The History of Communications Security in New Zealand
Part 1

By
Eric Morgon

Chapter 1
Early Days

"Admiralty to Britannia Wellington. Commence hostilities at once with Germany in accordance with War Standing Orders." This is an entry in the cypher log of HMS Philomel dated 5 August 1914.

HMS Philomel (Captain Hall Thompson RN) was a cruiser, third class of the Royal Navy and took part in the naval operations in the Dardanelles during the ill-fated Gallipoli campaign. Philomel's cypher logs covering the period 1914 to 1918 make interesting reading and show how codes and cyphers were used extensively by the Royal Navy during World War 1. New Zealand officers and ratings served on board Philomel and thus it can be claimed that the use of codes and cyphers by Philomel are part of the early history of communications security in New Zealand.

Immediately following the Admiralty cable to Navy Office, the Senior Naval Officer, New Zealand (SNO NZ) was advised that Cypher G and Cypher M had been compromised and that telegrams received by landline in these cyphers were to be recorded in Code C before transmission by Wireless Telegraphy (W/T). Apparently Cypher G was also used for cables between the Commonwealth Navy Board in Melbourne and the British Consul in Noumea. The Rear Admiral Commanding Her Majesty's Australian Fleet instructed that when signalling by W/T every odd numbered code group was to be a dummy.

It is interesting to note that up until the outbreak of hostilities, no provision had been made for the storage of code books or for precautions to prevent them falling into enemy hands. In October 1914 Admiralty gave instructions that a perforated metal box was to be prepared immediately in each ship for the stowage of confidential books and pamphlets in use in coding in the W/T office. The box was to be capable of being closed quickly and securely and code books were to be kept in the box except when actually in use. The instruction concluded with this sentence, "... The sinking power when full of books is to be tested on first opportunity." One wonders how literally this was interpreted by the ship's signals staff!

While in the South Pacific, Philomel read messages concerning the operation of the German warships Gneisenau, Nurnberg, Leipzig and in particular the Emden which was causing havoc among merchant shipping in the Pacific. When finally the Emden was chased and trapped in the Cocos Islands by HMS Sydney, W/T played an important part in the action. The signal, recorded in Philomel's cypher log on 9 November 1914 reads: "Emden located in Cocos Islands this morning 9 November. Chased and engaged by Sydney and beached herself to avoid sinking. Sydney casualties 2 men killed 13 wounded. Sydney standing

by wreck of Emden after having chased and sunk Emden's collier. Great credit attached to wireless telegraph operator at Cocos Island who stuck to his post and gave warning of Emden."

HMS Philomel reached Port Said on 2 February 1915 and shortly after was engaged in action off Alexandretta. On 10 February, as a result of a threat by the Turkish Military Commandant of Alexandretta to murder British hostages, Philomel was instructed to issue a grave warning to the Commandant that if murder was committed, his life and that of the Turkish Commander in Chief and all others concerned would "most assuredly be forfeit". Philomel was told to use Code C until further notice.

On 24 February, Allied Fleet Recognition Signals were brought into force and ships were advised that challenge and reply between ships of the Allied Squadron were always to be as laid down in the Allied Fleets Signal Book. On 23 March The W/T Code (1914) and Cypher D were brought into force. During this period Philomel's cypher log also makes mention of the Playfair Code being used to Troop Transports, the MV (Merchant Vessel) Code and the Economic Telegraph Code. The latter is presumed to be an unsecure code since HM ships were told not to use it unless the message had to be repeated to a French ship.

In 1915 Philomel was engaged in operations in the Persian Gulf. The codes and cyphers in use were Cypher X, the Economic Telegraph Code, Playfair Code and MV Code. The Fleet Signal Code Book 1915 had replaced the 1914 edition. A new General Service code was introduced in 1916 for communications with troop transports and merchant vessels. Cypher F was brought into force on the East Indies and Egypt Station in January 1916. It was in that cypher that Philomel reported that letters had been arriving to local ships from the German Consul in Kerman proclaiming the brotherhood of Germans and Turks in a holy war against England and calling upon all Mohammedans to join and drive the English out of Persia.

In March 1916 the Admiralty ordered Cypher F to be destroyed and Cypher X to be used instead until Cypher H was received. However, in July Cypher Q replaced Cypher X and Q was in turn replaced by Cypher S in November 1916. Other codes in use on the East India station were the Auxiliary Code No. 7, Aircraft Code No. 1 and of course the Playfair Code.

