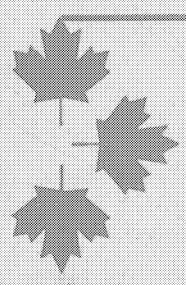
CSE ATIP A-2015-00045

History of CBNRC
Volume IV - COMSEC
N.K. O'Neill, August 1987

29



HISTORY OF CBNRC

VOLUME IV

THIS DOCUMENT CONTAINS CODEWORD MATERIAL

WARNING

THIS DOCUMENT IS

CANADIAN EYES ONLY

IN ITS ENTIRETY

HISTORY OF CBNRC

VOLUME IV

N.K. O'Neill

K.J. Hughes

AUGUST 1987

HISTORY OF CBNRC

VOLUME IV

COMMUNICATIONS & BASIC COMSEC

Chapter 14

Communications

Chapter 14 (cont'd)

Annexes:		**Para.**
SIGINT Communications	1947	14.A
SIGINT Communications	1949	14.B
Circuits into CBNRC	1950	14.C
Atlantic Communications	1952	14.D
Canadian Circuits	1957	14.E
SIGINT Communications	1963	14.F
CBNRC Traffic Load	1955-1967	14.G
SIGINT Communications	1968	14.H
SIGINT Communications	1971	14.I

CHAPTER 14 - Communications

Original Organization

14.1 As detailed in Chapter 1, preparations were underway in summer 1946 to set up a postwar establishment with the transfer of staff from the wartime Examination Unit (XU) and Joint Discrimination Unit (JDU) to the new organization, first called the Communications Research Centre (CRC) and later the Communications Branch of the National Research Council (CBNRC).

14.2 The new Centre was initially to consist of a Production Group and two Sections: Intelligence and Communications[1]. An extract from the Minutes of the Tenth Meeting of the JDU Staff Committee of 13 May 1946 describes the setting up of the Communications Section:

> "Lt. A.E. Parsons was selected to start organizing this section which will comprise the following subsections:
>
> 1. Station Control and Traffic Analysis
> 2. Cipher Office
> 3. Teletype Office
>
> Colonel Drake stated that this section will be required to compile and keep up-to-date Traffic Analysis (T/A) data on all communications which may be required for SIGINT purposes. In addition this section will carry out T/A work as required by the Production Group and as necessary to efficiently control the Canadian intercept stations. Other duties such as liaison with the Services on all matters of technical equipment, intercept tasks, training of operators, communications, etc. will be carried out by this section."

1. See para. 3.3

14.3 Lt. Parsons was succeeded in August 1946 by John D. Manson who continued to head up that part of the organization, as it progressed from Section to Group status, until his death in August, 1952.

14.4 This Chapter will be concerned only with the History of the "Communications Centre" - the teletype and cipher offices.

Basic Requirements

14.5 On 7 August 1946 Mr. Drake, as Director of the Communications Research Centre, (the following month it was renamed CBNRC) wrote a letter to the Chairman of the Communication Research Committee (CRC) stating the communications requirements for Signals Intelligence in Canada. He pointed out that

> "highly efficient communications are essential for the satisfactory functioning of the Signal Intelligence Service". He went on to say "a successful and profitable SIGINT effort could not be achieved unless it is backed by a flexible and efficient network of communications between the SIGINT Centres agreeing to coordinate their efforts and between each Centre and the intercept stations controlled by it". He added: "inadequate communications, on the other hand, result in poor control of the manpower used in the Centres and the intercept stations. The intercept station has to be dependent on the SIGINT Centre for all its assignments and technical information required to discharge such assignments. Since the assignments and the corresponding information change continuously, the operator personnel would be used uneconomically and valuable receiver hours wasted unless the necessary changes could be passed to them by the fastest telecommunications. It is safe to state that a station with a given number of intercept positions served by poor communications is less efficient than a station with half the number of positions

served by first class communications, through which rapid, sensitive and comprehensive control could be exercised."

14.6 Commonwealth and BRUSA Conferences held in London, England, during February and March, 1946[2], had addressed the subject of communications for SIGINT service and recommended that (a) provision be made for exclusive and readily extensible telecommunications between Centres and between the Centres and their outlying stations, and (b) each Centre should have operational but not necessarily administrative control of all SIGINT communications in its area.

Location and Control

14.7 The UK and US SIGINT Centres had complete operational control of their communications although administrative control was handled by the Signal authorities of their Military Services; and the communications terminals of all their SIGINT circuits were located in the Centres. Mr. Drake made a case for a similar arrangement and the same control over communications "to enable the Canadian SIGINT Centre to coordinate efficiently its interception and cryptographic assignments with the London and Washington SIGINT Centres".

14.8 As related in Chapter 2.3, the Chiefs of Staff Committee in August 1944 had approved "in principle" that three Army and three Navy intercept stations should continue to be maintained in peacetime. At their 345th Meeting on 15 March 1946 the Committee noted a recommendation by the Joint Intelligence Committee (JIC) "that the maintenance of postwar intercept facilities be a joint Service responsibility and be undertaken on an adequate scale in relation to the operations of the United States and other Commonwealth countries".

2. See para. 11.13

14.9 There followed then a protracted struggle to have communications facilities established between CBNRC and the intercept stations with terminals located in CB. Mr. Drake requested that the Service Departments, responsible for the provision of intercept stations, provide teletype landline or equivalent telecommunications service from the stations to CBNRC[3]. He said it had been proven necessary to terminate the circuits in the SIGINT Centre in order to maintain a sensitive and efficient coverage control over the intercept stations. Moreover, he pointed out that the intercepted material had to be retransmitted to other Centres after it passed through a sorting and discriminating process at CBNRC.

14.10 Mr. Drake suggested that traffic from two or even three stations could be handled on one landline channel by using high-speed automatic transmission and connecting the stations in one area into the common long distance line. He asked that the Services provide the terminal equipment at the intercept stations and at CBNRC, and the communications and cipher personnel at the stations, while CBNRC would provide staff for its own cipher and teletype offices.

14.11 Reluctance on the part of the Services to provide communications from the stations with terminals at CB is perhaps understandable since the SIGINT authorities wanted the circuits used exclusively for SIGINT traffic, or at least mainly for SIGINT and only, where absolutely necessary, for Service administrative communications. Thus the Services were being asked to provide all the facilities at the intercept stations, the communications circuits, the terminal equipment at CBNRC, and to pay all the costs, but were to be allowed little or no use of the circuits and were to surrender control over the intercept stations, at least operationally. Mr. Drake wrote to the Director GCHQ on 9 September 1946 "the Services were loathe to

3. See end of para. 5.2

let a civilian organization write to a Service intercept station and tell them what to do".

14.12 On 22 August 1946, at its 7th Meeting, the CR Committee approved the arrangement whereby CBNRC would exercise assignment control over the Canadian intercept stations and be provided with the necessary communications[4]. A month later, on 25 September, the Acting Chairman CRC wrote to the Chiefs of Staff Committee recommending "establishment of telecommunications between Canadian intercept stations and the offices of the Communications Branch, National Research Council (Canadian SIGINT Centre)".

Provision of Initial Circuits

14.13 One of the main reasons for delay in providing the circuits from the intercept stations to CB was that the stations themselves were in a somewhat disorganized state. Staff shortages were general as a result of demobilizaton, equipment was in need of replacement and several of the stations were due to be rebuilt or transferred to other sites. The Chairman CRC recommended on 21 October 1946 to the Chiefs of Staff Committee that they "expedite the building and equipping of the RCAF station in the Whitehorse area, the Navy station in the Churchill area and the new Army station in the Vancouver area which will replace the two existing Special Wireless Stations at Victoria, B.C., and Grande Prairie, Alberta"[5].

14.14 The CRC Chairman went on to point out that these recommendations should be dealt with in the immediate future whatever happened to the stated requirements for telecommunications and Direction Finding (D/F) positions "since a decision in regard to these two (latter) questions is not essential to the implementation of the intercept program". And so it was that the installation of circuits to CB from the stations was not considered a very high priority.

4. See para. 5.4
5. See para. 5.3

14.15 The Technical Steering Group (TSG) was formed in April 1947, and among its terms of reference was the responsibility "To engineer special communications to and from the Communications Branch and the stations, and to other Centres"[6].

14.16 An RCAF Monthly Progress Report on plans for the station at Whitehorse, dated 30 June 1947, and signed by S/L C.E. Denning for the Chief of the Air Staff (CAS), commented "if air mail is considered sufficiently speedy then the situation is reasonably good". There was one flight daily to and from Edmonton and Whitehorse by RCAF Transport, daily flights by Canadian Pacific Airlines Whitehorse-Edmonton and Edmonton-Whitehorse, and Trans Canada Airlines scheduled flights Edmonton-Ottawa and Ottawa-Edmonton. There was one heavily loaded landline teletype (T/T) circuit between Edmonton and Whitehorse with drops at all intermediate stations, but no automatic ciphering equipment available. In addition, there was one radio circuit from Edmonton to Whitehorse and intermediate stations (to be converted to radioteletypewriter (RTT) at a later date).

14.17 An Army report for the same month said "daily delivery by orderly" from Leitrim was satisfactory. Owing to its close proximity to CB, no requirement was seen at that time for telecommunication facilities for the intercept product of Ottawa Wireless Station. Traffic from Victoria Wireless Station during June was handled by registered airmail.

14.18 It is not clear from the records available just how all the traffic from the intercept stations reached CBNRC during 1946 and 1947. Some intercept arrived by mail and it is thought that other material was fed in by teletype. The only information found in the files regarding circuits into the JDU is a note from Mary Oliver to George Glazebrook dated 4 February 1946: "rental of circuit $350 per month, $4,200 per year." This was almost certainly a

6. See Annex 12.A

reference to the circuit to Oshawa, financed by NRC[7], which carried traffic between the JDU and London and Washington. The earliest CBNRC communications diagram, reproduced at Annex A, shows circuits to Washington and London but not to the stations. Relying on memory, the writer, who was an operator in the JDU teletype office beginning 1 June 1946, recalls traffic being received by line from Victoria Wireless Station (intercepted material) and from Station at Coverdale via a teletype circuit from NDHQ. Memory, of course, is not fully reliable. It is possible, if there were teletype circuits carrying station traffic into the JDU and CBNRC at the Guigues Street location in 1946, that such traffic was fed first into NDHQ and relayed via local circuits paid for by the Department of National Defence which therefore might not necessarily be mentioned in CB financial records or files. There is a lone reference to maintenance work being done on "Air Force circuit equipment"; and the Coverdale circuit is thought to have reached CBNRC via Naval HQ, as it did for the next 25 years. A communication from the Signal Security Agency, US Army, Washington, D.C., dated 16 February 1945, requested that 4-digit code traffic from Stations and (Gordon Head?)[8] continue to be forwarded; whether the traffic was received by line or by mail from Station is not known for certain. The traffic records for the early years, unfortunately, appear to have been destroyed.

s.15(1) - DEF

s.15(1) - IA

CB's Cipher and Teletype Offices

14.19 When the JDU/CRC became CBNRC on 1 September 1946, the Cipher Office had a staff of three, and was equipped with three TYPEX cipher machines with CCM adapters used exclusively for SIGINT communications between the Ottawa, London and Washington SIGINT Centres. Encipherment/decipherment (sent and received) early in 1947 totalled 136 messages

7. See para. 14.21
8. See para. 5.2

(averaging 300 groups) in January, 150 in February, 289 in March and 335 in April. (All of this was of course, enciphered and deciphered off-line). Operating staff was supplied by CBNRC but maintenance of the cipher equipment was provided by the Army Signals Office.

14.20 The submission by Mary Oliver, mentioned above, also included reference to six machines in the teletype office. Some of these would be terminal equipment on the Oshawa circuit and presumably the remainder would be used on circuits to NDHQ. The terminal equipment was furnished by Army Signals and maintained by Canadian Pacific Telegraph personnel. (In October 1948, Army teletype equipment was replaced by CBNRC-owned machines.) The CBNRC Teletype Office also had three staff members in September 1946, and operated from 0800 to 2000 hours daily. By April 1947 the T/T office was sending out an average of 12,000 groups daily - more than 360,000 for the month - and during May, with the addition of another operator, the staff transmitted almost 660,000 groups and received over 77,000. All "raw intercept traffic" was received and forwarded "en clair" (unencrypted); only administrative messages were encrypted.

HYDRA

14.21 During World War II a Morse radio transmitter had been installed at Oshawa Wireless Station. This communications facility, known as HYDRA, had been developed by the UK Secret Service and was in early 1946 still owned and operated by UK authorities. It was used to pass SIGINT traffic between Ottawa, London and Washington. The US paid fully for landline operations between Oshawa and Washington, and NRC had only the annual $4,200 cost of the teletype line between Ottawa and Oshawa. A radio teletype transmitter was under consideration for communications from Oshawa to London. These arrangements were reckoned to meet the recommendation of the Commonwealth Conference that exclusive SIGINT

communications facilities between Centres should be established as soon as possible[9].

