes in. For instance the German encyclopedia of newspapers of the world Handbuch der Weltpress, compiled in 1934, has been kept up to date by staff following all information about newspapers in various countries. Staff seemed to feel that one of their most useful books was Annual Pontifico, the Vatican yearbook, though it seemed to me to be no more than a catalog of Vatican representatives throughout the world.

One very interesting set of books is a series that is being published by the 'Naval Intelligence Section' of Admiralty about various countries of the world. This was started in nineteen forty two. I had brief look at books on France and Iberian Peninsula and they appear to cover every conceivable subject that would be interesting to one interested in the particular countries. They are called 'Geographical Handbook Series' and if Gee Two does not have them immediate steps should be taken to get on circulation list. They are not to be sold publicly but are for use within British Government. However Earnshaw Smith said he was sure that any United States agency could get on list if

it wanted to. Another excellent reference book that Gee Two should take steps to get if they are not getting it is an annual publication of the Empire Parliamentary Association called 'Report on Foreign Affairs'. This gives for each country of world a chronology of all the important events during the year. It has a good index and would make excellent reference book, especially for Arlington. Another publication that noticed, and I think Foreign Office gets it out every so often, is Q Book of Geographical names. They say that it is much used in identifying places referred to in messages.

Smith's section also receives foreign language press of various countries and (this is interesting) sends it to interested sections where it is read by crypt people or translators in order that they may keep up with developments in the respective countries. They do not cover German press, which is very thoroughly covered by other Government agencies, but they read at least one newspaper from principal cities in each other country in which they are interested. Note: I now have figure for present message numbers in Denniston's outfit to wit 117,000 odd, indicating that in last fifteen months some 17,000 messages have been circulated.

Continuing: in addition to files and indexes kept up by distribution and reference section, each geographical section maintains whatever files it may think helpful. We did not get a chance to see what files are kept, but have impression that long organized sections have built up substantial amount of reference material.

All foregoing may seem to you too detailed to justify use of cables, but we are anxious to give you as full a picture as possible in order that you and Corderman may ask any questions that occur to you or suggest what further lines of investigation we should pursue.

Whole key to this British operation lies in the infinite pains which they take with the files while never losing sight of their very practical objectives.

AS Nr 4216
Date Completed May 26 1943
Time completed 0200Z
(Special Friedman System)

ARLINGTON HALL STATION
MESSAGE CENTER

Date Filed May 24 1943
Time Filed 17250Z

INCOMING MESSAGE
FROM: AMEMBASSY LONDON
TO: MILID WASHINGTON
NR: 4860

(TO STRONG FOR CLARKE AND CORDERMAN FROM TAYLOR signed PEABODY)

Herein report on near Eastern Section of Denniston's show. Understand you have had through Johnson full information on cryptographic method which I am including cryptographic information given me for what it is worth. *Section comprises eighteen people of whom seven are linguists and do the book breaking and translating, ten are decoders and clerical, and one is keybreaker for Turkish traffic. Section handles Turkey, Saudi Arabia, Iraq, Egypt, Iran, Afghanistan, as minor sidelines Syria, Transjordan, Nepal and Ethiopia.* Head of Section Dr Thacker is Professor of Semitic languages at Durham University and can do all three languages involved to wit Turkish, Persian and Arabic but specializes in Arabic PYIOT KISH Most important branch comprises one keybreaker, five decoders and clerks and three translators and bookbreakers; Thornhill, a clergyman and former pupil of Thacker's at Durham has learned Turkish in last two years, Simpson, geographer at University of London has learned Turkish since war began, Gungry learned Turkish recently at School of Oriental Studies formerly in London now in Cambridge.

Persian section three decoders and two translators; Humphreys, elderly and only permanent employee, was Archivist British Embassy Persia for many years and knows other Near Eastern languages as well as Hindustani, Russian and many others, Boyle learned Persian at School of Oriental Studies.

Arabic section two decoders and two translators, Thacker and Dr Lewis lectured in Islamic history School for Oriental Studies.

Turkey uses Turkish except for one code book in French for treaties etc, *Saudi Arabia* and *Iraq* use Arabic, *Egypt* uses French, *Iran* and *Afghanistan* use Persian, *Syria* has not started code yet because has no diplomatic posts but will be in Arabic, *Transjordan* has no diplomats but Emi Abdullah has private

cipher in Arabic which British read but Emir has not yet said anything worth circulating.

Nepal uses simple substitution cipher in English and three messages have been circulated in last eighteen months, *Ethiopia* has five figure book for traffic between London and Adis Ababa, British have twelve messages but cannot read them.

Turkish section receives fifteen to thirty messages per day, slightly more to Ankara than from Ankara, and circulates from two to twelve per day perhaps six would be a fair average; majority of circulated messages are to not from Ankara. *Principal circuits covered are London, Kuibyshev*, Teheran, Budapest, Lisbon, Rome, Madrid, Stockholm also some Berlin, Washington, Vichy, very little South America, Helsinki, Bucharest, Sofia, good coverage Tokyo but very little traffic.* Two principal secret diplomatic code books introduced middle of nineteen forty one called CANKARA and ISMET INONU both ten thousand group two part codes.

---

* Kuibyshev - a town 500 miles east of Moscow where the Soviet government's main government agencies relocated in late 1941

ARLINGTON'S LIAISON WITH BERKELEY STREET

Excerpt from Cable No. 4989, June 6th, 1943.

In order to comply with instructions in your 2734, I will have to discontinue all discussions with Denniston, since there are no intelligence problems to discuss except those which have to do with crypt and traffic exchanges. Since Denniston is willing to let somebody here read, and if interesting to forward to Washington, all decodes not in special reserved series, the only questions that have been involved have related to whether the Government of the United States was willing to take particular classes of intelligence that way, or whether as to some or all of them it wanted to process the material itself. I will tell Denniston that these problems will be worked out directly by Corderman or perhaps through Taylor. It is disheartening, however, to work hard on getting the facts for Arlington and to get this kind of response.

While you prepare Washington Monument for appropriate part of my anatomy, I will say flatly that Arlington does not (repeat does not) understand the problems involved in crypt and traffic exchanges. For instance, *it has just thrown Denniston into a state of bafflement by asking for Iraqui keys. This request would be roughly equivalent – if we still had the Philippines - to the British asking Arlington for Philippine keys, since Iraq is not only in reality part of the British Empire but is the cornerstone, because of its oil, on which the whole Middle East and Eastern Mediterranean situation rests.* Denniston, however, wanted to put Arlington in a position to read whatever Iraq stuff it might intercept, insofar as he could do it without going to the Foreign Office for specific authority. Hence he authorized his people to explain the Iraq system to Taylor, and Taylor duly passed the information along, and Denniston felt that he had met Arlington's demands without having to create an issue here. If questioned by the Foreign Office, he could always say that Iraq uses simple substitution which any cryptanalyst who had an Arabic linguist at hand could solve in half an hour, and so he had really only told Arlington what it could have found out for itself in a very short time.