In January 1917 Philomel was overdue for a long and extensive refit and the Admiralty ordered her to return to New Zealand to pay off without recommissioning. Philomel left the Persian Gulf on 30 January 1917 and arrived in New Zealand on 16 March 1917. Three weeks later, on 7 April, her cypher log records the receipt of a signal from Admiralty advising that a declaration of war between the United States and Germany had been signed by President Wilson at 5 p.m. GMT on 6 April 1917. However, although Philomel was out of the war, her log continued to record changes in the codes and cyphers used during the remaining months of the war. By July 1918 Ship Cyphers H and N were in force and Cypher V was introduced on I October 1918. On 11 November 1918 a message in Cypher V from Admiralty advised SNO NZ that the Armistice had been signed. On 13 June 1919 General Cypher GA was and brought into force and messages from Admiralty in GA Cypher warned that hostilities would be resumed if Germany did not sign the Treaty of Peace. Germany finally signed on 28 June 1919 and only then was World War I formally terminated. If there was confirmation needed, the long awaited message was not encyphered but transmitted in plain language!

As we have already seen, the Playfair Code was used by the Royal Navy when communicating with troop transports. The first recorded use of Playfair in New Zealand Army documents is in a memorandum dated January 1917 from New Zealand Military Forces Headquarters in Wellington to Masters and Officers i/c Troops on board Transports en route to the war zone. The memorandum gives instructions that messages should be coded and despatched in Playfair code.

According to David Kahn in his book "Codebreakers", the Playfair code was first demonstrated in 1854. It was possibly used in the Boer War and was adopted by the British Army as a field system during World War 1. Twenty years later the Playfair code was still considered to be relatively secure and in February 1941 the New Zealand War Cabinet approved the use of Playfair to secure commercial messages sent by wireless between New Zealand and the Pacific Islands. In September 1945 the Playfair code was withdrawn and replaced by a one-time pad system, almost one hundred years after it was first demonstrated.

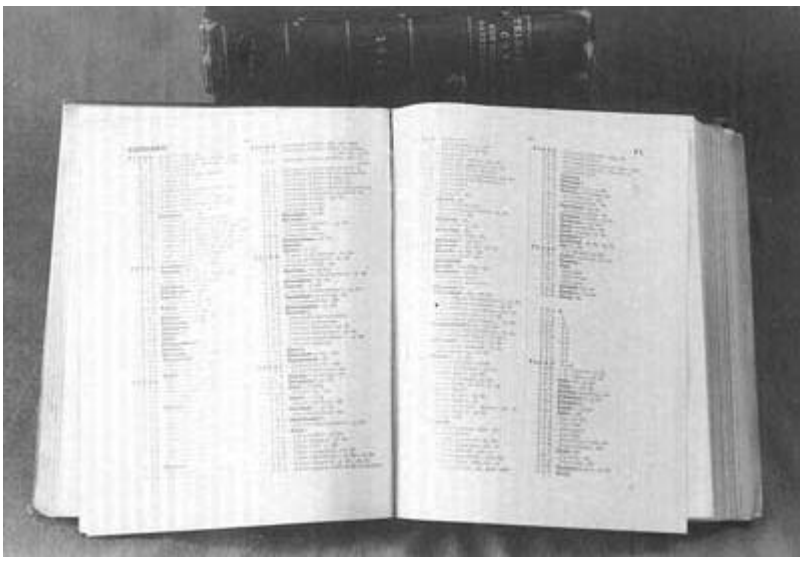
But to return to the period before World War 2. During these early pre-war days, secure book cyphers were used by the military forces and government departments. Naval cypher logs covering the period 1927 to 1929 show that the Navy Office, Wellington held a General Cypher, the Interdepartmental Cypher, a Small Ships Cypher, Flag Officers Cypher used for messages to and from Admiralty, a Reporting Officers Cypher, a Peace Code and a Fleet Code. Recyphering tables changed on a regular basis were used with most cypher systems. In 1929, copies of the Colonial cypher were loaned by the British High Commission in Government House, Wellington to the Department of External Affairs for confidential despatches between Wellington and Samoa. In 1934 Admiralty issued a new cypher "Admiralty Cypher No. 1" and a new code "Administrative Code" to replace the General Cypher and Fleet Code Volume 2. The Administrative Code was not recoded for

unclassified messages but was to be recoded with special tables for Secret or Confidential messages. By 1938, copies of the Interdepartmental cypher and the associated recyphering tables were held by the Governor General, the Prime Minister, Navy Office, Army and Air Force Headquarters, Wellington.

It was during these early years that the idea of national control of codes and cyphers originated. In 1920 an advisory committee on Defence was formed to report confidentially to the Minister of Defence on problems of defence and important policy questions. However, it was not until 1933 that the New Zealand Committee of Imperial Defence (NZCID) was set up to organise national activities so that all departments of state were in a position to deal immediately and effectively with duties which could develop on the threat of war or actual outbreak of hostilities.