14.22 The proposal was made in March 1946 that the Canadian Government should take over HYDRA and operate it completely in order to bear its proper share of the cost of the London-Ottawa-Washington communications system. This, it was felt, would be "a valuable gesture and would be more than offset by the advantages we gain in other respects". To carry the volume of traffic anticipated, Canada would have to purchase a 50-kilowatt transmitter from the US at a cost of $150,000 installed. Annual expenditure on staff and other overhead was about $90,000. These costs would be compensated for by the reduction in payments to commercial cable companies which reached a maximum of $60,000 a year for NRC alone during World War II. It was suggested that NRC might pay for the new transmitter and External Affairs might assume the annual charges. The existing civilian employees would be replaced gradually by Army personnel. The Canadian Government agreed with this proposal to assume responsibility for HYDRA, but, as usual, there was much delay in making it official. CBNRC assured GCHQ that there was "no question of Canada's readiness to take on the responsibility" and that it was "only a matter of difficulty of getting final signature". Regrets regarding the delay were exchanged regularly throughout the summer and autumn of 1946.

14.23 The transfer of ownership of HYDRA to the Canadian Government was eventually made effective 1 April 1947. The property and equipment were handed over to Canadian Army Signals at no cost. The terms of transfer were set out in Department of External Affairs telegram DTG 201506Z of November 1946 which stated "It is understood that the station will be used for SIGINT traffic between London, Ottawa and Washington". It was also suggested that the UK Foreign Office and Canadian External Affairs might use this channel for traffic other than SIGINT. It

9. See end of para. 11.27

was subsequently agreed that although the HYDRA circuit was to be used primarily for SIGINT, it could also be used by the Canadian High Commissioner's Office in London, the UK Embassy in Washington and by UK Foreign Office establishments in New York. When the UK end of the circuit was placed under the control of the Foreign Office Diplomatic Wireless Service (DWS), the Chairman CRC wrote from Canada House (Office of the High Commissioner) in London to Director CBNRC and to DSigs Army on 31 July 1948 expressing the fear that the circuit might be "filled up to the detriment of SIGINT" and especially that "SIGINT might be crowded out in the event of an emergency". It was agreed that non-SIGINT traffic should not exceed 25%.

14.24 In January 1949 Mr. Crean (Chairman, CRC) complained in a long letter to Director GCHQ about conflicting views concerning the use of HYDRA and declared "I am not at all happy about existing arrangements". Apparently other authorities were making proposals for using the circuit. Mr. Crean said: "It was certainly our understanding that the chief reason for taking over HYDRA was to obtain a virtually exclusive circuit for Signals Intelligence in order to avoid the inevitable confusion which takes place on combined circuits on the outbreak of war. It is certainly unlikely that the Canadian Government would have been prepared to take over HYDRA except for this purpose .... We accordingly take the view that the HYDRA circuit is still for the primary use of SIGINT and that the benefits which accrue to the other users are entirely subsidiary to the main purpose of the circuit, namely to carry SIGINT traffic." He was very direct as he added "We are certainly not prepared to depart from the principle which was originally agreed upon, that the SIGINT traffic should take precedence over any other traffic handled by this circuit, nor are we prepared to carry traffic over the HYDRA circuit, the volume of which is arranged between London and Washington without prior reference to us". He made clear CBNRC's position in the matter: "It has been agreed in Canada that, while the Army will continue to control the Canadian terminal of HYDRA, the

allocation and control of SIGINT traffic over the two circuits will be handled by the Communications Branch, and any questions affecting the volume and control of such traffic should be taken up with the Director." (The Minutes of the 80th CRC Meeting report that in December 1951, 75 percent of the traffic carried on HYDRA was SIGINT.)

Communications with Intercept Stations

14.25 The same argument was being waged with respect to circuits between CBNRC and the intercept stations. Mr. Manson, in a memo to Director CBNRC dated 14 June 1947 said that at the 6th TSG Meeting it was obvious that "some clarification was needed as to the communications system existing between CB and the stations. It should be made perfectly clear that any communications system is exclusively "Y" and installed for "Y" work only, and is not to be mixed up with any purely signal communications". Without indicating that some circuits were already in existence, the First Report of the Technical Steering Group, dated 8 September 1947, recommended "intercept communications facilities" between Ottawa and the stations at Coverdale, Churchill, Prince Rupert, Victoria, Boundary Bay, Leitrim and Whitehorse. The report added: "Circuits should be exclusively for "Y" purposes and should be direct from "Y" stations to CB without relays where physical handling is required. The routing of traffic by landline, for some distance from "Y" stations as a security measure, should be considered."

14.26 The following week (16 September 1947) a special meeting of the CRC discussed the inadvisability of Service Signal stations sharing accommodation with "Y" intercept stations. It was agreed that it was undesirable to combine intercept and Signals communications in one building or at one Centre and that this must be avoided in new or projected buildings. Where combined facilities existed, it was agreed that Service Signals must be regarded as "non-paying tenants" and should be prepared for eviction if "Y" intercept requirements

expanded[10]. There can be little doubt, then, that the delay in providing circuits to CBNRC from the intercept stations resulted more from the intransigence of both parties than from any other cause. The Services felt that they should have some access to the communications system and some voice in its control since they would be paying the lion's share of its cost; and the SIGINT authorities maintained that they could not "obtain the maximum benefit from available Signal Intelligence resources" unless they had "exclusive SIGINT telecommunications channels" -- indeed experience had shown that in times of emergency, especially in wartime, Service communications expanded to the point where SIGINT communications were crowded out completely.

14.27 Eventually, however, a decision was reached, and S/L Denning, Chairman TSG, outlined the "Vote 700 Financial Requirements" for the circuits in a memorandum to DCom (Navy), DSigs (Army) D of S (Air), Dir. CB and members of the TSG, dated 10 August 1948. The communications requirements included: Under Army Communications Services, $22,100 for "leased simplex teletype circuit from Army Tape Relay Room Edmonton, to CB, Ottawa, 15 September 1948 to 31 March 1949; 6 1/2 months at $3,400 per month. Circuit to carry traffic from both Whitehorse and Boundary Bay onwards to CB, Ottawa. TSG Paper of even reference dated 21 June 1948 refers. Since the Army will control this circuit, full cost is being committed by the Army." Under RCAF Communications Services is listed $15,300 for "leasing one simplex teletype channel from Radio Station Whitehorse to Army Tape Relay Room at Edmonton from 15 September 1948 to 31 March 1949; 6 1/2 months at $2,350 per month. TSG Paper of even reference dated 21 June 1948 refers." Thus, for lack of evidence to the contrary, it can be concluded that a spirit of compromise finally emerged.

10. See para. 5.6

Growth of Traffic

14.28 Meanwhile, the workload in the CBNRC Teletype and Cipher Offices continued to grow. Traffic from Coverdale alone was approaching 10,000 groups a day by June 1948. ROCKEX equipment, a one-time machine system employing random key tape, was being installed both in and the CB Cipher Office so that for the first time intercept material could be secured with an automatic electronic encryption process operating at telegraph speeds (off-line) and in a manner which ensured that only authorized personnel had access to the information. ROCKEX equipment would also be in operation by September 1948 at Victoria and Whitehorse. From that time forward, TYPEX was used at CB only occasionally, as when a message would be received from GCHQ with a multiple address including British offices abroad which did not hold ROCKEX equipment. As for enciphered communications between CB and the Army Signals Agency (ASA) in Washington, ROCKEX had replaced the CCM on 19 November 1947. A communications diagram, showing existing and proposed circuits as of 29 December 1949, is given at Annex B.

14.29 The arrival of ROCKEX was accompanied by an expansion of the Test and Design Section (T&D) which had been formed a year earlier. T&D technicians took over responsibility for repair and maintenance of CBNRC cipher equipment, relieving Army Signals of that responsibility. To make way for T&D workshop operations the Cipher Office vacated its quarters in November 1947 and moved into a sectioned-off part of the Teletype Office. These two offices were later combined into the Communications Section as the staff grew to meet the needs of the ever-increasing flow of information. Shielding was added to teletype and cipher equipment as the TEMPEST hazard came to be understood and appreciated. SIGINT communications with the stations and the other Centres soon reached 1,000,000 groups per month.

14.30 The Oshawa circuit was beginning to be overloaded. Unable to clear all the traffic for Washington in the available circuit time, CBNRC, on

12 October 1948, began forwarding the excess by daily courier. This practice was used from time to time when traffic levels proved too great for available circuits. There were also occasions when line troubles on the circuits from the intercept stations would reduce transmission time, and in these cases the intercept take would be forwarded by Service Air or by registered mail. The increase of traffic was felt on the circuits between GCHQ and US Armed Forces Security Agency (AFSA) too. In addition to HYDRA the RCAF and RAF operated single sideband (SSB) channels. GCHQ, in a letter to DIRCOMSEC dated 8 April 1949, agreed that there was a sound case for improving transatlantic communications by the establishment of links complementary to HYDRA and the RAF-RCAF links and by using a cipher less expensive in line time than ROCKEX. They proposed the use of Secratype, later called 5UCO, an on-line equipment using key tape; encryption was performed simultaneously with transmission and the process involved no formatting and therefore required less tape and less line time.

14.31 It was decided at this point to move the HYDRA receivers from Oshawa to Leitrim, and by October 1948 the Royal Canadian Corps of Signals was arranging the technical details for the transfer of the circuits. The HYDRA channels would terminate at Leitrim and be operated on a tape relay basis. At the same time four Air Force SSB channels would terminate at the RCAF Message Centre. During good radio conditions two SSB channels were patched through to CBNRC for SIGINT traffic and two to the DND tape relay room for Service traffic.

14.32 The expansion of CBNRC necessitated a move to larger quarters in Rideau Annex on Alta Vista Drive. The transfer of communications operations was accomplished without dislocation or interruption. Duplicate facilities were installed during November/December 1949 on the second floor of the refurbished building; the Comcentre found its new home in what had been the psychiatric ward of the Rideau Military Hospital during World War II. Circuits between the old and new quarters kept

communications up to date during the move of the remainder of the Branch the following month.

14.33 The deteriorating international situation which preceded the Korean crisis in 1950 produced a rapidly increasing flow of traffic from the other Centres and particularly from the Canadian intercept stations. More ROCKEX equipment was obtained and the Comcentre doubled in size, acquiring space across the hall. The requirement to speed up communications prompted a move to take advantage of the latest in technology - CB became the first organization in Canada to use 5UCO high grade on-line crypto equipment, received in July 1950 from GCHQ. For the first time CB could carry on plain language "tele-conversations" with NSA and GCHQ knowing that the words were being encrypted and decrypted virtually simultaneously. The 5UCO equipment, with its increased traffic capacity, rapid handling and automatic encipherment features, required considerably more technical support than the off-line systems previously used. The Comcentre staff had to be enlarged to cope with the technical load and also to take care of the increasing flow of communications.

14.34 Communication between CBNRC, External Affairs and NDHQ was by a once-a-day messenger service. To meet the increased requirement for delivery of SIGINT reports, NRC made a station wagon available on call from CB in September 1950. Within a month, however, it was necessary to install a circuit between CB and Director of Military Intelligence (DMI), secured by ROCKEX.

14.35 The CRC at its 60th Meeting, 7 September 1950, agreed that the TSG should include $33,700 in its 1951-52 estimates as the cost of the SIGINT share of landline service between Churchill and Ottawa.

11. See para. 14.41

14.36 The staff of the Communications Section grew to 18, and 24-hour operation seven days a week was instituted in September 1950. The traffic had doubled in the past nine months and would triple in the next year. Annex C shows the circuits terminating in the CBNRC Comcentre in September 1950.

14.37

14.38 The Canadian Ambassador to Washington in 1950 was fully indoctrinated but members of his staff were not; nor were the communications personnel in the External Affairs headquarters. SIGINT material for the Ambassador had therefore to be sent on the CB-AFSA communications channel to CB Senior Liaison Officer who would hand carry it to the Embassy and burn the copy after the Ambassador had seen it because the latter had no safekeeping facilities for SIGINT. This situation did not improve until 1957.

14.39 Only three of the four floors of the Rideau Annex were occupied by CB staff during 1950; the fourth floor was used for storage purposes. The CRC

at its 63rd Meeting on 10 November authorized an immediate increase of 166 to CBNRC staff with consideration of an additional 56 in a year's time[12]. This was accompanied by a capital expenditure of $15,000 to convert the fourth floor of the building for office use and in 1952 the Comcentre was moved there. The new quarters provided a more efficient and convenient layout with improved physical security features.