Now however, Arlington turns this matter into a major issue by a formal request for keys, forcing Denniston either to put himself on record as refusing something that Arlington specifically asked for or to create an issue by asking the Foreign Office for permission. If Denniston is right about the difficulty of solving the Iraq system, what sense does all this make?

Some of these Britishers, I think perhaps including Denniston, think we in Washington are a little bit at loose ends, and what do you suppose I would

think, if my thoughts made any difference, when I get three cables in short succession, one of which says that cables were omitted because nobody asked for them, the second says they were omitted because the parties were exchanging them through censorship, and the third says they were omitted by common consent. Jesus. Taylor has been talking to Deniston about the Iraq matter and he is holding it in abeyance until Taylor gets back and has further talks, after which Taylor will communicate with Corderman.

ARLINGTON HALL STATION
MESSAGE CENTER

Date Filed June 30 1943
Time Filed 1945Z

INCOMING MESSAGE
FROM: LONDON
TO: MILID WASHINGTON
NR: 5142

(TO STRONG FOR CORDERMAN FROM TAYLOR signed PEABODY).
AS Nr 5830
Date Completed July 1 1943
Time

Iranian principal diplomatic book has been photographed and was sent to day to Baker Peter for transmittal to Washington. Have been discussing smaller enemies and will have further information next week. Reference FLORADORA agreement Berkeley Street has sent off two batches for you and are sending specially about eight Dublin items at my request; they are interested to know how Arlington is coming on its share of back traffic, which is to be interchanged on fortnightly basis enciphered with forty figure subtracter. Washington does not figure subtracter, Washington does not hold ISMET which is perhaps the more secret of the two except at London which treats CANKARA as more secret, Tokyo has neither and uses one of three older books of same type enciphered with five to forty figure subtracter and used except at Tokyo only for administrative traffic. Subtracter changed at frequent intervals. In addition Turks have French book for treaties, obsolete consular book, and military attaché book held at all capitals one part thirty thousand groups enciphered with short subtractor or by switching order of figures within the groups.

Saudi Arabia intake fifteen to twenty messages per day, circulate two or three per day. Capital is at Riyadh but King nomads around and traffic may center at Taif summer residence, Mecca during pilgrimages, or Jedah where foreign diplomats are kept. Circuits are to Ankara, London, Baghdad, Cairo, Damascus, Jerusalem and Vichy (now defunct). Principal code is two years old three letter two thousand random groups used unenciphered, also two new books used at Ankara two letter seven hundred fifty random groups. For administrative financial and less secret political use simple two figure cipher.

Iraq traffic intake four or five per day circulate perhaps one a day. Circuits

are between Baghdad and Aleppo, Alexandria, Beyrouth, (Bombay, Cairo, Damascus, Jeddah, Jerusalem, London, Kabul, Teheran, Washington and Sanna (defunct). So far this year 21 messages Baghdad to Washington of which British have four, and 34 messages Washington to Baghdad of which British have all but one. Iraq messages are really in clear, they have arbitrary Roman letter equivalents for Arabic alphabet and only element of cryptography is that letter equivalents vary from post to post; also use cover letter combinations for names of people, places, dates etc.

Iran traffic intake about 1,000 messages per month, circulate about one hundred per month. Circuits covered are between Teheran and Ankara, Baghdad, Baku, Basra. Berne, Beyrouth, Bombay, Bucharest, Cairo, Hamburg, Herat, Istanbul, Jerusalem, Kabul, Karachi, Khanegin, Kuibyshev. London, Mosul, Quetta, Rome, Simla, Smyrna, Soleynanieh, Stockholm, Tokyo, Trebizond, Vichy and Washington. Washington traffic about ten percent of total. One diplomatic and one military book each alphabetical 12,500.

Afghanistan intake five or six messages per day circulate about every other day. Circuits are between Kabul and Ankara, Bombay, London, Teheran, Meshed, Berlin, Rome, Geneva, Tokyo and Vichy, traffic with Tokyo very infrequent and purely administrative. One book which closely resembles the Persian.

I spent several hours reading nineteen forty three output of Near East section. While the Iraq, Saudi Arabia, Afghanistan and Egypt output is picturesque and occasionally interesting I think it is a safe assumption that we can live happily without reading this mail immediately and in any event I will probably be able to send you decodes of anything of interest. Iran for the most part is dull stuff but contains some significant material in view of our present special interests in Iran and I think we should read this as soon as possible. Turkey is definitely an important line; it is disappointing in that messages from Ankara are largely administrative and do not substantially reflect leanings of the government, but *traffic to Ankara contains a fair number of very important messages such as interview with Molotov, or with JIG agents in Far East*; furthermore a great many messages from smaller European capitals seem quite as important as those of familiar ministers at some points whom we frequently honor with an item in the Bugle. Thacker tells me that since April all Turkish traffic has been sent to Washington, if Arlington has not been getting it please let me know promptly. Subject to your approval I propose to make photographing and mailing to you of important Turkish books matter of first priority and that of Persian books second priority and Chinese books third priority.
As Nr 4316
Date Completed May 27 1943
Time Completed 1850Z

ARLINGTON HALL STATION
MESSAGE CENTER

Date Filed May 25 1943
Time Filed 2050Z

INCOMING MESSAGE
FROM: AMGN EMBASSY LONDON
TO: MILID WASHINGTON
NR: 4861
(TO STRONG FOR CLARKE AND CORDERMAN FROM TAYLOR signed PEABODY).

Friedman and myself have seen *Italian* section Denniston's show, Friedman will report on personnel headed by Mr Catty and cryptanalytic features. British coverage includes hosts at Madrid, Lisbon, Tetuan, Tangiers, Tenerife, Lobito, Dublin, Stockholm, Oporto, Seville, Barcelona, Raima, Helsinki, Bratislava, Vienna, Budapest, Sofia, Bucharest, Belgrade, Athens, Rhodes, Istanbul, Izmir, Adana, Mersina, Kabul, and Sanna now quiescent. According to my recollection our coverage of above circuits has been poor or nonexistent. I am told that since April first they have been sending us copies of all their traffic; if traffic is now reaching you I assume it can be read at Arlington as well as here if not please let me know. Cryptanalytic exchange appears to be going smoothly and no pressing problems in this quarter, however I propose to read back files of decodes on above circuits and send you anything of real interest.