In 1936 the NZCID was retitled the Organisation of National Security (ONS) to avoid confusion with the Committee of Imperial Defence in England. The co-ordination of defence activities, was effected by the ONS by means of inter-departmental committees, one of which was the War Book Committee. It was at a meeting of this committee in February 1939 that it was decided to form a special sub committee to consider the question of the supply of cyphers.

Only a few months previously, the ONS had expressed concern that the existing cypher staffs of Government House and the Prime Minister's Department would be insufficient in an emergency. During September and October 1938 Navy Office conducted cypher training for 11 officers from the Posts and Telegraph Department, Air Department, Navy Office and the British Trade Commissioners Office. By this time an Administrative Code and Cypher had been introduced and on the same date (1 February 1937) the Peace Code had been withdrawn. Navy Office therefore provided instruction on the Government Telegraph Code, Administrative Code, Administrative Cypher, Interdepartmental Cypher, Reporting Officers Code and Reporting Officers Cypher. In addition, Naval Office staff were given instruction in Naval Cypher, Interservice Stencil Cypher and RAF Station Cypher. The last named cypher, both low grade and high grade, was used between Navy Office and RAF authorities for messages concerning the Walrus aircraft which operated from HMS Achilles.



The Telegraph Code of 1911 used by the New Zealand Government

At the first meeting of the special sub committee on cyphers in February 1939 it was agreed that there should be a central cypher pool for handling all outward Government telegrams excepting those of the three fighting services. As practically all messages were required to emanate over the signature of the Prime Minister, it was considered that the cypher pool should be attached to the Prime Minister's Department. The cyphers to be used would be either the Dominions Office Cypher... 'which is moderately secure"... or the Interdepartmental Cypher... 'which is absolutely secure". The Post and Telegraph Department agreed to release a further 8 officers to be trained in the use of various cyphers employed by the Navy Office and Government House. It was felt that those officers selected for cypher training should be "... about twenty years of age with a good knowledge of English, smart at figuring and of a superior personality..." It is no wonder that ever since that time, cypher staffs have considered themselves to be 'superior beings'!

The War Book Committee continued to function throughout the war but there is no further record of the cypher sub committee. The move to form a national committee responsible for cypher security did not come until after the war but interestingly enough, the first Chairman of the committee was a member of the War Book Secretariat. (See Chapter 4.)

On the 27th September 1938, during the Czechoslovakian crisis, a message was received in Flag Officers Cypher from the Admiralty giving advance warning of possible general mobilisation being ordered the following day (28th) as a precautionary measure against Germany. On the 28th two further Immediate telegrams were received from Admiralty in cypher. The first one gave the codeword SERVICE and the second STROKE MAST. The significance of the first telegram was "Mobilise in accordance with instructions for war with a European Power". The second telegram meant "Mobilise Naval Reserves. Retain Time Expired men". The following day Navy Office signalled Commodore Commanding the New Zealand Squadron (CCNZS) with the codeword SUSPEND which signified "The discharge of Imperial ratings in the NZ Squadron is suspended. NZ ratings permitted to take discharge until promulgation of a state of emergency when message PROCLAMATION will be sent signifying that the discharge of time expired NZ ratings is suspended". The same day Admiralty signalled Navy Office in Naval Cypher (which was handled only by officers) with the information that Lloyds had reported that all German shipping lines had recalled all their vessels on the high seas. German W/T stations broadcast the recall to merchant ships using the prefix BLIND which meant that the ship did not answer.

As we know, the British Prime Minister, Neville Chamberlain returned from a meeting with Hitler in Munich with the message "Peace with Honour". The Czechoslovakian crisis had been averted. On 5 October Admiralty signalled Wellington in Administrative Cypher that the international situation was generally stable but the mobilisation of the British Fleet would continue on account of the experience gained to all concerned. A further signal encyphered in Flag Officers Cypher advised CCNZS that the he could retain any officers called up locally until they could be spared. The remainder could be released but should remain liable to recall should the necessity again arise. Finally on 25 November the state of emergency was formally terminated and the order to mobilise was suspended.