14.40

12. See para. 3.5
13. See para. 11.75

14.41

14.42 Concern was being expressed about the ability of available facilities - circuits and off-line cipher equipment - to handle the increasing traffic levels. Mr. Drake told the 76th CRC Meeting on 12 September 1951 that 5UCO with ROCKEX as standby was used to communicate with the US and UK, but that only ROCKEX (off-line) was available for communicating with the stations. This situation continued until 1959. The heavy traffic loads required enormous quantities of key tape. Both ROCKEX and 5UCO used one-time tape with which each plain text character was matched by at least one character on key tape. Shipments of key tape produced by T and D Group weighed several tons each month. The users all wanted a tapeless device, one with a built-in electronic key generator. Both the US and UK were developing such equipment. Mr. Drake thought that Rollick (a UK device) would replace 5UCO; the RCAF wanted ; the RCN were using CCM/CSP 1700 (a US machine); and the Army was holding out for a tapeless machine. The Directorate

of Supplementary Radio Activities (DSRA) Member advocated coordinating the selection of cipher machines. Mr. Drake said the Communications-Electronic Security Group (CSG) planned to produce a paper every six months detailing the development of new machines as well as trends and variations.

14.43 The UK-US-Canadian COMINT Communications Conference held at CBNRC in October 1952 considered the existing, future and wartime requirements for SIGINT communications. The delegates discussed the facilities to be used by SIGINT authorities, as portrayed graphically in Annex D. The RCAF was able to commit two SSB channels for exclusive SIGINT use both in peace and war, although at the time one channel was being used to supplement HYDRA tape relay working. In addition, one HYDRA circuit was permanently allocated as a standby 5UCO circuit between GCHQ and CBNRC, but was currently being used for tape relay. Four HYDRA circuits were permanently allocated to Leitrim Traffic Centre tape relay working. The CBNRC traffic with other Centres in 1952 totalled as follows:

CB to AFSA	27,000 groups daily	88% by 5UCO (remainder by ROCKEX)
AFSA to CB	9,000 groups daily	93% by 5UCO
CB to GCHQ	8,300 groups daily	47% by 5UCO
GCHQ to CB	15,500 groups daily	26% by 5UCO

(meanwhile GCHQ transmitted 22,000 groups daily in ROCKEX to AFSA and received 6,500 from AFSA; 5UCO between GCHQ and AFSA averaged five hours daily).

Further Expansion

14.44 The traffic levels continued to climb and the Comcentre staff grew to 22 by June 1952. In September Whitehorse transmitted for more than 15 hours on several days and on 22 February 1953 for almost 19 hours, threatening to crowd Ladner's intercept material off the 24-hour circuit the two stations shared from Edmonton to CBNRC. In 1952 the total traffic to and from CB amounted to 111,000 groups daily. A year later this had reached 124,000; in

1954 it climbed to 147,000 per day, in 1955 to 177,000 groups (600 messages), in 1956 to 191,000, in 1957 to 221,000, in 1958 to 246,000 and in 1959 to 278,000.

14.45 The sudden death of John Manson in August 1952 was followed by a reorganization (dated 26 June 1953 but implemented 17 November 1953) in which Mr. Manson's Communications Assistant, C.E. Denning, was named Head of C Group - the Communications and Collection Group. Irv Hughes, the previous Section Head, had resigned in July 1953, whereupon K.J. (Ken) Hughes (no relation) was appointed Section Head of C2-Communications Section. By 30 July 1954 the Comcentre staff had grown to 31 persons. Traffic was flowing in from the two RCN stations, Coverdale and Churchill (and from two intercept positions at the Aklavik test site); from the two Army stations, Leitrim and Vancouver; and from the RCAF station at Whitehorse (as well as from two positions at the Resolute Bay Test Site). Until April 1955, T&D Group technical personnel were responsible for service maintenance of Comcentre equipment. When T&D Group was preparing to move to a Montreal Road location (NRC laboratories), eleven technical positions were transferred to C from T&D on 1 April 1955.

14.46

Changes in Transatlantic Communications

14.47 The RCAF-RAF SSB channels used for CBNRC-GCHQ 5UCO working were very good in earlier days, but in the mid-50s, after a reorganization of transmitter/ receiver facilities, the service became so poor that SIGINT traffic was gradually transferred to the HYDRA system, which at the same time was being improved to the point where it became the main (almost the sole) transatlantic carrier for SIGINT traffic. The SSB system was closed down in early 1956 for servicing. In May the RCAF reported that the system reliability had been improved and CBNRC suggested a 5UCO comparison test between an Air Force channel and an Army-DWS (HYDRA) channel. They proposed re-opening an SSB circuit on 5UCO between 1200Z and 2000Z Monday to Friday without alteration to existing arrangements for 5UCO working on HYDRA. By April 1958 trouble was still being experienced with the two SSB channels. The UK agreed to CB's suggestion that one SSB channel be returned to the Air Forces, subject to recall if needed, and the other be retained for off-line working directly between CBNRC and GCHQ. HYDRA operation with 5UCO on a radio channel was usually satisfactory. When radio conditions deteriorated large quantities of traffic had to be diverted to air bag.

14.48 In a discussion about the financing of the HYDRA facilities, Mr. Crean told the 18th Communications Security Board (CSB) Meeting on 15 December 1955 that the Departments of External Affairs and National Defence shared the costs of HYDRA, each including funds in their own estimates:

> "Mr. Crean reviewed the origin of the HYDRA system and indicated that the system was operated by National Defence (Army) on behalf of External Affairs and that the External Affairs contribution was in the form of payment for leased lines. These lines were connected to NSA and GCHQ and, in addition to CBNRC traffic, they also carried External Affairs and British Foreign Office overseas traffic."

> "Mr. Crean explained that Leitrim was in effect a government traffic centre and, since at present the HYDRA system was really the only government strategic communications network, he referred to the advantages of a tie-in with the planned transatlantic cable facilities, a matter which had so far been considered mainly only from the standpoint of the needs of individual departments. Mr. Crean also reminded the Board that the current use of the HYDRA system for (Chiefs of Staff) traffic was not in accordance with the original agreement and that, while such traffic could be handled in peacetime, the inevitable increases in wartime traffic would be such that high priority Service traffic would tend to crowd out other essential traffic."

14.49 Less than two years later, at the 21st CSB Meeting on 2 October 1957, Mr. Crean expressed surprise that the Army had apparently assumed responsibility that year for the total costs of the HYDRA operation, including transmitters, operators, leased lines, etc. He found it paradoxical in the light of DND's expressed concern about cutting costs, and especially since External Affairs, unaware of the Army action, had included funds to cover the share of the costs which they had borne in past years. External objected on the grounds that this would give DND control of HYDRA. Actually, DND did control the system, but External, by paying part of the costs, had some say in how much diplomatic, as well as SIGINT, traffic could be passed. On the other hand, the 23rd Meeting of the CSB on 6 November 1958 heard a complaint from the Chairman, Chiefs of Staff (Gen. Foulkes), that although National Defence was paying about $500,000 annually for the HYDRA system, there was no guarantee that a military message would be passed during a period of extreme tension.

14.50 A transatlantic cable, known as TAT-1, had been laid in 1956 on the ocean floor between Clarenville, Newfoundland, and Oban, Scotland. (Incidentally, the laying of a transatlantic cable

had first been attempted in 1857 but failed. The discovery of gutta-percha, however, made possible the protection of the cables with a latex insulation, and the first successful cable was laid in 1858. The cable was loaded aboard two ships which met in mid-Atlantic - one headed east and the other west, both paying out the cable until a complete link was made. By 1885 there were five cables in use, although they were used for Morse Code telegraphy only. Cables were still being used 100 years later, but mostly for teletype and voice communication.) In 1958 arrangements were made to rent a cable circuit to add to the HYDRA system. External Affairs shared with the UK half the rental cost. It was agreed that, although this specific channel was inaugurated solely to ensure a reliable and instantaneous means for the passage of "alerts" messages, it would be connected into HYDRA as an additional facility available to common users in normal times.

14.51 Mr. Denning, as Secretary of Communications Operations Policy Committee (COPC), wrote to DIRCOMSEC and Director CBNRC on 7 March 1956 pointing out that the charges for the Canadian portion of the duplex teletype circuit between CBNRC and Washington were still being paid for by the Department of External Affairs. He reported that it had been decided at the COPC that, with effect from 1 April 1957, responsibility for the Canadian portion of the circuit, including the provision of funds, was to be borne by CBNRC, and would be reflected in its FY 1957-58 Financial Estimates.

New Canadian Circuits

14.52 Late in 1956 an urgent requirement necessitated a change in the dissemination of SIGINT end-product traffic to the RCAF. The Directorate of Air Intelligence (DAI) became the major addressee, and Air Defence Command (ADC) Headquarters required the same traffic. This entailed the provision of simplex teletype circuits between CBNRC and DAI (Beaver Barracks) and between DAI and ADC HQ, St. Hubert, P.Q. Also required was a switch at Beaver Barracks controlled by DAI to permit the connection

and disconnection of the CBNRC-DAI and DAI-ADC circuits. The installations were made in November 1956. The lack of 24-hour staff at DAI and ADC soon made it clear that the arrangements were inadequate for the quantities and the urgency of the SIGINT traffic and within a month plans were under way to change to an exclusive CBNRC-DAI-ADC omnibus simplex teletype circuit, with CBNRC as control station, and with the DAI and ADC offices manned throughout the 24 hours. A year later, however, writing regarding Strategic Air Command Pre-flight information notices, Jaff Wilkins for Director CBNRC said to CANSLO/W: "... we do prefer the SAC-NSA-CBNRC channel as being, from our experience, more direct and expeditious; the DAI and RCAF/ADC SIGINT message centres are now operating on a 24-hour basis but still occasionally revert to a call-in arrangement whereby the SIGINT message centres close down at night or on weekends and the main ADC or the AFHQ communications offices call in the operator for messages of a certain precedence." A further development occurred when a Joint Indications Room (JIR) was set up at NDHQ to evaluate events and occurrences throughout the world that might indicate an increase in tensions or possibilities of serious trouble. SIGINT information was fed into the JIR around the clock by the CB Comcentre via the Chairman Chiefs of Staff (CCOS) Comcentre.

14.53 In November 1956 it was proposed that communications facilities between a new intercept site at Aklavik and Churchill should be established. (It is believed that the proposal originated with DSRA.) In February 1957 CBNRC gave support to the suggestion, adding that Whitehorse should also be included. Several advantages were cited, including the potential for alternate routing to CBNRC from Churchill, Whitehorse and Ladner and for close working between stations on SIGINT tasks. This proposal met with opposition at the COPC from the RCAF. As a result, the Navy went ahead with only the

14. See para. 5.36

Aklavik-Churchill link in the spring of 1958 - a 14-hour, 60 words-per-minute teletype circuit for exclusive SIGINT use. A communications diagram, prepared during discussion of the proposal in February 1957, is reproduced at Annex E. It shows all CB landline and radio contacts.

14.54 The Director of Communications Security (DCS) in September 1957 approved a communications channel between CBNRC and the Canadian Embassy in Washington for the transmission of Category III material. A prerequisite, of course, was the indoctrination of Embassy communications staff to handle SIGINT material. This provided an alternative route for CBNRC to send sensitive or "CANADIAN EYES ONLY" messages to CANSLO/W and CANCOMSLO/W. The OTLP system with the liaison officers was retained but could now be used less frequently[15]. (It was phased out in 1972.)

14.55 In August 1958 in a message to DIRNSA, the USAF requested approval to establish a circuit to pass SIGINT communications between HQ NORAD and CBNRC[16]. The purpose was to transmit intelligence, some of which would be derived from SIGINT, between the Canadian Joint Intelligence Committee (JIC) and NORAD. The CANUSA Agreement specified that SIGINT arrangements between US and Canadian agencies required the prior approval of USCIB and the CRC, which had now been effectively replaced by the US Intelligence Board (USIB) and the Canadian CSB. USIB concurred in the request and wrote to DIRCOMSEC in November 1958 seeking CSB concurrence, noting that the communications channel would also be used for direct dissemination of CBNRC SIGINT end-product to meet NORAD's operational needs for timely warning information. DIRNSA objected to the use of SIGINT channels to handle non-SIGINT; and CBNRC shared this reluctance. Mr. Denning explained that a study was being conducted of existing facilities and the delays being experienced, to see whether new facilities

15. See para. 14.37
16. See para. 11.85

profile". The CRC gave consideration to the possibility of allowing CBNRC to advertise for staff with qualifications that would be useful in crypto operations. At the 97th CRC Meeting on 10 April 1953 the Chairman said he "personally was of the opinion that security regulations dealing with cipher production by CBNRC could be relaxed somewhat". The Cipher Policy Committee (CPC) and the Communications Security Group (CSG) took the opposite view. The CPC considered the subject of unclassified references to crypto duties and "agreed that, since unclassified information of this nature provided disloyal persons with an opportunity for penetration into cipher offices, such advertisements were prejudicial to security and should be prohibited". At the 14th Meeting of the Senior Committee, now called the Communications Security Board (CSB)[13], on 19 October 1953 "the question was raised as to whether recruiting was so seriously hampered by the secrecy which prevailed in connection with SIGINT work that some consideration should be given to publication in general terms of the nature of the work of the Branch. It was suggested that one possibility might be to make public the fact that the Branch was engaged in the production of ciphers. No decision was reached on this general question".