This section includes two ladies who handle *Vatican*. Work started on this line April 1942 after lapse of two years in continuity. Up to December first nineteen forty two British had received six hundred sixty four messages in all ciphers and read five hundred fifty or eighty two percent, Only sixty four were found worth translating and circulating and these are made to be of little interest; I plan to read these as well as later and current traffic and send you if important. Most traffic is ecclesiastical charitable or personnel. Apparently stuff goes by bag. One system in use London, Vichy, Berlin, Madrid, Lisbon and Washington is not yet cracked because of traffic shortage.

AS Nr 4319
Date Completed May 26 1943

ARLINGTON HALL STATION
MESSAGE CENTER

Date Filed May 25 1943
Time Filed 1817Z

INCOMING MESSAGE
FROM: AMCN EMBASSY LONDON
TO: MILIDWASHDC NR: 4871

(TO STRONG FOR CLARKE AND CORDERMAN FROM TAYLOR signed PEABODY).

Herewith some miscellaneous information on Berkeley Street *Brazilian* and *Portuguese* sections, Friedman will report in detail on crypt observations. Section comprises ten people of whom five are decoders and clerical and five are linguists bookbreakers of whom two do cryptanalysis. No permanent employees. Head of section -ELL is a botanist who has researched on Portugal and colonies. Brazilian largely handled by his wife and one assistant. Enterprise started February nineteen forty at which time all continuity had been lost. As in case of Italian. British have been covering several Portuguese continental circuits inaccessible to us, I will run over these old decodes and send you nuggets Am told that since April first they have been sending us all Portuguese DIP traffic, but not Portuguese colonial traffic, which can be read here. One basic book for all colonial with variety keys. Am told colonial traffic is most uninteresting but will look it over. *Portuguese military use PLAYFAIR at Lisbon and Lourenco Marques, simple substitution at Atlantic islands, British read both kinds. At end of March this year the Portuguese bought some Swedish HAGELIN repeat HAGELIN machines and have them at Air, War and Colonial Ministries,* some Azores traffic in Hagelin has been observed. Portuguese security police in Azores at Ponta Delgada are using ten alphabet substitution, I am told British have sent us the keys for this
AS Nr 4337
Date Completed May 27 1943
Time Completed 1800Z

ARLINGTON HALL STATION
MESSAGE CENTER

Date Filed May 25 1943
Time Filed 1700Z

INCOMING MESSAGE
FROM: AMEMBASSY LONDON
TO: MILID WASHINGTON
NR 4874

(TO STRONG FOR CLARKE AND CORDERMAN FROM TAYLOR signed PEABODY)

Herein the smaller European enemies. *Hungarian* not read and continuity lost but Denniston expecting return of someone who will soon undertake it; however Hungarian commercials in clear are translated by member of Swiss section and circulated if important.

Paragraph two. *Roumanian* section consists of Griefenhagen former diplomat and one secretary started nineteen forty having lost continuity and started reading nineteen forty one. Intake zero to twenty messages per day perhaps twelve average. Principal circulation a day perhaps twelve average. Principal circuits covered are to Lisbon, Madrid and Rome, also get some Stockholm, Helsinki, Tokyo and Buenos Aires. Highest grade code not read, is in early stage of reconstruction. Bulk of traffic in two large two part codes called Roger Forty Two and Roger Forty Four, some of the traffic is enciphered. Roumanians follow French practice of numerous and voluminous two part codes. Bulk of traffic which is circulated is commercial in nature, for instance purchases of Spanish lead and blankets and Spanish demands for oil in exchange. So far as is known there is no Roumanian exiled government traffic.

Bulgarian section. Woods elderly permanent and one secretary. Continuity since 1934. Small traffic intake circulate perhaps one per week. Principal circuits covered are Berlin, Kuibyshev, Roge, Vichy, Budapest and Bratislava; Tokyo which has new book can't be read and Stockholm can't be read. No Bucharest traffic. Coverage on all circuits very poor; for instance between Sofia and Berlin they got only twenty four out of 450 messages. For administrative purposes an old one part code is used unenciphered, pagination changes twice per month. Secret stuff in newer books used unenciphered.

Woods also handles *Jugoslav* traffic; diplomatic books not yet read, *Jugoslav Army Chief Cairo named Pretnik talks to London and Istanbul in double*

transposition but British switch the keys. Jugoslav intelligence organization headed by Piritch is housed at Istanbul and is in touch with Mihailovitch. apparently using same system. Three or four Jugoslav messages per day are procured and about seventy five percent of the intake is circulated.

Friedman will I hope supplement crypt data herein. Will look over old decodes of all this stuff. Please advise have sent dozen letters home hope some received.

AS Nr 4330
Date Completed May 27 1943
Time Completed 1145 Z

ARLINGTON HALL STATION
MESSAGE CENTER

Date Filed May 25 1943
Time Filed 1912Z

INCOMING MESSAGE
FROM: AMCN EMBASSY LONDON
TO: MILID WASH DC
NR: 4875
(TO STRONG FOR CLARKE AND CORDERMAN FROM TAYLOR signed PEABODY)

Research section Berkeley Street four men two women, headed by Sainsbury. Main job is to take problems about which nothing is known and penetrate far enough so that problem can be turned over to language section for bookbreaking etc, and secondary job is to handle odd sticky problems for language sections. Sainsbury speaks Finnish and his section theoretically handles Finnish Hagelin but in fact is doing little on it; Norwegian Hagelin was dropped long ago and Swedish Hagelin has been dropped as impossible because of excellent Swedish use. In fact Hagelin activity at Berkeley Street appears to be at complete standstill, possibly because best Hagelin man is at Baker Peter. *Main current occupation of this research station is Free French; they appear to have made a considerable penetration of principal diplomatic system, but I was told there has been no interchange of cryptanalytic data on Free French with Arlington as yet.* System in question is based on four figure code groups, the first figures are reinciphered on a table into three figures producing five figure groups, and this result is transposed on a key derived from the magazine France Libre. Bulk of traffic perhaps ninety percent is furnished by Cable and Wireless Ltd.

Next job scheduled for research station is Dutch about which nothing is known.