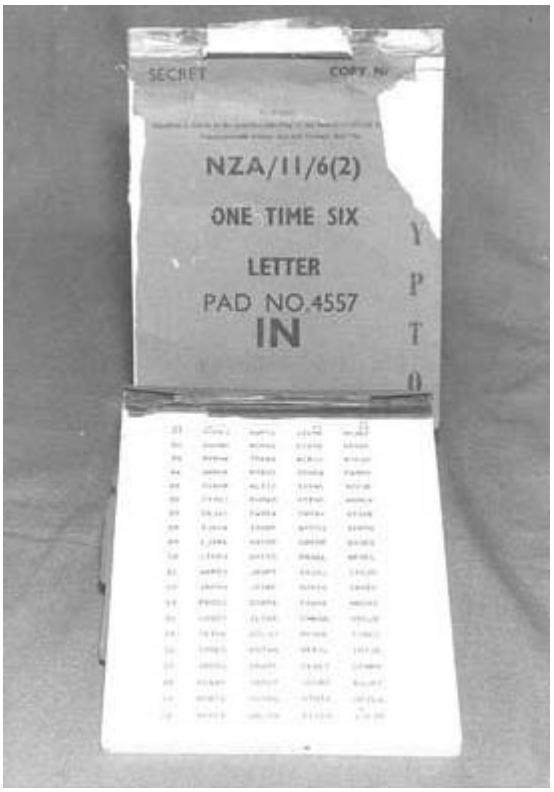
Although the immediate threat of war had been averted, the Admiralty continued to make preparations to improve communications security in time of war. In April 1939 they advised the Governor General, Viscount Galway, that arrangements were being made to provide British merchant ships with secret W/T callsigns for use when rendering certain reports or when confidential official messages are addressed to particular merchant ships. It was considered preferable to issue these callsigns in time of peace to avoid the delay that would occur in issuing them on the outbreak of hostilities. Each individual callsign together with instructions for its use was to be placed in a double sealed envelope marked "Secret Envelope Z". The authority to open Secret Envelope Z and bring the secret callsign into force was broadcast by W/T as an Admiralty message "B" which contained Wireless Instructions Nos. 1 and 2 and instructions to open the envelope. Secret callsigns were to be used for reporting enemy warships, enemy aircraft, or of a moored mine cut by a paravane. They were to be used for messages coded in Merchant Navy Code and for cancelling a false report of a submarine. Navy Office Wellington adopted this procedure and secret callsigns were used by merchant ships registered in New Zealand. Secret envelopes Z were issued by Navy Office to ships operating in New Zealand coastal waters and throughout the Pacific.

Chapter 2
Codes and Cyphers in World War 2

When the war started New Zealand was still using book cyphers which had hardly changed since World War 1. Not only was the Playfair code in use in the Pacific Islands but in July 1940 the Ministry of Supply authorised New Zealand Trade Commissioners abroad to use Bentley's Second Phrase code if it was considered indiscreet or expensive to despatch messages in clear. The Playfair code was to be reserved for secret messages! In March 1941 the War Cabinet issued an instruction that all commercial messages sent by Wireless Telegraphy, (W/T) to or from the Chathams, Niue, Raratonga, and the Kermadec Islands should be encoded in the Playfair code. The use of commercial codes such as the Government Telegraph Code and Bentley's code was cancelled and smaller islands were instructed to use the native language when no codes were available. Considerable precautions were taken to preserve the security of the Playfair code and as many as 100 different key words were used and regularly changed. Navy Office continued to use the more secure Interdepartmental Cypher for secret messages between New Zealand and certain authorities such as the Resident Naval Officer Suva and the High Commissioner Suva and to Army and Navy Offices in Melbourne.

The Playfair code was also used extensively by the coastwatching stations in the Pacific. In November 1942 Navy Office advised the New Zealand Naval Liaison Officer in Suva that it was certain that the Japanese were aware of the type of code in use for communications with British coastwatching stations in the Pacific as well as the W/T frequencies used. It was considered that even with frequent changes of keywords, no message sent in Playfair code was secure for more than a few hours at the most. Therefore to deny the enemy of even the smallest amount of information, messages should not be transmitted to coastwatching stations except in exceptional circumstances, other than short innocuous words such as YES, NO, CONCUR etc.

In June 1945 the Joint Communications Board came to the conclusion, which was confirmed by the Chiefs of Staff, that it would be impracticable to discontinue the use of codes altogether at that stage of the war. The Board decided that in view of the limited security value of the Playfair code it should be replaced by a more secure code and that a one-time letter code should be made available. The Navy view was that the transmitters in use at Wellington, Chathams, Niue, Raratonga, Apia and the Kermadecs were of sufficient power for their transmissions to be picked up in Japan but that the transmitters of the outstations centering on Apia and Raratonga were not. It was therefore decided to withdraw Playfair code from all islands and provide the islands which used high-powered transmitters with both IN and OUT pads of one-time letter code. The minor stations were to be provided with IN pads only for the receipt of traffic. The use of codes for commercial traffic was considered no longer necessary.