17.46 Meanwhile, the responsibilities of the Test and Design Group continued to expand. Production of book ciphers, key settings

TYPEX inserts and ROCKEX tape was progressing apace. Preparations were under way for the generation of 5UCO tape. Along with their routine maintenance and fault-finding and correction routines, T&D staff were required to build five random signal generators, a timer and five isolators. In preparation for the move of the Comcentre to the fourth floor of the Rideau Annex, T&D built new control racks and prefabricated jack panels, connecting blocks and cable assemblies. Overtime was necessary, and five more technicians were sought, as well as a draftsman.

13. See para. 2.13

on-line crypto equipment) on the channel. CBNRC demurred on the grounds that the operation of the national SIGINT net was based entirely on the use of ROCKEX and while the latter had the disadvantage of being off-line, its employment at CB and at all intercept stations provided operational flexibility and standardization of procedure and maintenance which they would not wish to lose. Mr. Denning added, however, that the national SIGINT communications net was under review and a change to on-line systems wherever practicable was being considered. In fact, Mr. Denning, as Chairman Communications Security Technical Group (CSTG), had written to DIRCOMSEC on 11 May 1956 to say "CSTG has given further consideration to the provision of on-line cipher machines at stations" and it had been agreed to proceed with a two-stage program, with the first stage being to acquire "a simpler type of machine using key tape - simpler to maintain and cheaper than machines with 'built-in' key generation". The second stage would be dependent on the success of US and UK cipher machine development. CB hoped to purchase four of the simpler 5UCO machines out of 1956-57 funds for trials on the long landlines, and if the tests were satisfactory an additional eight would be acquired.

14.58

14.59 Although planning for on-line equipment had begun as early as 1948, action to implement on-line working on circuits to the stations was slow in coming. In January 1959, the Acting Director (A/D) CBNRC wrote to the Director of Communications Security expressing concern that CB communications were inadequate to meet the responsibility for rapid reporting of COMINT indicators of possible hostile intentions. He said the use of the ROCKEX, an "off-line" device, imposed delays which were no longer acceptable and recommended that a change to an "on-line" equipment be made as soon as possible. The A/D requested that consideration be given to the conversion of communication facilities between CBNRC and Churchill, Whitehorse, Vancouver and Coverdale to on-line.

The Cipher Policy Committee (CPC) approved the KW-26 for use on this circuit on 9 February 1959, and the KW-26, with an electronic key generator incorporated, replaced the 5UCO between CBNRC and NSA, beginning 20 April. Thus began the gradual phase-out of 5UCO equipment even before it had been phased in on the Canadian SIGINT network.

14.60 There was a clear need to move to on-line quickly to avoid the delays inherent in off-line operation, and the SIGINT authorities were anxious to adopt 5UCO on an interim basis, mainly because it provided the advantage of speed in handling traffic, but also because it would serve as a stepping-stone to a tapeless device such as the KW-26 when the latter became available for general use. Meanwhile, the Services were considering the impact of conversion of the COMINT network to on-line operation. The RCAF agreed in principle to the move, acknowledging that the operational advantages to be gained by the adoption of 5UCO equipment outweighed the disadvantages, but the RCN and Army asked for

justification, such as indications that traffic loading exceeded the capacity of existing circuits; they felt that the desire for more expeditious handling did not warrant the increase in technical personnel that would be involved. The RCAF acknowledged that "the conversion from ROCKEX to 5UCO at this time (February 1959) will facilitate conversion to a non key-tape using on-line equipment such as the TSEC/KW-26, when such equipment is available to Canadian users in 2-3 years time". They specified, however, that adoption of 5UCO must not "prejudice future conversion to KW-26 equipment that has been recently approved for the CB-NSA circuit".

14.61 In mid-1959, the Director of Communication Security (J.K. Starnes) wrote to DSRA (Navy), DSigs (Army) and DComm (RCAF) in support of the proposal to convert CBNRC-to-Station communications from off-line to on-line crypto operation. The conversion would require changing the circuits from half duplex to full duplex and this had to be justified by proving there was sufficient traffic to warrant it. He pointed out that CBNRC-to-Station landlines had an accepted operating capacity of 45,000-50,000 groups per day but that there were times when the circuits were unable to handle all the traffic intercepted. The "Western" circuit, shared by the Vancouver and Whitehorse stations, had for the past year averaged 40,000 groups daily, with peaks well above that figure. Since September 1958 there had been more traffic than the circuit could handle and, to prevent a continuous backlog, both stations had been forced frequently to dispatch by mail material urgently required at CBNRC. The CBNRC-to-Churchill circuit also served the Aklavik and Alert stations and had been operating at or near full capacity for the past year. With the expansion of the two more northerly stations and with the introduction of forward processing at Churchill, it was considered certain that the existing landline would be inadequate to carry the required traffic volume. Coverdale to CBNRC traffic, which was "tape relayed" at DSRA, was peaking at 30,000 groups a day and was on the increase.

14.62 The projected dates for conversion of the CBNRC-to-Stations communications to 5UCO were:

Churchill circuit	-	December 1959
Whitehorse circuit	-	February 1960
Coverdale circuit	-	April 1960
Vancouver circuit	-	June 1960

NSA's offer of 5UCO equipments was accepted and DIRCOMSEC requested the Services to take action to implement the plan. Although some problems were foreseen by the Services, such as the training of technical personnel, duplex lines were installed and all the circuits were converted to the use of 5UCO as planned, with only one missing the target date - Vancouver was two months late. The Services attributed the slowness in implementing the on-line crypto program to austerity measures, which although they had not interfered with the procurement of equipment, had affected the acquisition of personnel needed to operate and maintain the new equipment, and had also made it impossible to finance the structural changes associated with the installation of the machines.

14.63 Mr. Denning wrote to the Director CBNRC on 18 August 1959 to say that he would propose to DSigs (Army) the provision of an on-line (5UCO) crypto system on the CBNRC-JIR circuit as well. This was part of the overall plan to speed up the delivery and dissemination of indications intelligence from the intercept stations. The continuing overloading of the circuit from the CBNRC Comcentre to the DND Communications Centre which served the JIR prompted Mr. Denning to write again to DSigs Army on 27 October 1961, once more urging conversion of the circuit to on-line operation. Traffic, mainly from CB to the JIR, was averaging 25,000 groups daily and frequently reaching 40,000 groups per day during prolonged periods of increased SIGINT activity. Considerable operator effort could be saved by converting from the double process of off-line operation to on-line. By that time, however, KW-26 equipment had become available. Moreover, (mirabile dictu), CBNRC was in the fortunate position of being able

to offer the loan of equipment instead of having to borrow from others as they had for many years. Mr. Denning offered to lend KW-26 equipments to the Army until their own would become available in mid-1962, and to assist in their installation and maintenance until Army technicians could be trained.

14.64 Mr. Denning was anxious to standardize operations on the SIGINT network with one type of crypto equipment if possible. KW-26 had become available for the SIGINT links before the end of calendar year 1961, technicians were trained in January and April 1962, and conversion to KW-26 effected in the spring and summer of 1962 (Churchill to CBNRC in May; Churchill to Inuvik in May; Coverdale to CBNRC in July; Whitehorse to CBNRC in June; Ladner to CBNRC in August; and CBNRC to the Navy Crypto Office Ottawa, in February). The 5UCO had done its job; it had rendered good service even though it had been needed on the station circuits for only two years. As KW-26 went into operation, the 5UCOs were returned to CBNRC for disposal. However, Mr. Denning found it necessary to write once again about the circuits to the JIR and DAI. On 14 November 1962 in a letter to DComm RCAF he said "the very heavy traffic load during the recent Cuban situation has again shown that off-line crypto is completely out of place in a communications system that must respond to crisis conditions. The inter-Centre and most of the Station-CBNRC circuits have been on-line for some time ... the last station to change to KW-26 will do so quite shortly. However, the circuits to the Joint Intelligence Room and to DAI/ADC are still using the off-line (ROCKEX) method". He referred to RCAF proposals two years earlier on the use of ALVIS equipment which, it appeared, would not be available before 1964. He therefore urged that KW-26 be adopted for the CBNRC-DAI circuit to avoid further delay. The circuits to DAI and the JIR were eventually converted to KW-26 on-line, the former in March 1963 and the latter in September of that year.

14.65 While C Group Head was endeavouring to improve communications facilities, he received cooperation from the other Groups in a continuous effort directed toward eliminating redundant material and removing less timely series of reports from electrical forwarding. In spite of this, the traffic load handled by the Communications Centre grew each year. Significant changes designed to improve the handling and distribution of intelligence were effected; new routing and delivery procedures were introduced to speed up the relay and distribution of messages from CBNRC and Canadian stations.

Developments at Stations

14.66 The greatest remaining problem was the establishment of more reliable communications with Alert . The HF circuits ALFA and BRAVO from Alert via Leitrim had been deteriorating as the period of minimum sunspot activity in the 11-year cycle approached. By the end of 1963 arrangements were completed for a through channel (LF to Thule, Greenland, troposcatter to Cape Dyer, and microwave and landline from Cape Dyer via Goose Bay to CBNRC) to be ready by February 1964. In fact, this circuit (Alert CHARLIE) was in operation using KW-26 by 29 January. Preliminary arrangements were also made to replace the Churchill-Inuvik radio link with a landline circuit. This facility would be in a position to be implemented when the Canadian National Telegraph Company completed their northern landline to Inuvik from Edmonton in 1965. Coming nearer home, there was no circuit from CBNRC to station as such. Messages for were sent on the CBNRC-OTC (Ottawa Traffic Centre at Leitrim) circuit to the tape relay office and taken upstairs by hand to the intercept station. Messages to and from CANCOMSLO (CB's Canadian Communications Security Liaison Officer) in the Canadian Embassy, Washington, were also routed through the OTC. The tape relay centre at Leitrim continued in use until a formal proposal was made to close it down in 1966; with the virtual elimination of off-line systems user-to-user patching became the mode, and this led to the situation where no tape relay operation at Leitrim was required.

Policy direction and operation of the HYDRA communications system was assumed on 1 December 1964 by the Directorate of Communications Plans, CFHQ.

Page 986

is withheld pursuant to sections

est retenue en vertu des articles

13(1)(a), 15(1) - IA, 15(1) - DEF

of the Access to Information

de la Loi sur l'accès à l'information

Miscellaneous Items 1959-1963

14.70

14.71

14.72

14.73 CBNRC moved to the Sir Leonard Tilley Building in June 1961 and the Comcentre was installed on Saturday, June 17, in the north end of the building, third floor. The Communications Office files/records from the Rideau Annex were apparently not retained. The second CBNRC-NSA circuit (BRAVO) was converted to full duplex using KW-26 on 20 September 1961 to cope with the expanding traffic load. At about this time, the increasingly frequent recurrence of serious traffic backlogs between Centres was causing CBNRC, GCHQ and NSA more than a little concern. It was obvious that greater traffic-handling capacity was needed, particularly on transatlantic circuits. In June 1962 NSA noted that they were realizing less than 40 per cent availability on the HYDRA channel - less than the capacity needed for an effective third channel. They were, however, reluctant to abandon HYDRA because it did provide an alternative route which could be used when the transatlantic cables experienced problems[17].

14.74

17. See para. 14.70

14.75 Canadian officials, including CBNRC, were somewhat unhappy that the UK and US had inaugurated the CANTAT submarine cable channel and a duplex landline from Washington, both having Canadian termination at Ottawa Wireless Station (Leitrim), without notifying CBNRC. Though chagrined, CBNRC felt that "No doubt the general crisis atmosphere prevailing at that time prevented the action that normally would have been taken by the other two Centres to consult all concerned". An additional palliative was, of course, the fact that the ability to use the cable route through NSA to GCHQ provided CBNRC with a reliable means of communication with GCHQ for the most vital messages; and, since the other two Centres shouldered the total cost of the new circuits, apparently no complaint was lodged. The alternate route **was** used: for example, from 20 to 24 January 1963 CBNRC was given the use of the CANTAT cable for a total of 43 hours. During the same period radio communication was available for about 50% of the time as well; even so GCHQ diverted 148 routine and priority messages to courier on 25 January.