ASNr 4355
Date Completed May 27 1943
Time Completed 1845 Z

ARLINGTON HALL STATION
MESSAGE CENTER

Date Filed May 27 1943
Time Filed 2132Z

INCOMING MESSAGE
FROM: AMCN EMBASY LONDON
TO: MILIDWASHNDC
NR: 4894 M g 7

(TO STRONG FOR CLARKE AND CORDERMAN FROM TAYLOR signed PEABODY)

Continuation of my message on Commercial Section number four eight seven six. Extent of shift from commercial code to clear is most surprising; excluding JIG, out of some 7,000 intake per day only about one hundred are in code all the rest in clear. French and English branch of commercial section comprises four people, intake about two thousand per day, circulate in Charlie Sugar series about two hundred per day. No translation done in this branch, British assume everyone can read French and circulates French messages in French.

German branch ten people, circulates from one hundred fifty to two hundred per day; small amount is MOSSE repeat MOSSE but the bulk is in clear, HISROWAK traffic not handled by this branch in considerable German traffic to Far East, some of which reflects German sales of machinery; other traffic deals with transactions in grain, mohair etc with Turkey and Spain, seems to be an important line of traffic. *Italian* section five people, all the traffic they handle is in clear; circulate about one hundred per day, covering BARFDV* with Turkey, special articles, list of other MEW papers which can be procured on request, etc; MEW Far Eastern weekly intelligence summary classified secret ten pages covers broadcasts and other information including Charlie Sugars, arranged by geographical areas within Far East with special sections on shipping and trade with Europe; MEW monthly statement of action taken secret twelve pages arranged geographical sections special sections on relief, contraband control, enemy transactions. MEW also furnishes secret daily Lloyd's Shipping Index showing sailings and locations of merchant ships. MEW also puts out short weekly list most secret summary of comm. Series which has very limited circulation.

I examined March file of comm. Series covering serial numbers 7540 to 8500 about thirty per day. JIG messages averaged perhaps twelve per day,

usually two to four each German, Portuguese, Spanish and Swiss, scattering French, Italian, Turkish, Belgian, Persian and South American. Also included occasional Spanish Naval Attache messages between Berlin and Madrid sent down to Hope from Baker Peter called 'XIP Series' dealing chiefly with German naval supplies to Spanish Navy.

Also hastily examined two days output of Charlie Sugars each about important trade with Spain, and most important purchases of Roumanian and Hungarian oil by Italian companies such as AXSP (Axienda Generate Italiana Petrol) and Sterava Romana. Portuguese Charlie Sugar circulation about fifteen per day, Spanish forty, miscellaneous (comprising Hungarian, Roumanian, Bulgarian, Finnish and Japanese) one hundred per day. Cryptanalytic section five people headed by Hooker, whose routine job is to handle HISROWAK KRYHA traffic but also do other commercial ciphers; for example Italian 1STCAMXI cipher based on Mengrini code used Rome to Lisbon, German MELCHERS cipher used Bremen to Tientsin and Mukden, Italian commercial attaché cipher used by Angelone, and a cipher which lay on top of JIG OKURA book was pulled off and book was turned over to Berkeley Street for breaking.

The six thousand messages rejected by Hooker are sent to Information and Records branch of censorship which re-examines them and sends about five hundred per week to MEW.

Relations between Hope and MEW very close and MEW gives Hope lots of stuff to assist his work as follows: MEW weekly intelligence report classified secret ten to twelve single space legal size pages contains notes covering week's developments, long term five hundred messages. Single messages rarely meaningful and it seems clear to me that either we must rely on British and accept their intelligence summaries based on this mass of material and other related material from other sources, or else we must start a very substantial operation of our own. It would be impossible for us to process or digest the Charlie Sugar series even with several assistants

May be twenty

AS Nr 4414
Date Completed May 28 1943
Time Completed 1600Z

SECRET
ARLINGTON HALL STATION
MESSAGE CENTER

INCOMING MESSAGE
FROM: LONDON
TO: MILID WASHINGTON
NR: 5142

Date Filed JUNE 30, 1943
Time Filed 1945Z

(TO STRONG FOR CORDEMAN FROM TAYLOR SGD PEABODY)

IRANIAN PRINCIPAL DIPLOMATIC BOOK HAS BEEN PHOTOGRAPHED AND WAS SENT TODAY TO BAKER PETER* FOR TRANSMITTAL TO WASHINGTON. HAVE BEEN DISCUSSING SMALLER ENEMIES AND WILL HAVE FURTHER INFORMATION NEXT WEEK.

REFERENCE FLORADORA AGREEMENT BERKELEY STREET HAS SENT OFF TWO BATCHES FOR YOU AND ARE SENDING SPECIALLY ABOUT EIGHT DUBLIN ITEMS AT MY REQUEST. THEY ARE INTERESTED TO KNOW HOW ARLINGTON IS COMING ON ITS SHARE OF BACK TRAFFIC, WHICH IS TO BE INTERCHANGED ON FORTNIGHTLY BASIS.

AS Nr 5830
Date Completed JULY 1 , 1943
Time Completed 1300Z

---

* Bletchley Park

SECRET

17. G- Section (Floradora).

The G Section is primarily 'Floradora'. It started out as strictly an amateur show under the present section head, who is attractive 25-year old Patricia Hartley, whom Tiltman took at the beginning of the war fresh from Oxford and trained in his school. Assisting her in the central direction of crypt work are Lt. Filby, Librarian of one of the Cambridge libraries attached to Trinity College, and 2 civilian men who formerly worked for Barclay's Bank In Germany. The total personnel of the section is 37, of whom 3 are registers of traffic, 17 are code clerks, who are proficient in German, and the 13 not included in the above figures are the following: Key breakers, Fett Erlien [sic Fetterlein], dean of crypt people and a permanent employee of great age, who was the leading figure in this work in Russia during the last war and has been with the British ever since, Adcock, Professor of Classics at Cambridge, and Trainor, another permanent employee; three who comprise the liaison section and do practically everything except break keys, depending where the heat is on; and 7 top-flight translators. Including a schoolmaster named Pallinger, and one Potter, who before the war was the German Foreign Office expert on diplomatic English.

18. Conversations with Denniston.

Certain gleanings from conversations with Denniston may be of interest to you, in case you are discussing with Arlington any of the problems involved in diplomatic and commercial.

First, as to Japan, Denniston says that if Arlington wants to divert any talent from present Japanese operations to turn them to JAC (?) he is prepared to take up the full slack and to transmit finished translations of all material here plus anything that Arlington wants to send him for that purpose.