One-time Figure Pad as used by the New Zealand Army

More secure cyphers were used by the fighting services. As we saw in Chapter 1, secure book cypher systems were in use by Navy Office and the Commodore Commanding the New Zealand Squadron before the war. In April 1940, General Freyberg, Commander of the New Zealand Expeditionary Forces in Egypt was supplied with the Interdepartmental Cypher to allow direct secret communications with the New Zealand Government in Wellington without the necessity of despatching messages through Army Headquarters. The 1936 edition of the Interdepartmental cypher was at this time held by the Governor General, Viscount Galway who received his copies from the Dominions Office in London. In May 1940 the Commodore Commanding the New Zealand Naval Squadron was receiving copies of the Naval Cypher, the Administrative Code, Auxiliary Code and the Merchant Navy Code. By the end of 1940'one-time' pad subtractor recyphering tables were in use with figure cyphers. Subtractor tables consisting of numbered IN tables and correspondingly numbered OUT tables were intended for single line communications either for vulnerable posts or for any special purpose for which added security was considered essential. In December 1940 when Naval staff was considering distributing these tables to Pacific Islands, one staff officer commented "... our coding and cyphering systems seem to be coming more complicated every day".

While the book cyphers and subtractor tables employed by the services and government departments were certainly more secure than Playfair code or Bentley's Second Phrase Code, nevertheless they were time-consuming in use and prone to arithmetical error. In addition, the system suffered from a primary disadvantage in that if any one set of code books was captured or compromised new sets had to be issued to all users, and in wartime that could be a very lengthy procedure.

With the benefit of hindsight we know that most of these codes and cyphers were already compromised before they were received in New Zealand. The Administrative Code had been used before the war both with, and without, the subtractor tables and this had enabled the German naval B-Dienst to break the code and its tables. By the outbreak of war the Germans were reading traffic in this system extensively. Success with the Administrative Code enabled B-Dienst to break the Naval Cypher and by April 1940 they were reading 30 to 50 percent of intercepted traffic. On 20 August 1940 Naval Cypher No. 2 replaced Naval Cypher No. I and on the same date Naval Code No. I replaced the Administrative Code. Because of improvements to the security of the long subtractor system, B-Dienst's success against Naval Cypher No. 2 was comparatively limited but in September 1941 an indicator procedure was abandoned for a much weaker one. From then until January 1942 when Cypher No. 4 replaced No. 2, B-Dienst again succeeded in reading a good deal of traffic in generally held tables. Fortunately by October 1942 Naval Cypher No. 4 had been reconstructed to an extent that the enemy was unable to achieve results comparable to its success against the previous No. 1 and No. 2 cyphers.

While it is not part of the New Zealand story, it is worth noting that Naval Cypher No. 3 was employed by the British, US and Canadian Navies in the Atlantic. To begin with it was used without the improvements to the long subtractor tables which had been applied to Cyphers No. 2 and No. 4. As a result the enemy was sometimes obtaining decrypts about convoy movements between 10 and 20 hours in advance and was able to decrypt the daily signal in which the Admiralty issued its estimate of U-boat dispositions. From November 1943 the Naval Cypher was being progressively replaced for British/Canadian/US communications in the Atlantic with the Combined Cypher Machine (CCM) against which the enemy made no progress.

The Merchant Navy Code, which was also held by the Commodore Commanding the New Zealand Naval Squadron, was a simple recoding system. By March 1940 B-Dienst was having some success in decrypting this system and it was greatly helped by the capture of copies of the Merchant Navy Code at Bergen in May 1940 after which it was able to read the bulk of the traffic with little delay. Reading the Merchant Navy Code was of substantial assistance to B-Dienst's work on Naval Cypher No. 3 since it contained intelligence about convoys and stragglers.

The Inter-departmental Cypher issued to General Freyberg in April 1940 was also compromised. A basic book with subtractor tables, it was held by the British Foreign Service, the Colonial, Dominions and India Offices and the British services. The Germans captured the basic book at Bergen in the summer of 1940 and soon broke the system. Until June 1943 when the Germans stopped work on it, it provided valuable political intelligence and information about merchant shipping. It is not known whether the Germans ever intercepted General Freyberg's messages but certainly if they had, the information they contained would have been compromised.

The story of' Enigma' and the introduction of machine cypher systems is well documented in other histories concerning codes and cyphers but its connection with the Typex system used by the New Zealand Government is worth recording here. Enigma was adopted by the German Navy in 1926, by the German Army in 1928 and by the Luftwaffe in 1934. The British were also considering the replacement of book systems by cypher machines and in 1928 two commercial Enigma machines were purchased at Admiralty initiative. It was not until 1935 however, that it was decided that Air Ministry should arrange for the construction of three

sets of cypher machines of an improved "Enigma" type. Air Ministry commissioned Creed & Company, a commercial teleprinter manufacturer to produce copies of the commercial Enigma. By March 1936 Creeds had made two copies which became known as the RAF Enigma with Type X attachments and subsequently as 'Typex'. The Air Ministry adopted Typex before the outbreak of war and by September 1939 it was in use at all RAF HQs. It proved to be completely secure for more important RAF ground-to-ground communications throughout the war. British War Office adopted Typex before the war and by September 1939 this system, which remained secure throughout the war, was in use between the War Office and commands, at home and overseas and within commands down to division level.