14.76 An impetus to the search for other channels was provided by the poor service rendered by the SSB circuits, and by an attempt on the part of the RAF-RCAF to improve them by reducing them from six to three working channels. This would have resulted in a re-allocation of channels, and CBNRC-GCHQ were asked if they would relinquish one or both of the two SSB channels allocated for SIGINT. Although GCHQ felt that both could be released because they now had a cable channel, CBNRC was reluctant to agree, since they did not yet have the use of cable facilities, and in the existing atmosphere of austerity a request for a submarine cable circuit was unlikely to receive favourable consideration. GCHQ sympathized with the desire not to "let the Air Forces off the hook" since

they in fact were committed fully to providing at least one channel, whereas "the HYDRA people were only brought in (out of the kindness of their heart) ... when it was apparent that the circuit provided by the Air Forces was not giving us good service".

14.77 C Group Head had a problem. The CB Comcentre staff ceiling in November 1962 was 70 people, of whom approximately one quarter were technicians. The current austerity program had inhibited the replacement of the few who had resigned, so that he had about 48 operators and 16 technicians. With this staff he could man the circuits on a 24-hour, 7-day-a-week basis, but could not be sure of having surplus staff available to man 3 or 4 circuits to the UK whenever radio conditions were good and NSA-GCHQ traffic levels permitted extra circuits to be used. The only circuits committed for on-line working between CBNRC and GCHQ used HF radio, which was far from reliable, and which would be at its worst for the next three or four years until conditions climbed out of the sunspot trough. Radio conditions were "out" for many hours on most days. It was not possible to have reserve manpower standing by waiting for conditions to improve and therefore CB was often unable to comply when GCHQ would, without warning, ask them to open up two or three extra circuits.

14.78

Cable Versus HF Radio

14.79 Radio conditions continued to deteriorate as the mid-1960s approached. The UK Defence Signals Staff wrote to NDHQ on 4 December 1964, expressing concern about the reduced availability "in the present Sunspot Minimum given by existing HF radio communications between the UK and Canada". The letter reported that in September the UK Defence Signal Board, MOD, had agreed there was need for an additional cable channel between London and Leitrim, with appropriate 'tails' to meet the requirements of the Service Departments and GCHQ. The UK proposal would have a submarine cable circuit terminate at OTC Leitrim, to be patched through to CBNRC for twelve hours daily seven days per week, and through to a chosen Service Comcentre for the remaining twelve hours each day. When in use between GCHQ and CBNRC the channel would by-pass the Service Comcentre (at CFHQ, or CFEHQ Carp) and be patched straight through to CBNRC.

14.80 In January 1965, DND invited comments from CBNRC, and Mr. Denning's letter of 16 February expressed "emphatic support of the UK (MOD) proposal" with the following justification:

> "At the present moment we are virtually completely dependent on HF radio for transatlantic working. The outages on these circuits frequently result in GCHQ having to divert to mail large quantities of signal traffic, including precedence 'PRIORITY' material, for various Canadian recipients."

As a matter of fact, the proposal had originally been broached by GCHQ to CBNRC in November 1963, but Mr. Denning had pointed out that UK MOD would have to approach DND Canada. He explained that the provision and financing of transatlantic communications for Canadian SIGINT were dealt with on an interdepartmental basis, and therefore CBNRC was not empowered

to enter into any agreement for leasing communication facilities. As time passed and no proposal was received in DND, Mr. Denning, in February 1964, urged GCHQ to press the case through defence channels, promising strong support when the question was raised in committee. A further ten months had passed before the proposal was made in December to NDHQ. By that time the integration of the Canadian Armed Forces was well under way, and this resulted in a wholesale shifting of communications staff officers and responsibilities. At the same time a large and detailed study of both national and international communications was initiated, commanding the attention of the slowly reorganizing defence signals staffs. Thus it was not until October 1965 that this particular proposal was again given active consideration. In the meantime, as integration of the Forces proceeded, the three circuits to Naval HQ, the JIR, and the Directorate of Air Intelligence were replaced by two -- CANFORCEHED ALFA and BRAVO -- effective 1 June 1965.

14.81 The traffic load in the CBNRC Comcentre had increased by 12% to 15% annually in the early 1960s, straining capabilities to the limit. Unable to add to the reduced staff total[18], the Comcentre was only able to handle the increased traffic load by streamlining procedures. By 1965 other measures were necessary. Changing patterns in message types, series and reporting methods, increased relay responsibilities as well as the acceptance of new commitments, all required a more specialized knowledge on the part of the operators. The technicians, too, were under greater pressure, faced with a more varied array of equipment and many more individual units to maintain; they had been given maintenance responsibility for recorders, cameras, "SWAMP" plotters and demultiplexers[19], and ancillary equipment used by other sections in the processing of intercept material. A reorganization of the Communications Centre was required - a change

18. See para. 14.77
19. See para. 12.38

in layout, the introduction of more automation and the upgrading of operating and technical skills. After a TEMPEST survey, new partitions were installed and systems (control desk, intercom, teletype terminals, off-line and on-line crypto) were repositioned. A conveyor belt and a tape factory (six-channel multiple transmitter group fitted with message identification modules) were installed. These and numerous other modifications were instituted in order to enable the staff to meet the steadily increasing requirements. Several new circuits had to be opened to carry the heavier traffic load, and these are reflected in the network diagram reproduced in Annex F.

14.82 In February 1966 the Chief of the Canadian Defence Staff announced that the UK proposal, referred to in paragraph 14.79, to lease another transatlantic telegraph cable circuit had been endorsed by External Affairs, CBNRC and DND. The UK General Post Office were instructed to provide the duplex circuit by 4 June 1966 from the UK to Montreal COTC (Canadian Overseas Telecommunications Corporation). The circuit would be extended from Montreal to Leitrim via a DND circuit funded by External Affairs. The circuit, installed on a time-shared basis, would then be patched through to CBNRC from 0001Z to 1200Z hours daily and to Carp STRAD from 1200Z to 0001Z hours daily. Actual operation commenced 9 June 1966. The HYDRA radio circuit (Leitrim-LTC) continued in operation, providing efficient communication for CBNRC during the 12-hour period between daily cable allocations, thus ensuring a continuous 24-hour on-line service.

14.83 A meeting was held in Ottawa in October 1966 at which representatives of External Affairs, DND and the UK Diplomatic Wireless Service agreed to close down the HYDRA Telegraph Relay Centre (TRC) at Leitrim on 1 November 1966. Most circuits through Leitrim carried on-line communications and tape relay operations were no longer needed at that location. The transfer of the circuit switching operation from Ottawa Wireless Station to 704 Communication Squadron, Rockcliffe, was made in January and

February 1967. An appreciation of the complexities involved in the management of HYDRA can be gained from the following excerpt from the Minutes of the meeting:

> "After some discussion it was agreed that matters of policy should be dealt with through Mr. McCardle, DIRCOMSEC (or his successor), that matters of financing should be dealt with through Director of Communications Requirement and Support (DCRS) (Col. Finch), that operational problems should be dealt with through No. 704 Communication Squadron (S/L Grainger) and that traffic, lost circuit time and other reports should be dealt with through DCRS."

The Director CB wrote to External Affairs on 21 November 1966 regarding the changes to the HYDRA system pointing out that "matters such as transmitter/circuit allocation and use and possible future facility consolidation plans with other communications systems" were also of concern to CBNRC, and he requested that he be informed prior to any discussion on the subject so that CBNRC could be represented at early stages of consideration. This was only one of many instances that illustrated CBNRC's sensitivity to being overlooked when changes were being considered which would impact on CBNRC. The closing down of the tape relay facilities at Leitrim led to a UK proposal to dispense with ROCKEX communications between CBNRC and GCHQ as a back-up to on-line communications, seeing that ROCKEX had not been used in the past six years. CBNRC agreed in March 1967, noting that ROCKEX would be retained as a standby with some stations (particularly Alert) for at least two or three years, if the Services could continue to provide trained technicians and operators for the off-line machine.

14.84 In January 1967, at the request of CFHQ, CBNRC proposed to GCHQ that the requirement for CAF 93, the SSB circuit originally provided by the two Air Forces, be cancelled. The UK agreed in March. The 24-hour service provided by the cable circuit and

HYDRA was considered sufficiently reliable to warrant release of the troubled SSB channel.

CB-Alert and CB-Customers

14.85

14.86 The heightening of world tension in 1967 and the resultant increase in the amount of traffic from CBNRC for DND prompted the inauguration of a third circuit to CFHQ on 9 June. This was followed by the installation of a KW-26 circuit from on 13 September. The June 1967 Middle East Crisis and the developing situation in Cyprus during the latter half of 1967 also illustrated the inadequacy of arrangements for the forwarding of SIGINT from CBNRC to the Department of External Affairs. Most of the traffic was transmitted by a daily (Monday to Friday) courier service. There was also an improvised crypto-communication channel -- an

off-line system relayed through CFHQ. The large volume of diplomatic material forwarded, particularly during crisis conditions, and the need for timely delivery coupled with the requirement for discussions, often on short notice, underlined the urgency of providing direct, secure communication between CBNRC and External. Moreover, the risks attendant upon frequent use of the open telephone and the awkwardness of rushed "ad hoc" liaison visits gave emphasis to the need. Mr. Drake wrote on 11 December 1967 to the Head of Defence Liaison (DL(2)) Division, External Affairs, recommending the installation of an on-line teleprinter circuit and/or a secure telephone circuit. The need for an improved service was agreed, but because of congestion in the External Comcentre, the teletype terminals, protected by ALVIS cryptographic equipment, would have to be located in a "special crypto centre", an anteroom of the DL(2) Office. CBNRC would be able to borrow CID/610 (Canadian-built ALVIS) equipment from DND. Two simplex 100 w.p.m. circuits, rather than one duplex, were considered preferable because most of the traffic was "one way" (CB to External) and this permitted more flexibility (CB could transmit on both simultaneously). External Affairs would bear the cost of the circuits. Three additional operators would be required in the CB Comcentre. However, External found themselves unable to support the request for the additional staff in CB, and the project was consequently postponed for six years. A telephone circuit could not be considered pending the availability of suitable, affordable ciphony equipment.

14.87 In September 1967, the Director of Communications Requirements and Support, CFHQ, approached CBNRC with the object of reterminating at CBNRC the Ottawa end of the CFHQ-Northern NORAD intelligence circuit. CB refused on the grounds that its Comcentre staff was already over-extended, and that such a retermination would result in CBNRC becoming responsible for relaying operational intelligence traffic from CFHQ to NORAD.

Traffic Problems 1967-1968

14.88 Traffic in 1967 had reached an all-time high, increasing 25% over the previous year. During the critical week 5-11 June (Arab-Israeli conflict) the daily group counts averaged 1.4 million; on June 14 the total was 1.9 million. A comparison of average daily group totals from 1955 to 1967 is given at Annex G. It should be noted that these figures include groups processed as well as transmitted and received. An additional "two-way half-duplex" circuit for traffic from NSA to CBNRC was initiated in December 1967, operating with KW-26 at 100 words per minute. This link, dubbed "NSA DELTA", brought to four the number of circuits between the two Centres.

14.89

It was difficult for NSA to keep CBNRC informed by message of the topics discussed in these "telecons". CBNRC felt "left out in the cold" temporarily on a number of occasions upon learning, by inference from subsequent correspondence, of decisions made by the other two Centres, decisions which had to be made without delay. In the spring of 1968 arrangements were made to enable O2 to engage by telecon in informal technical exchanges with NSA on current analytical problems. The telecon would take place just after that between NSA and GCHQ each Monday. Other groups in CBNRC were interested in having access to the telecon facilities, but only on a contingency basis. A three-way telecon arrangement, CBNRC-NSA-GCHQ, was mooted, but there were technical problems and the need for tri-centre discussions was not considered sufficient to warrant greater effort.

14.90 In January 1968 the Deputy Minister, DND, announced the intention to close the Oshawa Radio Transmitting Station (ORTS) in order to eliminate the high cost of manning, maintaining and operating what was considered a redundant facility. The system included a radio channel to act as back-up to the Ottawa-GCHQ portion of an NSA-GCHQ cable circuit, but

this had not been brought into use for many years. Continuing CBNRC-Alert communications would be assured by arrangements to relocate the southern transmitter terminal of the Alert circuit to "another DND station near Ottawa". Some consternation was felt at CBNRC, however, because deactivation of the HYDRA radio system would result in CBNRC losing the sole means of direct communication with GCHQ for twelve hours of each day, leaving only the twelve hours daily during which they had access to the transatlantic cable. CFHQ intended to cease transatlantic radioteleprinter facilities in December 1968, and invited CBNRC to use the intervening time to make alternative arrangements for communicating with GCHQ. By 18 April 1968 Canadian authorities had agreed to a proposal to provide a cable channel on a 24-hour basis for CBNRC-GCHQ working. External Affairs would assume the burden of the Canadian share of the additional costs. In mid-September UK agreement to the proposal was obtained. As NSA had also used HYDRA facilities, US concurrence was also secured. On 5 December HYDRA was deactivated and "UK ALFA went to cable, 24 hours a day". Thus, where two years earlier CBNRC-GCHQ communications had involved five separate circuits, only the cable circuit was now necessary. The demise of the HYDRA system came without fanfare. After performing reliably during World War II, it had rendered another 22 years of service as the main transatlantic carrier of SIGINT and diplomatic traffic. The UK Foreign and Commonwealth Office (FCO) took note of the splendid cooperation on what had "consistently been the best transatlantic HF circuit in service".