Second, *he expresses a desire to give Arlington traffic and information of every kind that has to do with winning the war, by which he means complete exchange of all enemy traffic and crypt information plus anything that Arlington wants to get out of the non-enemy field where, as in the case of Turkey, we have asked for it and stated reasons connected with the war effort.*

Third, he agrees that in the crypt field each country wants to establish for itself a position of independence so that it can get and turn its efforts toward any class of traffic that may interest it.

Since in the European field the British have been in the game much longer than we, and can supply both traffic and solution information, he agrees that it is only fair for them to give Arlington the benefits of their experience and also traffic if they want it. The only lines that he appears to draw are these. He has express instructions from the Foreign Office which prevent him from giving cable traffic into or out of London. He is not enthusiastic about giving us traffic on areas which are considered by the British as their primary concern, such as various Near East areas, but nevertheless admits that we are now so committed in those areas in their war aspects that, if we ask for that solution information, he will have to furnish it though not including traffic to and from London by cable. As you know, the British have a cable running around Africa and of course have their own communications net over which they can permit the Shah of Persia or whoever else it may be to communicate with his representatives in London or elsewhere. Finally, he distinguishes between information as to solution methods and crypt documents (defined to mean code books and key tables obtained either by cryptography or by S.S. methods). While he is prepared to give everything that they know about methods of solution, so far as Arlington may now or hereafter want them, he does not want to commit himself to give crypt documents except where required for immediate jobs related to the war. It is not clear how much in this case he is influenced by the difficulty of copying some of the books that Arlington might want, though he stresses that point, and his facilities for copying are rather limited; and he mentions some instance of a year or so ago where he had some stuff copied for Arlington which was valuable only as library material and not for current use connected with the war.

In general, he would like to employ liaison on the intelligence side of those cases where liaison on the crypt side does not seem to him desirable. He is willing to let Taylor and another properly vested officer look at all material which is circulated by Berkeley Street, including all material into and out from London which is thus circulated. There is a limited class of material that his office sends to C instead of circulating, just as in the case of Park. He illustrates these by the case of some British diplomat 'dropping a brick' but very likely any case where, from the British standpoint, a delicate subject was involved would fall into this reserve class, and with an American officer reading the material it would only be natural that a new class of reserve material would arise, to wit, those that it might be unwise to let an American officer read. However, Denniston's whole approach is very reasonable and he says he has great hopes that all mutual misunderstandings will be cleared up and the line of liaison straightened out. While the basis for his feeling is not yet entirely clear to us, it is plain that he has been annoyed by the way Bailey and Maidment have handled the exchange problem, without consulting him as he

thinks they should, and without giving his people any clear idea of just what the exchange is supposed to cover. Taylor found that Waterfield, the man in charge of traffic, had no list to guide him on material to be interchanged and that he was sending what the various geographical sections gave him. Taylor then went around to the geographical sections and found that they had no very precise idea of the problem and that the section heads were deciding what to send on their guess as to what might be wanted.

This situation needs clarification, and *Denniston has said on several occasions that he did not like being unable to deal directly with Arlington on traffic exchange problems or on how exchanges should be handled. He also is very anxious to obtain good liaison with G-2 and has been going on the assumption that Taylor is to be quartered with him to function in that capacity. While there would be no point in trying to work out any revised traffic deal now, certainly not for us to try it, it appears to me that there is some value in pursuing discussions with Denniston along the above lines, so as to test his general ideas by specific cases, in order to carry back a fairly good idea of what sort of deals his authority permits him to make and what the general viewpoint here is on these various problems. His attitude, in my opinion, will permit all important intelligence problems along his alley to be solved satisfactorily, one way or another. Note also that Denniston, more than anybody else here, has turned his people over to us for questioning and given us a free run of his place.*

TOP SECRET
ULTRA

CHAPTER NINE

AGD's views on US/UK crypt co-operation 1943

TOP SECRET

Informal Memorandum by Cmdr. Denniston Outlining His Original Concept of the American Liaison

(Written In May 1943 and handed to Colonel Alfred McCormack)

It has occurred to me and others here that your visit provides a good opportunity to define the scope and limits of the liaison which we are trying to build up between G.C. & C.S. (Civil side) and Arlington Hall and G2 (Diplomatic and Commercial).

For my own personal part in this matter I have urged during and since my visit to Washington in August 1941 that Arlington's greatest contribution to the war effort is the effective and operational reading of Japanese military cyphers and that G.C. & C.S. was and is prepared to fill any intelligence gap in diplomatic work which may result from a supreme effort on Japanese Military by Arlington. I wish to repeat this and I know I shall have the support of my superior officers.

Colonel McCormack's letter to me on his arrival gave me great hope that mutual misunderstandings were going to be cleared up and that we should straighten out the line of liaison. I have arranged that you should see every section and every detail in order that you may be familiar with 'our methods and appreciate our aims, which are, in short, to provide our several customers with all possible intelligence derived by cryptography from telegrams from enemy and neutral sources. When you know all our departments who are in any way affected by our liaison, e.g. (in England) Foreign Office, M.E.W. and the Service Departments, whose efforts may be influenced by the knowledge of our cooperation.

The bases of the liaison between A and B are:

(A) (i) Cryptographic documents, i.e. code books and key tables obtained either by cryptography or by S.S. methods.
(B) Raw material, i.e. telegrams obtained by W/T interception, by cable censorship or by S.S methods
(C) The translated versions of the raw material.

Note: In London it is not the duty of G.C. & C.S. to extract intelligence from these translations: that is left to the Intelligence Sections in the receiving Ministries with whom G.C. & C.S. is in close touch.

I. So far as enemy countries are concerned (Germany, Japan Italy) it should be our aim to make the liaison absolutely complete and I believe we are already achieving this. If either A or B requires a telegram in cypher or en clair, it is passed without delay. It might be noted that Arlington helped us into the Japanese purple:

The immediate problem is the prosecution of the war and I consider it would be to our mutual advantage if G2 had their representative in London (Lt. Col. Taylor) as a liaison officer to GC&CS (civil side). He should have the entry to our D & R and all section … As to the purely cryptographic part of the liaison, this should continue to be direct between Arlington Hall and the sections but Colonel Taylor would be available here to clear up questions hard to solve by letter or telegram.