Typex was not used at sea by the Royal Navy during the war but the Combined Cypher Machine (CCM) was used from November 1943 and it was eventually held by all HM ships. CCM was based on the US Electrical Cypher Machine (ECM) and the British Typex machine which had been made available to the US on their entry into the war. By an agreement in June 1942 the US undertook to modify the ECM to work with Typex and develop an adaptor for the latter. The modified ECM and Typex machines became different marks of the CCM. Like Typex, CCM proved to be totally secure and the Germans made no serious attempt to solve either system.

A German Navy Enigma Machine of the type used by
German Raiders against New Zealand shipping in the Pacific

By April 1941 Typex had been adopted by service departments in Canada and the Union of South Africa and was being considered by Australia. Ten Typex machines were supplied by the British government for use by New Zealand government authorities nominally without charge, but in the event the New Zealand government insisted on payment and the cost of 145 pounds for each machine was finally paid in 1947. In June 1941 the Navy Department, with the concurrence of Admiralty, made one machine available on loan to the Prime Minister's Department. In December of that year, Air Department assumed responsibility for the inspection and maintenance of all Typex machines used by service departments, the Prime Minister's department and the United Kingdom High Commissioner's Office. In January 1942 Typex communications were established between the Prime Minister's Department and the Secretary of State for Dominion Affairs in London. In May of that year special Dominion drums and settings were held by the Prime Minister's departments in New Zealand and Australia, the Department of External Affairs in Canada and the Union of South Africa, the Governors of Newfoundland and of Southern Rhodesia and the United Kingdom High Commissioners in Australia, New Zealand, Canada and the Union of South Africa.

Typex machines remained in service in New Zealand after the war until they were replaced by modern machine systems. The RNZAF destroyed Typex in 1963 but the last machines in use by the Ministry of Foreign Affairs were dumped at sea some ten years later. An ignominious end after over 30 years of loyal service! Fortunately one was salvaged and is held in GCSB archives for future display in a museum of cryptology.

Chapter 3
The Post War Years: 1945-1960

The end of hostilities in Europe and the Pacific found the New Zealand services and government departments using a mixture of machine and book cypher systems. The Navy and Army were using the Combined Cypher Machine (CCM) which was a Typex Mark 2 machine adapted for and held with special adaptors to enable the New Zealand forces to operate with American services. The Air Force and the Department of External Affairs were both using Typex. On I January 1950 Typex Mark 2 and Mark 3 were superseded by the Mark 22 and 23 (BID/08/2 and BID/08/3) the latter being a Mark 22 modified for use with the CCM adaptor. Both these models were fitted with the crossover device which provided additional security. The crossover consisted of a base plate fastened to the right hand side of the Typex containing a plugboard with 26 Ieads lettered A to Z which could be plugged into a lettered hole in accordance with a settings key which was changed at set intervals.

TYPEX Mark 22 (BID/08/2) fitted with the crossover device for extra security

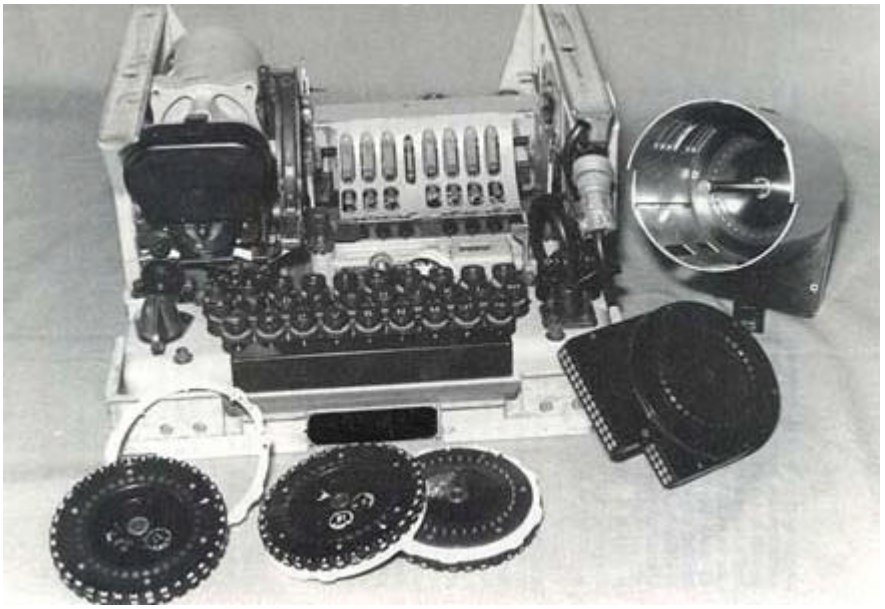
The need to reorganise the signals staffs of the military forces in keeping with a peacetime establishment now became necessary. In 1942 the cypher staff in Army Headquarters, Wellington consisted of two officers and eleven female civilians who were enlisted into the WAAC the following year. In September 1944 the staff numbered twenty but by November 1946 it had been reduced to three.