14.91 The year 1968 saw the closing down of two intercept stations - communications with Churchill ceased on 23 June and with Whitehorse on 6 July[20]. The CBNRC SIGINT Communications Network Diagram as of December 1968 is reproduced at Annex H, with a separate listing and description of circuits.

20. See para. 5.42

14.92

14.93

14.94 A Communications Centre planning team, composed of members from R(E&E), RA, R3 and R4, was set up in 1969 and tasked with the responsibility of proposing a new Comcentre concept, together with a program for implementation. Its objective was to propose an integration of communications and preliminary processing facilities, compatible with the M Group data processor, to meet Branch needs for the period 1973-1983. In January 1970, Coord/P sent a memorandum around to the Groups regarding changes anticipated during the period 1973-1983 including

computer-to-computer exchanges, telecon, facsimile and secure voice facilities and circuits terminating in Group offices.

14.95

14.96

14.97 Arrangements were made in 1969 for the transmission of SIGINT material from CBNRC to the Maritime Command Headquarters on the east and west coasts. In February on-line communication between Ladner and CANMARPAC, Esquimalt, B.C. was established, allowing CBNRC to use Ladner as a relay point to both Esquimalt and Inuvik. This resulted in an increase of 43% in traffic loading in the first three months, causing CBNRC to consider the advisability of increasing circuit speed to 100 w.p.m. or, alternatively, the establishment of a direct duplex circuit from CB to Inuvik. At the same time, approval was given for on-line communication of SIGINT material between Coverdale and CANMARCOM, Halifax, with Coverdale assuming the responsibility for relaying traffic between CBNRC and CANMARCOM. This gave rise to an immediate increase of 19% in line loading from CBNRC to Coverdale.

14.98 The emphasis on timeliness and the requirement for increased traffic handling capability led CBNRC in January, March and June 1970 to recommend upgrading to 100 w.p.m. the circuits from CBNRC to Alert, Inuvik, Ladner, Coverdale and Leitrim. Within months, however, this proposal was caught up in discussions involving the planned shutdown of two of the intercept stations and the initiation of circuits to two others[21]. A 100 w.p.m. circuit to Gander, Newfoundland, was activated on 3 June 1971 and communications with Coverdale ceased two days later. Another 100 w.p.m. circuit went into operation with Masset, B.C., on 16 July; contact with Ladner ended on 31 August and the 60 w.p.m. circuit was dedicated to Inuvik. It was not until 21 February 1972, however, that the CBNRC circuits to Alert and Inuvik were cranked up to 100 w.p.m.

14.99 Because of the nature of CBNRC's main function (SIGINT), the Branch had, in the late 1950s,

21. See para. 5.43

given up its World-Wide Routing Indicator and its listing in the routing indicator publications which were classified only RESTRICTED. Thereafter, messages for CBNRC transmitted over non-SIGINT nets were routed to Canadian Forces Headquarters and passed by courier to CB. At best this occasioned delays in delivery, and in the worst cases certain relay stations along the route refused to forward messages to an addressee not listed in ACP117 (the routing indicator publication). Permission was given by the CB Security Officer in February 1970 to have CBNRC listed in a RESTRICTED publication and the Branch obtained its own routing indicator.

14.100

s.13(1)(a)

s.15(1) - DEF

s.15(1) - IA

14.101

14.102

14.103

14.104 As average daily utilization of the data link climbed, consideration was given to the possibility of increasing the operating speed of the circuit. In March 1975 the problem of finding available line time was overcome by upgrading the high-speed circuit to 7200 b.p.s. This improved the

22. See para. 13.12

data handling capacity by a factor of 2.5. At the same time changes in the program brought about a significant reduction in the number of reruns. A further advance was the establishment of a "chatter capability" between CBNRC and GCHQ through development of the software at NSA for very little additional cost. This was to NSA's advantage, too, because it relieved technical personnel there of the responsibility of interpreting and relaying information between CB and GCHQ.

14.105

SAMSON and DELILA

14.106 Traffic totals increased about 5% each year in the early 1970s, and because world crises caused communications to peak to record levels periodically, CBNRC was studying methods to increase message handling and distribution capability and, if possible, to reduce operational costs. At the same time, the Department of National Defence was planning to automate its communications by the introduction of a common user system -- the SAMSON (Strategic Automatic Message Switching Operational Network) project. If DND could enlist the support of other communications users and convince them to join in the project, there would be a stronger case for the huge expenditures involved. Discussions began in the spring of 1972 between CFHQ and CBNRC regarding the DND proposal to integrate Canadian SIGINT communications in some manner with the SAMSON project.

23. See para. 13.10

During the next two years a basic concept for integration of communications was developed. It was agreed to have DND Intelligence Communications and SIGINT Communications handled by CBNRC using a message switch in isolation from the rest of the SAMSON system. A dedicated Intelligence communications switch, called a Local Distribution Message Exchange (LDMX), and involving a "stand-alone" sub-system named the Canadian Supplementary Military Network (CSMN), would provide communications for the whole intelligence community. It was to centre its operation through an automatic message switch at Carp. The overall SAMSON project received Treasury Board approval for activation of the first phase of the program in August 1975. The introduction by 1977 of an automated external relay function, the Ottawa Semi-Automatic Exchange (OSAX), was intended to eliminate the manual relay of traffic in the CBNRC Communications Centre. Integration of the Comcentre into the CSMN was to be accomplished by changing the existing torn tape relay to an automatic system.

14.107 Meanwhile, the objective in CBNRC, once relieved of the relay responsibility, was to develop its own automated system for traffic distribution and message preparation. Originally CB had planned to have the switch located in the Tilley Building, which would have allowed it to install a message distribution system for the whole intelligence community to be financed by the SAMSON project. Space considerations and other factors had argued against installation at CB, and the OSAX was eventually located at Carp. As a result, the availability of this particular message processor to provide an internal distribution system for the Branch was lost, and CB was left to supply and fund its own IDS (Internal Distribution System) for local dissemination of traffic. Incidentally, the IDS was originally slated to be called DELILA (DELivery Into Local Addresses)[24]. The upshot of all this was Project TERRIFIC, to prepare the accommodation and install new communications equipment in the CB

24. See para. 12.45

Comcentre in readiness for operation within the CSMN. This project was approved by the Treasury Board in February 1975; delivery and installation followed in the next two to three years. Although it was intended that receiver terminals would be located in user areas (i.e. Group secretariats or Sections), the problems of noise and of servicing the terminals with paper etc. during "silent hours" were found to defy early solution. Message preparation in the Group secretariats, however, was instigated in the ensuing years as MPF (message preparation facility) equipment became available.

Summary

14.108 In its 28 1/2 years of existence (1 September 1946 to 31 March 1975) the CBNRC Communications Centre had grown from a simple teletype office receiving and sending raw traffic in the clear to a sophisticated Comcentre equipped with the latest in technology not only in communications equipment but also in crypto devices. Starting with a few machines enclosed in two small rooms, handling mainly unencrypted traffic (a mere 1,000 to 1,500 groups of cipher and 12,000 groups of plain language daily) in 1946, it had progressed to a point where it was handling in excess of a million groups per day. Always in competition with other priorities for scarce finances, the communications office advanced in stages, each of which seemed to be interminable, yet on the whole, managed to keep pace with "state-of-the-art".