A.G.D. 21/5/43

Coffee Series: In December of 1944 it was decided by the State Department that the American Ambassador In Paris, Mr. Jefferson Caffery, should also be given access to diplomatic Ultra, and the American representative In London, Major Littlefield, went over to Paris and put Mr. Caffery into the picture. Subsequently, Mr. Caffery was serviced by Capt. Kellogg, the American Ultra officer, stationed at Versailles. In order to facilitate Capt. Kellogg's task, a series of messages, known as the Coffee Series, was instituted and dispatched to him by daily pouch. The American representative at Berkeley Street made the daily selections for the Coffee Series from the various British logs; he included in the series any diplomatic or commercial messages which bore on the situation in France or the Low Countries.

Bay Series: During the war the liaison officer selected from the various logs any messages containing information of a military character. His selections were telephoned to 3-US at Bletchley Park, who passed them in the form of signals to the interested commanders in the field. That series of signals was known as the Bay Series.

Stark Series: The liaison officer also read the various logs for messages containing political or economic information of interest to the various field commands, and selections made on that basis were incorporated by 3-US into the so-called Stark Series, which was forwarded to the top commander + G-2 at SHAEF (and to Mr. Murphy) and later to top commanders G-4 USFET and 21 Army Group by pouch.

Foreign Office Agreement on RES Series: As mentioned in a footnote above, at the time of the original liaison agreement the British reserved the right to continue withholding from circulation messages which they considered too hot for general distribution. Such items, which were consigned to a so-called Res (for reserved) Series, were not shown to the American representative. From time to time Col. Taylor urged on Cmdr. Denniston the desirability of abolishing the Res Series, or failing that, limiting it to the greatest possible extent. Finally, late in the summer of 1944, an agreement was reached between Gen. Carter Clarke, Deputy Chief of the Military Intelligence Service, G-2 and Mr. Peter Loxley of the British Foreign Office. By the terms of that agreement, which went into effect on 16 October retroactive to 1 September 1944, the only traffic reserved was to be London terminal traffic, since all other traffic could, at least theoretically, be intercepted by Washington, and since it was clear that duplication of effort in intercepting could be avoided only if the British agreed to exchange all non-terminal traffic. It was also agreed that all items which were designated for the Res Series were to be forwarded to the Foreign Office, and Mr. Loxley was to divide them into 4 categories, as follows:

(1) Items which could be 'derestricted' and released for general circulation.

(2) Items concerning military operations which, although not released for general circulation in London or in Washington, could be forwarded by the American liaison officer to Washington 'for G-2 only', with the understanding that

(3) undiplomatic remarks by British representatives abroad, etc. which the liaison officer was allowed to read in Mr. Loxley's office, but which he was honor bound not to copy or to summarize for Washington.

(4) Items which would continue to be unqualifiedly withheld.

In practice, the agreement proved to-be satisfactory. During the first year the number of items placed in category (4) averaged slightly over one a month, while the number in categories (2) and (3), although considerably larger, caused no serious inconvenience to Washington. The liaison officer called at the Foreign Office at least once a month to read the items in category (3) and to discuss the general development of the agreement. Relations with Mr. Loxley and (after his death in January of 1945) with Mr. Bromley were thoroughly pleasant at all- times. On at least two occasions the liaison officer queried the number of items placed in a given category, and the Foreign Office each time resolved the issue in favor of the Americans.

Future of the Liaison: After the end of the war in Europe certain of the liaison officer's duties will be terminated, and at the close of the Japanese war the scope of the liaison was automatically curtailed.

CHAPTER TEN

How The Story Broke

My father never talked to us, his children, about his 30 secret years from the beginning of WW1 to the end of WW2. He was totally discreet. My mother must have known what was going on in his mind from his retirement in 1945 till her death in 1960, but whether they discussed the heights of his success and the depth of his bitterness at the way he was returned to London from BP in 1942, and then dropped out of Berkeley Street to retire on a pittance, no one knows. Though now he had more leisure it seems unlikely that he devoted much of that to reminiscence. When he died, a year after our mother, my sister and I found the typescript of his 'The GC&CS between the wars' (here reprinted as chapter 6) and realised that his title was an accurate one and he had written most of what posterity would want to know about British government diplomatic deciphering between 1919 and 1939. Its publication, by Christopher Andrew in 1986 in the first issue of *Intelligence & National Security* was the signal for a flow of books and reminiscences, chiefly of BP, the main ones of which are listed in the bibliography. But a different front opened up in 1974 with the publication of Group Captain Frederick Winterbotham's *The Ultra Secret.*

Before that I know of only one reference to my father's work, and that was in an unkind memoir by the Soviet spy Kim Philby published in 1968. Philby revealed, quite casually, what the government had till then maintained strict secrecy about – the existence of BP in general and the split of its service from its diplomatic work in 1942. Philby realised that the German diplomatic intercepts he had collared from Switzerland would be right up my father's street and sent them to him for analysis: which he did, full of enthusiasm and demanding more, so that he and his team were then able at last to break 'Floradora', the German diplomatic cipher. No-one seems to have noticed this illegal and deliberate breaking of the Official Secrets Act by Philby, by that time very much a *persona non grata* in Whitehall, though his book was duly published in the UK, the USA and in translation. So 24 years after my father's retirement, he could have read something about himself no-one else was supposed to know about. But by 1968 he had died.

I did not publish *My Silent War* myself but I helped Philby's agent find an English publisher. By this time I was keen to put my third-hand knowledge of British sigint to good use in my own career as a publisher, but even keener to see some rehabilitation of my father's career in secret intelligence. Though I did publish Winterbotham's book in 1974 while at Weidenfeld, I was happy to let other publishers build the new public interest in spies and spying – fiction as well as non-fiction. So Gordon Welchman's book *The Hut Six Story,* on which I advised as to its early chapters, came out from McGraw Hill in 1982, and Peter Calvocoressi's *Top Secret Ultra* from Cassell in 1980.

The magisterial primary source for BP went to OUP after I had retired from the Press: *Codebreakers*, edited by Harry Hinsley and Alan Stripp, contained Hinsley's deep understanding of what made BP tick, as well as many first hand accounts of the work there. It was published in 1991 and later Michael Smith's *Station X* (1998) and Smith and Erskine's *Action This Day* (2001) added to the tapestry of wartime memories. These are the primary source for any account of BP's wartime activities.

For secondary sources, the leader is Ronald Lewin's *Ultra Goes To War* (1978) which went to Hutchinson; while David Irving's great account of Churchill in 1941 (quoted in chapter 2), a source wrongly avoided by most other historians because of the author's damaged reputation and right-wing political views gives a definitive account of Churchill's daily use of Ultra through the fraught months of that year. Irving discovered new PRO files (HW14) released under the freedom of information act detailing Bletchley's information on *Wehrmacht* intentions and achievements, and relates these to Churchill's conduct of the war in the months before the Soviet Union and the USA joined the Allies. Another excellent secondary source is Jozef Garlinski's *Intercept* (Dent 1982).