The Air Force determined that both mechanical and book cypher systems would be held at Air Department, Group Headquarters and on flying stations although it was considered that little cypher activity would occur at stations in New Zealand. Cypher duties were performed by signals officers assisted by the senior signals NCO, WRNZAF officers were employed in the Secret and Confidential documents section of the Air Force signals directorate (S5) and in the signals distribution and cypher sections. Flight Officer M. C. Middleton was appointed Cyphers 1 in the Directorate, a post she held until her retirement in 1958.

The post war years saw the replacement of many cypher systems that had been used continuously throughout the war and either the systems themselves had become less secure or the machines had become worn out and parts were hard to replace. In 1948 the British Admiralty decided that the Stencil Subtractor System could not remain secure if it were to be exposed to a rapid rise in traffic in an emergency and until a replacement system could be found, double subtraction appeared to be the only acceptable solution. Luckily the Stencil Frame system was purely a stand-by system and its use was fairly limited. A more fortunate change was the decision to withdraw the CCM machine which in the early fifties was the N.A.T.O. off-line machine cypher system. The replacement was an American-built machine, the AFSAM 7 (later retitled KL-7) which was released to N.A.T.O. nations plus Australia and New Zealand.

The KL-7 was a small lightweight (20 lb) electromechanical, keyboard operated cypher machine which encyphered and decyphered at a rate of approximately 60 wpm. The encrypted message was printed out on gummed paper tape in five letter groups and the decrypted message was printed out in clear text. The gummed tape was then affixed to a message form for transmission or delivery to the recipient as appropriate. The cryptographic principle used with the KL-7 was the ADONIS system which was brought into force with Commonwealth navies on I July 1956. In typical Navy fashion the signal from Admiralty quoted biblical verse.

"TYPEX. 2 Timothy Chapter 4 verses 6-7. ADONIS. John Chapter 14 Verse 15". Translated the verses are appropriate to the demise of Typex and the introduction of KL-7. Thus: 2 Timothy. "For I am already being offered and the time of my departure is come. I have fought the good fight, I have finished the course, I have kept the faith". John 14 reads "If you love me you will keep my commandment".



The KL-7 Electro-Mechanical Cypher Machine used by the New Zealand services.

On the same date a number of other changes were made by Admiralty. The Stencil Subtractor System was abolished as was the Admiralty and Naval Stations One Time Pads. A Commonwealth Naval Edition of the Britex system (the British version of Natex) was introduced for use between the RN and Commonwealth navies and a single basic book, the Inter Departmental Basic Book, was adopted for all purposes.

Although the use of one-time pad systems was discontinued in the New Zealand Navy, they were maintained by the Air Force and by the Department of External Affairs. Also a number of Typex Mark 23 machines were transferred from the RNZN to the RNZAF and the Departmental of External Affairs. RNZAF holdings of codes and crypto systems in 1958 included Typex MK 23, One time Pad, Stencil Subtractor, Britex and Natex systems, the Colonial Defence Code as well as the KL-7. At the end of the fifties the New Zealand Army had no cypher system in use in the field. An equipment called 5 UCO was installed in Army Headquarters and provided on-line encryption on the teleprinter channel between Wellington and Canberra. The RNZN also had three 5 UCO machines installed in Navy Office, Wellington for operation with HMAS Harman in Australia but this circuit did not come into effect until later in 1960.

Chapter 4
The Growth of Communications Security in Government

The first move towards the formation of a national body charged with responsibility for communications security in New Zealand came during the war years when in August 1943 the Secretary of State for Dominion Affairs in London wrote to the Minister of External Affairs in Wellington. In his letter the Secretary of State advised the Minister of the existence and responsibilities of the United Kingdom Cypher Security Committee and asked whether similar measures had been taken by the New Zealand Government and whether it had any cypher security problems which could brought before the London Committee. After seeking the views of the three services, the Minister of External Affairs replied that as all cyphers used by New Zealand were received from British sources and as the accompanying security instructions were strictly observed, it was considered unnecessary to set up a local New Zealand cypher security committee.