Page 1011

is withheld pursuant to sections

est retenue en vertu des articles

15(1) - IA, 15(1) - DEF

of the Access to Information

de la Loi sur l'accès à l'information

Page 1013

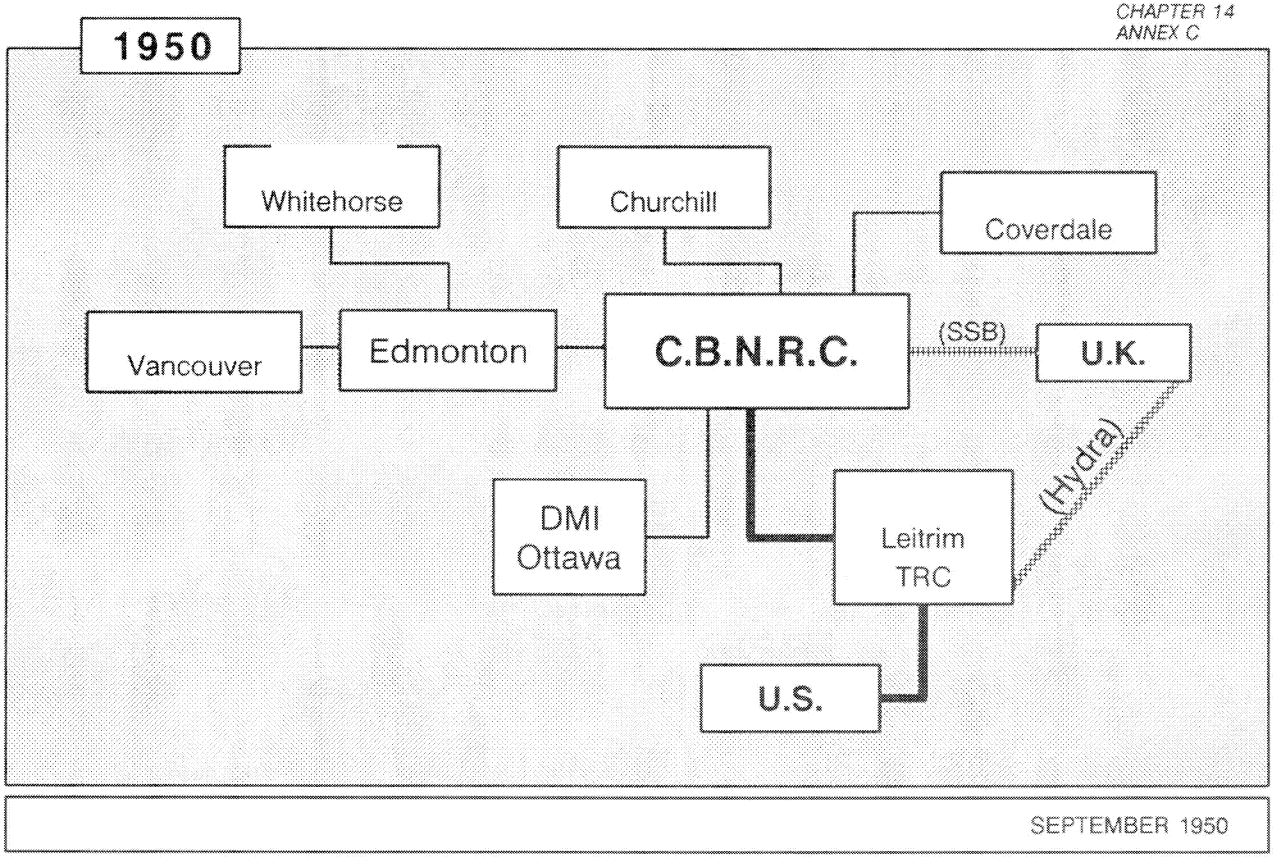
is withheld pursuant to sections

est retenue en vertu des articles

15(1) - IA, 15(1) - DEF

of the Access to Information

de la Loi sur l'accès à l'information



Page 1017

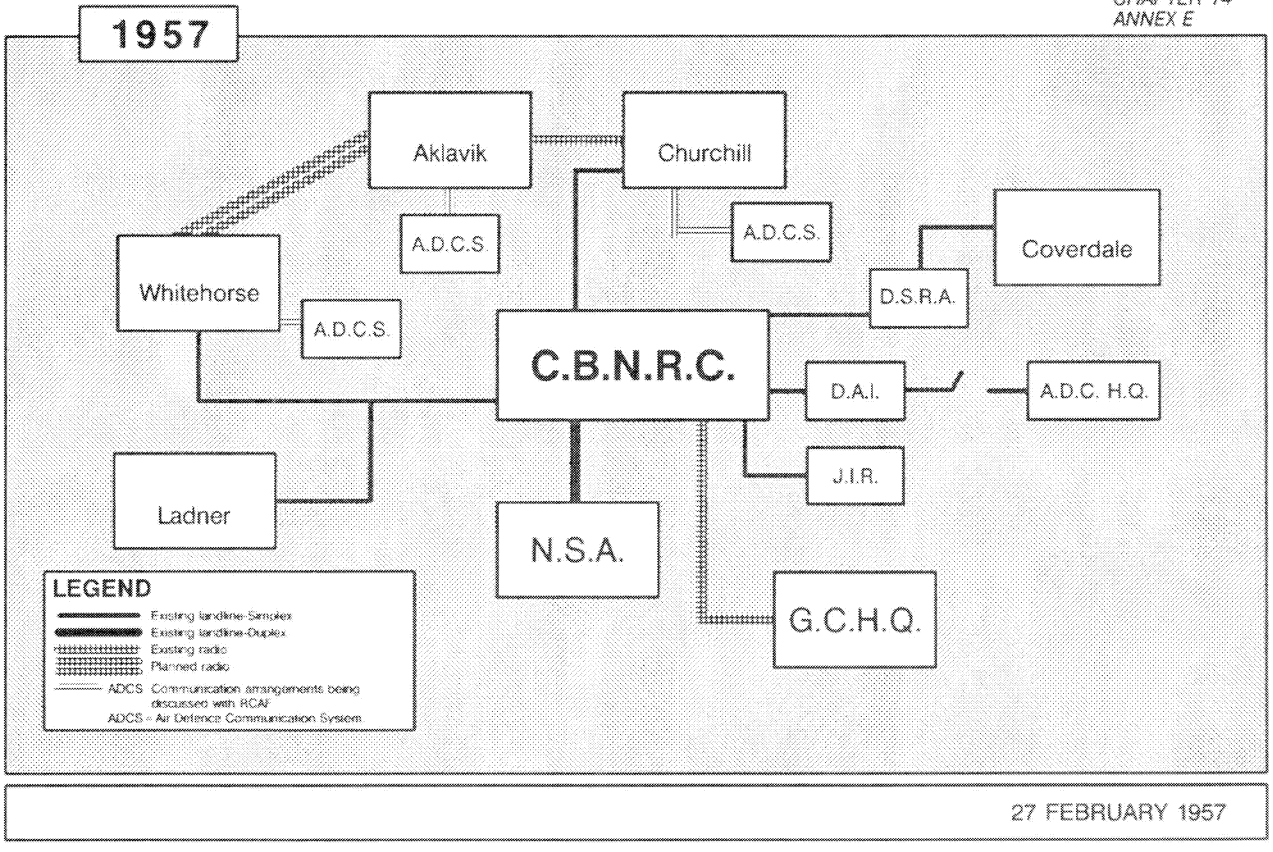
is withheld pursuant to sections

est retenue en vertu des articles

15(1) - IA, 15(1) - DEF

of the Access to Information

de la Loi sur l'accès à l'information



Page 1021

is withheld pursuant to sections

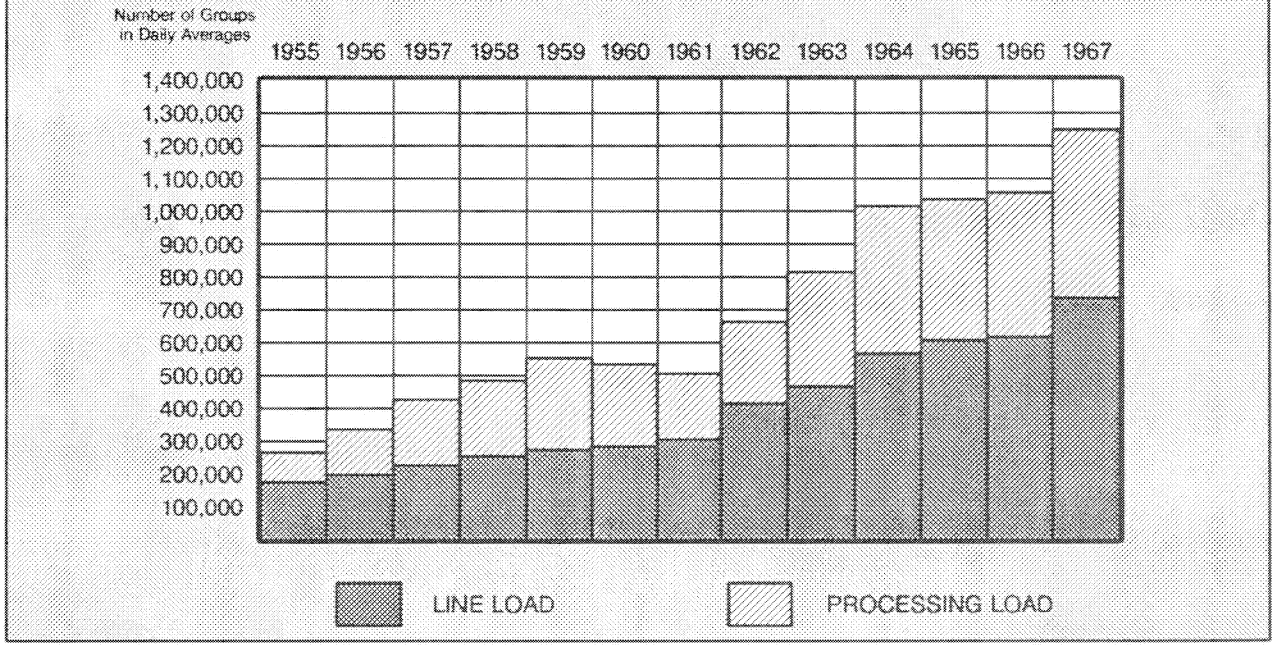
est retenue en vertu des articles

15(1) - IA, 15(1) - DEF

of the Access to Information

de la Loi sur l'accès à l'information

CBNRC COMMUNICATIONS OFFICE TRAFFIC LOAD



Page 1025

is withheld pursuant to sections

est retenue en vertu des articles

15(1) - IA, 15(1) - DEF

of the Access to Information

de la Loi sur l'accès à l'information

s.15(1) - DEF

s.15(1) - IA

COMMUNICATIONS CIRCUITS SERVING CBNRC TO MEET COMMITMENTS OF THE CANADIAN SIGINT ORGANIZATION

	TERMINAL IDENTITY	DESIG-NATION	SYSTEM	CIRCUIT NUMBER	LINE CO	LINE FUNCTION	SPEED	RESTO-RATION	LEASED BY	REMARKS	RENTAL
A		LTC	Cable to LTC via OCSF		Bell	Full Duplex	100 wpm	A	CBNRC	Charlie Fox-trot X-ray cable.	$45.00
B		Ft. Meade Washington D.C.	Landline		Bell	Full Duplex	100 wpm	A	CBNRC to US/CAN Border	Bell cct ngar to Border only. Now combined with DOT lines, for billing purposes only.	$94.10
C		Ft. Meade Washington D.C.	Landline via OCSF		Bell	Two two-way half Duplex	100 wpm	A	CBNRC to OCSF only	($22.50 + $22.50)	$45.00
D		Ft. Meade Washington D.C.	Landline		Bell	One two-way half Duplex	100 wpm	B	CBNRC	Bell cct to Moores Forks. Combined with DOT Telepac. for billing puposes only.	$94.10
E		Ft. Meade Washington D.C.	Landline via OCSF		Bell	One two-way half Duplex	100 wpm	B	Ext Alt. to US/CAN	This cct has dual use primarily exper-iencing CBNRC-Rockcliffe-USA Border.	
F		Ft. Meade Washington D.C.	To OCSF		Bell	Two two-way half Duplex	100 wpm	B	CBNRC	Overload CT/used only when NSA not using cable. ($22.50 + $22.50)	$45.00
G		Ft. Meade Washington D.C.	Landline		Bell	Full Duplex	60 wpm	A	CBNRC	Opscomm.	
H		Alert NWT	Landline to OCSF then H/F radio to Alert		Bell	Two two-way half Duplex	60 wpm	A	CBNRC to OCSF	Transmitter Oshawa via OCSF (Rck) Receiver Ottawa Wireless. ($21.22 + $18.00)	$39.22
I		Alert NWT	Landline to OCSF then H/F radio to Alert		Bell	One two-way half Duplex	100 wpm	B	CBNRC to OCSF	Employed as 60 wpm. Engineering cct.	$22.50
J		Alert NWT	Landline microwave to troop-scatter & L/F radio		Bell	Full Duplex	60 wpm	A	CAF to G. Bay	Used as full Duplex. This cct follows facilities of USAF early warning system to Thule then L/F radio to and from Alert	$1829.76
K		Ladner BC	Landline		CN	Full Duplex	60 wpm		CAF	Inuvik now terminated at Ladner.	
L		Coverdale NB	Landline		CP	Full Duplex	60 wpm	A	CAF	Entry into Western Atlantic D/F network through	
M		Lettrim	Landline		Bell	Full Duplex	60 wpm	A	CBNRC	Lattrim co-locatad with OWS.	$34.03
N		Local	Landline		Bell	Full Duplex	75 wpm	A	CAF		
O		Local	Landline		CN	Full Duplex	75 wpm	B	CAF		
P		Local	Landline		CN	Full Duplex	75 wpm	B	CAF	Overload use only.	

Update to 10 DECEMBER 1968. D. Milne

Copies: Coord/T, R, R3, R4.

Page 1029

is withheld pursuant to sections

est retenue en vertu des articles

15(1) - IA, 15(1) - DEF

of the Access to Information

de la Loi sur l'accès à l'information

Chapter 15

COMSEC in Canada before CBNRC

Chapter 15 - COMSEC In Canada Before CBNRC

Early Ignorance

15.1 COMSEC in at least some Canadian Government Departments, up to and including the early years of World War II, appears to have amounted to little more than the motto "Be Careful". There is no indication that any of the communications security techniques were known, let alone practised. There existed no group during the war dedicated to COMSEC in Canada comparable to the more or less centralized organization for SIGINT interception[1]. Even today each Deputy Minister is responsible for security within his own department, but in the early forties there was no one to provide COMSEC advice. To be sure there were codes and ciphers, but the procedures for their use were so loosely applied that in many cases the intended purpose was defeated.

15.2 In the 1930s and early 1940s messages of lower security classification were encoded using the "Government Telegraph Code" produced by the UK Government in 1932. Heavy usage of this code rendered it effective only as a brevity system. The Department of Trade and Commerce was informed in May 1952 by the Security Panel Committee (SPC) on Codes and Ciphers that the code had no security value. It was withdrawn from use in DND in 1958, and in External Affairs and Trade and Commerce in 1966. Nevertheless, it was still used for security purposes by Government House in Ottawa until November 1983, when it was replaced by NOREEN.

Code-Books and "One-Time Pads"

15.3 Higher classified messages were encrypted in the "Dominions Office Cypher", in which four-figure groups from a basic code-book were enciphered using one-time pads and "non-carrying subtraction". This would have been a secure system if it had been used properly, but this was not always the case. In the

1. See end of para. 1.11

"Prime Minister's Code Room" (Mackenzie King held both portfolios, Prime Minister and Secretary of State for External Affairs), one-time pads (OTPs) were used more than once; when the pads were filled, the cipher clerks were instructed to erase the pencilled entries in order that the "one-time" groups might be reused.

15.4 Perhaps the reuse of one-time pads was dictated by their scarcity and by the cost and effort of replacing them; they were produced in the UK, and wartime conditions made it difficult to obtain them readily. At the 100th Meeting of the British Cypher Security Committee (CSC) on 7 March 1945 it was stated that "all Dominions Office cypher material was carried by the Admiralty (i.e. by ship) save in very exceptional circumstances ... that distribution by this method was very slow". The inconvenience and particularly the cost of security have always been major inhibiting factors. For example, certain departments (e.g. Trade and Commerce) preferred to risk the compromise of an occasional classified item rather than to accept the expense of providing "specially cleared Canadian staff at posts where local employees were considered satisfactory" to meet normal requirements. It is also possible, however, that the users of this cipher did not realize the significance of the term "one-time pad", i.e. that it would not provide security unless the key groups were used only once.

TYPEX

15.5 The introduction of TYPEX, a cipher machine using rotor wheels, into the External Affairs Cipher Office in late 1941 or early 1942 brought increased security to diplomatic communications, although the practice of allowing operators to make up their own indicators in the early days probably introduced a degree of vulnerability. Apart from those messages sent on TELEKRYPTON channels, most External Affairs messages were sent by commercial cable facilities, and so could be available for exploitation, although cable is much less vulnerable than radio. TYPEX equipment and enciphered code-book systems were also

used by the Defence Services and by the Joint Discrimination Unit (JDU)[2] during the war.