Ralph Erskine continues to keep an expert eye on all new relevant releases of HW and other secret wartime files, and there will certainly be others after the publication of this book. There are now 150,000 diplomatic decrypts in HW12 alone. But one has to start and stop somewhere, and there seems enough evidence of the importance of my father's wartime work in Bletchley and London, to stop here.

All these authors and researchers are concerned with the importance of signals intelligence in the conduct of foreign policy in peace and war. But not all historians share this view: in fact most of the fashionable historians of the 1990s consistently ignore the whole subject, and go for biographies of earlier statesmen and imperialists. Christopher Andrew regrets that the main streams on western historiography bypass his subject comprehensively. So do

I. But perhaps the loss is theirs, not ours. However, even the most sceptical investigative historian must note the appearance of intercepts on the desks of the highest in the land; before they could be used, new skills at GC&CS and elsewhere in cryptanalysis extended activities and expertise into the wider task of providing relevant messages, requiring detailed knowledge of the mindset of senders and recipients alike, the exact state of whatever emergency or situation is being targeted, the 'ministerial requirements' and their representation by officials, their occasional emergence as official jargon and disappearance when duly burnt after reading, their re-appearance in Parliamentary answers, in obscure references still lurking unweeded in Foreign Office files, or muttered at a diplomatic reception, or pillow talk between clandestine lovers.

Fact here may seem to merge into fiction, but the distribution of diplomatic intercepts throughout the chancelleries of many powers may suggest an interesting new angle on both the conduct and study of international diplomacy, both in war and in peace. Spy fiction is a vast field but only John le Carré understands the uses and abuses of diplomatic eavesdropping via signals intelligence.

Postcript

The McCormack visit to Bletchley Park and Berkeley Street in May 1943 marks the end of the currently available record of US/UK signals intelligence co-operation, though in fact such co-operation continued throughout the rest of the war, and beyond, through the whole cold war, and we must presume Arlington and GCHQ Cheltenham are still in daily communication as they strive to serve the security of their countries and the 'special relationship' with new targets, mostly of the anti-terrorism variety. This special relationship is the major theme of this monograph on my father's secret work from 1914 – 1945, as are the other principles for the good conduct of diplomatic eavesdropping on which my father instructed his colleagues, his superiors and his American counterparts, and which have all played continuing parts in the special relationship.

Whether the British public feel they have benefited from the Blair/Bush axis is not something for this monograph, but what needs remembering is that in 1939 there was no possibility of such relationship. The USA was bent on isolationism and keeping neutral, the British thought the Americans loud and vulgar and unreliable, but more intelligent views - those for instance of Winston Churchill - prevailed. My father's two transatlantic visits of 1941 totally changed his views of America and Americans. He had had no previous experience, had never visited the country, his political interests were all European, as were those of most in Whitehall. So the change, though slow to mature, started violently when America was dragged into the war by December 1941 and there has hardly been a harsh word ever since.

What my father would have thought between McCormack's visit in 1943 and his retirement two years later he certainly kept to himself. He was not a communicative man, even to his family and close friends. I hope he feels something like satisfaction, wherever he now is, that his remarkable contribution in changing the course of world history in 1916 and 1941 has been, however inadequately, acknowledged.

The influence of my father's work continued long after his retirement and is

still evident in the vital importance sigint has for the security services of the UK, the USA and a score of other developed nations, great and small. A leading sigint historian, Christopher Andrew, observed that while the main Japanese diplomatic cipher was broken and extensively publicised in the Pearl Harbor enquiry in 1946, only a few actually traced the origins of successful American sigint from Room 40 in WW1, which hastened American entry into the war, to British BP's success with Enigma and Ultra from 1941, which materially aided Allied victory in 1945. But the story not only does not stop there, it is only the beginning of a huge postwar international surveillance operation, sparked by BP and aided by an American discovery of a major Soviet spy network in the USA. A cryptanalyst called Meredith Gardener deciphered messages, known as 'Venona' which revealed the identity of 'Homer' as their most important agent, Donald Maclean. This was part of the unmasking.

The US/UK sigint alliance forged in WW2 meant that Clement Attlee, the British PM 1945-50, knew more about the achievements of postwar American cryptanalysts and Soviet espionage against the USA than the President.

Only 10 years earlier my father had facilitated this sigint superiority over his American counterparts by touring British universities looking for mathematicians and linguists to work for him at BP on the Enigma cipher. His long-term colleague Josh Cooper wrote after the war that it would be hard to exaggerate the importance of this recruiting drive for the future development of GC&CS, naming Gordon Welchman and Alan Turing as outstanding recruits. Later this work was overlooked but my father's critics 'did not realise that Denniston, for all his diminutive stature, was a bigger man than they'.

After the BP crisis of February 1942, and more sophisticated recruitment procedures, the numbers at BP increased in 1943 to over 5,000, in 1944 to 7,723 and by January 1945 to 8,995, after which GCHQ managed to escape from the control of 'C' and the even more frequent management problems of the whole SIS under Menzies. Throughout the Cold War GCHQ continued to service its customers in Whitehall and Washington. It was divided into five main directorates, moved house several times and still provides a valuable sigint service from what was, in the view of historians, the jewel in Britain's wartime intelligence crown.

After the war geopolitical concentration was on an increasingly hostile Soviet Union. GCHQ was relocated from Bletchley first to Eastcote in north London, and later to Cheltenham, and became an independent international surveillance operation separate from MI6, although still under Foreign Office control.

The Soviet nuclear bomb took all the western allies by surprise in late August 1949, and by that time the Soviets massively changed their codes and cipher security, eliminating most of the channels the west could read, including some machine-based mid-level military systems. GCHQ was thereupon directed towards Arab nationalism and later the Zionist movement, while Chinese and Soviet radio traffic was intercepted by its Australian counterpart as well as the British sigint centre in Hong Kong.

GCHQ's new interest in electronic intelligence and airborne sigint lasted throughout the 1950s and 1960s, partly because most high-grade ciphers, and OTPs, still remained unbreakable. But 'BJs' were still circulated to specific users in government in the same blue-jacketed files as they were in my father's day prewar, and make daily reading for all concerned with our national security.