In May 1946 the British Government tried again to awaken the Government of New Zealand to an awareness of communications security. On this occasion it was the UK Cypher Policy Board that wrote to the Department of External Affairs through the UK High Commission in Wellington. The letter stressed the importance of communications security and the need to have a fully co-ordinated policy and practice in respect of cypher matters among all government departments. The Policy Board said they would welcome assurances that their views were shared by Dominion Governments and asked for details of any comparable Commonwealth organisation.

On 31 July 1946 a meeting was held in the Prime Minister's Department. The members present at that meeting were, Mr Foss Shanahan, Acting Permanent Head of Prime Minister's Department in the Chair, Squadron Leader C. C. Turner, Director of Signals, Air Department (later to become Air Vice Marshall Turner, Chief of Air Staff), Major R. W. Foubister, Chief Signals Officer, Army Department, Lt Cdr Foster, Senior Signals Officer, Navy Department, Mr G. R. Laking, Prime Minister's Department (later Sir George Laking, Chief Ombudsman), and Mr P. A. Orr, Cypher Officer. Mr Shanahan said that while he was in the UK he had been approached by the Secretary of the UK Cypher Policy Board with the suggestion that a similar body be established in New Zealand to co-ordinate cypher policy and to provide a channel of communication with the UK Board.

The British cypher organisation by this time consisted of a Cypher Policy Board, a Cypher Security Committee and a Cypher Machine Development Committee. The New Zealand meeting considered there was no necessity for a similar Cypher Policy Board nor was there a need for a Cypher Development Committee. However, they recommended that a Cypher Security Committee should be established with functions comparable with those of the UK Committee plus the responsibility to co-ordinate security and other arrangements for the use of cyphers in New Zealand and in the Island Territories under New Zealand control. They further recommended that the committee be established in the Prime Minister's Department and that it comprise the Permanent Head of that Department as Chairman plus the senior signals officers of the three services. These recommendations were forwarded to the Prime Minister in September 1946. However, in September 1949, the Prime Minister's Office, in replying to a query from the Joint Intelligence Committee, noted that no actual approval from the Prime Minister to the recommendations made three years earlier could be found but that the Cypher Security Committee was established and operating although it had never met. Matters were apparently considered by the committee by an exchange of correspondence.

Following this discovery, a more positive approach was taken and the first meeting of the New Zealand Cypher Security Committee (NZCSC), was held on 3 May 1950 under the Chairmanship of Dr R. A. Lochore from the War Book Secretariat of the Prime Minister's Department. Present at that first meeting were Lt Cdr R. A. H. Panter, Director of Navy Signals, Maj J. E. Anderson, Director of Army Signals, Wg Cdr R. J. Gibbs, Director of Signals RNZAF and Lt Cot B. R. Bullot of the Prime Minister's Department as Secretary. Mr P. A. Orr, a Communications Officer from the Prime Minister's Department was also present. Items discussed at that meeting included the Terms of Reference of the Committee and its composition, the clearance of telegrams paraphrased for war history purposes, the storage of Typex MK 22 equipment, the reporting of compromises and papers received from the Australian Communications Electronic Security Committee.

In December 1950 Air Staff agreed to provide the secretariat for the committee and Flight Officer Middleton served as Secretary until August 1958 when she retired and Flt Lt Broomhead was appointed. Liaison with overseas cypher committees was conducted by Chairman to Chairman correspondence. This latter appointment changed with staff movements in the Prime Minister's Office. In October 1956 Mr M. P. Chapman replaced Dr Lochore as Chairman and Chapman was replaced by Mr J. C. Templeton in March 1961. Mr R. L. Hutchens assumed the Chairmanship in 1963 and he was followed by Mr R. J. Lawrence in 1965. In July 1966 the committee was retitled the New Zealand Communications Security Committee and the Defence Secretariat transferred from the Prime Minister's Department to the Defence Office on the Formation

of the Ministry of Defence. In 1968 Mr I. K. McGregor was appointed Chairman but no replacement was found for him in late 1971 when he was transferred.

The committee did not meet again until September 1974 when as a result of concern expressed by both the UK and the Australian cypher committees (see Chapter 9), a meeting was arranged by Group Captain R. Thorpe, Director of Defence Communications and chaired by Mr B. R. Finney of the Prime Minister's Department. Following Finney's departure overseas in 1975, Mr Peter Bennett served briefly as Chairman and he was replaced by Hugo Judd who was the last Chairman of the NZCSC. It was Hugo Judd who chaired the meeting in November 1976 at which the Tovey/Rushen Report was presented to senior government officials. This report resulted in the establishment in 1977 of a national communications security authority, the Government Communications Security Bureau (GCSB) whose Director, Mr C. M. Hanson became Chairman of the newly formed Government Communications Security Committee (GCSC) which replaced the NZCSC. This is covered more fully in Chapter 9.