At BP my father's sure touch in finding the best recruits bore further fruit when two BP veterans, Clive Loehnis and Leonard Hooper, were successively promoted to the top job, while it is estimated that in the Soviet Union 350,000 experts applied their minds to similar work breaking the ciphers, increasingly sophisticated, of the western allies, its former enemies, now uneasily becoming friendlier. Anglo-American sigint extended throughout the Cold War and into the Iraq war. By 2000 all GCHQ's activities were brought together on one site in Cheltenham - a vast new circular building with an open centre, and underground slip roads - the largest ever government private and public investment initiative costing £330 million to build and countless more millions to operate.

Any links between this vast new establishment at Cheltenham and the 100 or so cryptanalysts who manned BP in 1939 is beyond the scope of this monograph, and I doubt whether my father, at the ripe age of 125 would be much interested. But I hope he would approve of this attempt to link his 30 secret years with the 90 years in which British signals intelligence has proved such a valuable government tool, in peace as well as war.

---

* one time pads

List of Abbreviations and Terms

AGD	Alexander (Alastair) Guthrie Denniston.
BP	Bletchley Park, WW2 home of the Government Code and Cipher School, Britain's inter-Service code-breaking organisation.
BJ	Blue Jacket, diplomatic translation done by the GC&CS
C	Head of MI6
COS	Chief of War Staff
DID	Director of the Intelligence Division of the Naval Staff. Later renamed DNI
DNI	See DID
ENIGMA	German cipher machine.
FO	Foreign Office.
GC&CS	Government Code and Cipher School (now GCHQ).
GCHQ	Government Communications Headquarters.
JAC	Joint Analysis Centre.
JIC	Joint Intelligence Centre.
JIG	Joint Integration Group
MAGIC	The cover name for translations from Japanese diplomatic messages.
MI	Military Intelligence.
MI5	Department of British Security services responsible for counter-espionage within the UK.
MI6	The British Secret Service responsible for security and espionage services outside the UK.
PRO	Public Record Office, Kew, London (National Archives).
SIGINT	Signals Intelligence.
ULTRA	Cover name for intelligence derived from high-level cryptanalysis
WSC	Winston Spencer Churchill
WO	War Office
W/T	Wireless Telegraphy

Bibliography

Andrew, Christopher *Secret Service: The Making of the British Intelligence Community*. Heinemann 1985

Beesly, Patrick *Room 40: British Naval Intelligence 1914-18*. Hamish Hamilton 1982

Bennett, Ralph *Behind the Battle: Intelligence in the War against Germany*. Sinclair Stevenson 1994

Bryden, John *Best Kept Secret: Canadian Secret Intelligence in the Second World War*. Lester (Toronto) 1993

Cairncross, John *The Enigma Spy*. Century 1997

Calvocoressi, Peter *Top Secret Ultra*. Cassell 1980

Cave Brown, Anthony *Bodyguard of Lies*. Michael Joseph 1968

Clark, Ronald The Man Who Broke Purple. Little, Brown (Boston) 1977

Copeland, B. Jack (Ed.) *Colossus: The Secrets of Bletchley Park's Codebreaking Computers*. Oxford University Press 1997

Denniston, Robin *Churchill's Secret War*. Sutton 1997

ibid Yardley on Yap. Intelligence and National Security 9, no. 1 (1994)

ibid Three Kinds of Hero: Publishing the Memoirs of Secret Intelligence People: Intelligence and National Security 7, no. 2 (1992)

ibid Fetterlein and Others. Cryptologia Vol. 19, no. 1 (1995)

Erskine, Ralph (with Michael Smith) *Action This Day: Bletchley Park from the Breaking of the Enigma Code to the Birth of the Modern Computer*. Bantam Press 2001

ibid Churchill and the Start of the Ultra-Magic Deals. International Journal of Intelligence and Counterintelligence 10, no. 1 (1997).

ibid What did the Sinkov Mission receive from Bletchley Park? Cryptologia Vol. 27, no. 2 (2000)

ibid The Poles Reveal their Secrets: Alastair Denniston's Account of the July 1939 Meeting. Cryptologia Vol. 30, no.4 (2006)

Erskine, Ralph, & Freeman, Peter. *Brigadier John Tiltman: One of Britain's finest cryptologists*. Cryptologia Vol. 27, no.4 (2003)

Hinsley, F. H. (with Alan Stripp) *Codebreakers: The Inside Story of Bletchley Park*. Oxford University Press 1993

Irving, David *Churchill's War: Triumph in Adversity*. Focal Press 2001

Kozaczuk, Wladyslaw. *Enigma: How the German Machine Cipher Was Broken, and How It Was Read by the Allies in World War Two*; Warsaw, Ksiazkai Wiedza 1979

Lewin, Ronald *Ultra Goes to War*. Hutchinson 1979
ibid *The American Magic*. Hutchinson 1986
Smith, Bradley *The Ultra Magic Deals: the Codebreaker's War and the Most Secret Special Relationship 1940-6*. Praesidio (Novato) 1993
Smith, Michael *Station X: The Codebreakers of Bletchley Park*. Macmillan 1998
Welchman, Gordon *The Hut Six Story: Breaking the Enigma Codes*. McGraw Hill 1982
Winterbotham, F.W. *The Ultra Secret*. Weidenfeld and Nicolson 1973
West, Nigel *GCHQ: The Secret Wireless War 1900-86*. Weidenfeld and Nicolson 1986
ibid *MI6: British Secret Intelligence Service Operations 1909-45*. Weidenfeld and Nicolson 1973
Wright, Peter *Spycatcher*. Heinemann (Sydney) 1988

Documentary sources:

1. National Archives, Kew. HW1 series GC&CS Churchill files. HW3 series GC&CS official histories and personal memoirs. HW14 series GC&CS correspondence files.
2. National Archives, Washington
3. DENN 1-6 at Churchill College, Cambridge

VISAS

Thirty Secret Years eveals how an enterprising Scottish linguist was able to decipher German naval messages in the Admiralty in World War One. Alastair Denniston became head of the British government's *cabinet noir* or cipher-breaking bureau in 1919, developed his team of fellow experts between the wars by spying on the Soviets from Whitehall. In 1939 he went on to lead an enlarged body of secret service men and women to Bletchley Park where they solved the vast problems of machine encipherment, enabling Churchill to avoid defeat in 1941 and invade Western Europe in June 1944. It is the story of how one man, working in obscurity and total secrecy, influenced the course of world history over 30 years of war and peace, told by his son.

ISBN 978-09553648-0-8

ISBN 978-09553648-0-8

9 780955 364808

£9.95