The TELEKRYPTON

15.6 A commercial device called TELEKRYPTON (T.K.) was introduced in April 1942 for communication between the Department of External Affairs and the Canadian Embassy in Washington. This device was a "mixer" which combined the plain text message tape with a key tape. It would have been secure if the key tape had contained random key and was used only once; however, the key tape was made locally with a Teletype reperforator using as "key" a paragraph taken from a newspaper or magazine. This tape was then formed into a loop which was stepped through the TELEKRYPTON with the plain text tape, using the key again and again until the key tape became so frayed that it had to be replaced. There were no COMSEC courses then, and the cipher clerks were simply obeying instructions. At the beginning of each day the operator at each post on the network set his own tape at a position agreed in advance, and each tape was then run round continuously when cipher messages were being transmitted. The Minutes of the 98th Meeting of the British CSC on 7 February 1945 make it obvious that the TELEKRYPTON was only intended to be used with one-time tape. A T.K. machine belonging to British Security Coordination (BSC) in New York was installed in the Examination Unit (XU)[3] on Laurier Avenue, also in April 1942, and was later moved to Guigues Street. Expenses for this T.K. operation (salaries and rental of equipment) for 1943 amounted to $42,000. When BSC requested the return of the equipment in August 1944, the Examination Unit fell back on TYPEX.

15.7 The T.K. equipment held by External Affairs was later turned over to CBNRC, as indicated in a letter from Director CBNRC to the Department of National Revenue in March 1951: "TELEKRYPTON equip-

2. See para. 1.9
3. See para. 1.8

ment previously imported into Canada by the Department of External Affairs from the Canadian Embassy, Washington, D.C., is now held by CBNRC and will be used solely for experimental and research purposes." External Affairs assured CBNRC on 28 March 1951 that the T.K. unit had been imported into Canada duty free. Incidentally, prior to 1947 most cryptomaterial, including cipher machines, used by the Canadian Government was provided free of charge by the UK.

The Appleby Scrambler

15.8 What was claimed in 1944 to be an improvement on T.K. equipment was the Appleby Teletype Scrambler, Model No. 2, named after its inventor, a Mr. Appleby of Canadian Pacific Telegraphs. The fundamental difference between the two was that in the Appleby device the encipherment and transmission formed a simultaneous process (i.e. were "on-line"), whereas with the T.K., at least as employed by some users, the encrypted message would be produced on a separate tape, which was then fed into a transmitter. Both devices could have provided security if used with random one-time tape. The Appleby scrambler was, however, also sometimes used with an "endless" tape; for example, the Canadian Ministry of War Transport (MOWT) used a tape loop made up of 500 characters, which was changed daily and reversed at noon. The Directorate of Naval Intelligence had assured MOWT that the device would protect shipping movements if used with a one-time tape. This precaution was obviously misunderstood or ignored. CBNRC obtained the specifications for making five-unit key tape (usable with the T.K. or Appleby devices) from the UK in February 1947. A tape generator was set up in the communications room, and shortly thereafter a security modification was incorporated as the radiation/TEMPEST problem came into prominence. (The TEMPEST problem is covered in Chapter 24.)

Local Initiatives

15.9 In general, there was a tendency for some Government departments to resort to local methods in

an attempt to provide security. One cipher office (the RCMP) would add "5000" to each key group the second time the "one-time pad" was used. This kind of insecure practice was not uncommon. Even today many communicators think they can easily invent a secure means of communication. Warnings against such naiveté were issued but went unheeded. A caution against the use of "local ciphers" (systems developed by non-experts in the crypto field), contained in the Minutes of the 94th Meeting of the British CSC, was communicated by the Dominions Office, Downing Street, dated 21 December 1944, to the Department of External Affairs Cipher Office: "there was still a number of local ciphers in use outside the United Kingdom which had little security value but which were considered by their user to be secure ...." The covering letter from H.W. Hart, Dominions Office, to A.L. Hall, External Affairs, stated "The Cipher School have felt rather uneasy recently over the reported existence and bad quality of ciphers prepared by certain Colonies ... for purpose of local communications ... able to break them down completely in a matter of hours ... were thought by the holders to be perfectly safe ... obviously child's play to the experienced Government cryptographer ...". The improvements achieved after the creation of CBNRC, including the acquisition of ROCKEX machines and the production of keying material in CB, are detailed in Chapters 17 and 19.

Chapter 16

COMSEC Policy and Committee Structure

Annexes:

CHAPTER 16 - COMSEC Policy and Committee Structure

Introduction

16.1 From time to time COMSEC policy has found itself under the direction of the same authority as SIGINT policy, partly because it has always been difficult to distinguish between security and intelligence, and also because COMSEC provided (and still provides)
COMSEC and SIGINT have usually been collocated because, as someone aphoristically stated, they are the two sides of the same coin

Thus the development of the COMSEC committee organization is to some extent covered in Chapter 2.

16.2 The chronological development of the committees concerned with COMSEC is set out at Annex H, with their subordination and dates of inauguration. The establishment and growth of the COMSEC committee structure were closely interwoven with the development of the Canadian COMSEC Agency as dedescribed in Chapter 17.

The CRC and Communications Security Group

16.3 COMSEC policy problems were handled by the Communications Research Committee (CRC) from its establishment in June 1946. The membership and functions of the CRC are described in paragraph 2.4. Its COMSEC responsibility was formalized at the CRC's 12th Meeting on 5 December, when it was agreed that the Committee should control Cipher Security Policy for the Services and the Department of External Affairs[1]. In June 1948, the Communications Security Group (CSG) was set up as a sub-committee of the CRC with representatives from External Affairs, the three Services and CBNRC, to deal with cipher security problems of user departments, although

1. See end of para. 2.6

control of cipher security policy was retained by the CRC. The formation and terms of reference of the CSG were promulgated in CRC/73, dated 5 June 1948, relevant portions of which are given at Annex A.

Conflict with DND

16.4 Difficulties arose later in the year when it was realized that there was a conflict between the terms of reference of the CSG and those of the SCSC (Security and Cryptographic Sub-Committee of the Joint Telecommunications Committee (JTC) of the Department of National Defence). The SCSC consisted of the Service members of the CSG. The Services wanted to be responsible for internal jurisdiction and directives within their own departments; they would rely on the CSG for specialist technical information but they wanted the CSG to "recommend" and leave it up to the Services to "act". The Chairman, at the 36th Meeting of the CRC on 4 February 1949, agreed so long as the "recommendation" was definitely accepted. The terms of reference of the CSG were thereupon amended to read as in Annex B.

16.5 In June 1950 the Director of Military Intelligence (DMI) proposed to the CRC "that the production and security of ciphers should be under the direction of a separate committee, which would not have to include intelligence representatives"[2]. The Directors of Signals met to prepare terms of reference for a proposed Cipher Policy Committee (CPC), and to decide upon the relationship between such a committee and CBNRC. The Chairman CRC and the Director CB (perhaps fearing that control of cipher policy might get into the wrong hands) pointed out that "split control over various facilities in CB would be neither workable, nor acceptable to NRC, and therefore suggested that, should a separate Cipher Policy Committee be established, it should exercise its direction of CB through the CRC". The RCN and the RCAF Directors of Communications did not agree that a separate committee for cipher policy was either

2. See para. 2.11

necessary or desirable and proposed as an alternative "that the CR Committee continue to be responsible for cryptographic matters of a policy nature ... and that the CR Committee function in two sections, with full committee meetings as required". They argued: "Canadian government users, including the Services, employ almost exclusively cryptographic aids of UK or USA origin. To a large degree, the policy governing the use of such aids is prescribed by the appropriate policy body in the UK or USA and we must necessarily conform to such policy as a condition of using such aids." While Canadian users continued to employ crypto equipment of UK or US origin, by 1950 most other COMSEC aids such as key tape, key settings and one-time pads were being produced in Canada by CBNRC, and the policy management of cipher security consumed more of the CR Committee's time than most of the members were prepared to give, since their main concern was for SIGINT matters.

The Security Panel Committee on Codes and Ciphers (SPCCC)

16.6 Accordingly, as COMSEC activities expanded and became more diverse and complex, the CRC concluded that its responsibilities in the area of SIGINT constituted a full-time occupation, and that cipher security policy should be assigned to a body created specifically for that purpose. Thereupon the Privy Council Security Panel, at the suggestion of the Department of External Affairs, recommended the formation of a committee of the Panel to deal with the problems of cipher security. In March, 1952, the SPCCC (Security Panel Committee on Codes and Ciphers) was set up to answer "the need for a single central authority in the field of cipher security to maintain consistent standards and practice in all government departments using codes and ciphers". It was charged with examining in detail all problems connected with the use of codes and ciphers, correcting misuse where possible, and reporting to the Security Panel on the means necessary for dealing with these problems on a permanent basis. The SPCCC Chairman, who also chaired the CRC, "pointed out that this authority would also be concerned to some extent with questions of physical

security arising for instance, from the need of safe-guarding codes and ciphers; with problems of cipher production; and with relations with equivalent bodies in the United Kingdom and the United States".

16.7 On the latter subject, attention was drawn to the fact that in communications matters the Services and the Department of External Affairs were regularly in contact with corresponding authorities in the UK and the US[3]. "The Committee agreed that where appropriate these relations should continue, but that the Committee itself should take preliminary steps to establish relations with comparable authorities in the United Kingdom and the United States on general matters of cipher policy." (Minutes of the First Meeting of the SPCCC, 31 March 1952.) The SPCCC composition and terms of reference are given at Annex C.

COMSEC Liaison

16.8 A working relationship was established by the SPCCC with the Cipher Policy Board of the United Kingdom for the exchange of information on problems related to cipher security. As will be seen, arrangements were also made with the Coordinator of USCIB in Washington that communications from Canada might be referred to him for transmission to the US authorities concerned in the field of crypto security. This access to US COMSEC authorities was long overdue. The Director CBNRC had had to ask GCHQ for a UK security appraisal of a US crypto device in September 1950 because, as he pointed out: "CSG's liaison with the USA on cipher security is practically non-existent." Indeed, GCHQ and US Armed Forces Security Agency (AFSA) negotiated COMSEC arrangements for CBNRC, sometimes without notifying the latter. The Head of CB's Test and Design (T&D) Group was irritated, to say the least, when he discovered in April 1953 that GCHQ (Captain Hodges) had arranged with AFSA (Captain Enderlin) in August 1951 to discontinue a private cryptochannel (COMINT) between AFSA and CBNRC! So the Chairman CRC wrote to

3. See para. 11.101

Major General R.J. Canine, the Director of AFSA, on 13 May 1952 notifying him of the creation of the SPCCC "to deal with all cryptographic questions of concern to the government" and expressing the hope that there might be an exchange of information between the SPCCC and AFSA. General Canine, who was also Coordinator of the US Communications Intelligence Board (USCIB), replied in the latter capacity that such matters were the subject of current deliberations in the US, and that, until a decision was made as to which US body was responsible for cryptographic policy, communications should be addressed to him as Coordinator, USCIB, and he would refer them to the cognizant authority. The subject of COMSEC Liaison is discussed in greater detail in the Section beginning at paragraph 11.100.

COMSEC Committees and Groups 1952-1955

16.9 At its 5th Meeting (21 May 1952), the SPCCC reorganized the CSG as a "technical working group", changed its name from the "Communications Security Group" to the "Cipher Security Group" and approved proposed new terms of reference as shown in Annex D. As a committee of the Security Panel, the SPCCC derived its authority from the Cabinet, and matters that could not be resolved by the Committee would be referred through the Chairman of the Security Panel to the Cabinet Committee on Emergency Measures.

16.10 The Cipher Machine Production Group (CMPG) was set up following agreement on its organization by the SPCCC at its 8th Meeting on 15 September 1952. The Committee agreed that the "functions of this group should be limited to investigating the possibility of the production of approved types of cipher machines and associated spare parts in Canada". The responsibility for the design and development of crypto equipment was put in abeyance for the time being.

16.11 In October 1952 the name of the SPCCC was changed to the Cipher Policy Committee (CPC). Responsibility for cipher security policy shifted during the next three years as the result of changes

in jurisdiction among committees. The Senior Committee (SC) was renamed the Communications Security Board (CSB) in 1953, and at the same time the Head of the Defence Liaison (DL(2)) Division of the Department of External Affairs, G. de T. (George) Glazebrook, was named Director of Communications Security (DCS)[4]. At first the CSB did not include COMSEC in its terms of reference, but later the responsibility for general policy control over communications security was transferred from the Security Panel to the CSB[5]. This shift placed the CPC and its two sub-committees, the CSG and CMPG, under the aegis of the CSB. The DCS served as Chairman of the CRC, Executive Agent for the CSB and Chairman of the CPC. The secretary of the latter committee was provided by CBNRC. The CPC assumed broader responsibility for COMSEC generally, "to tidy up the COMSEC organization by giving the Cipher Policy Committee responsibility for transmission security and for establishing Canadian communications security standards with some authority for ensuring that these standards were observed". Details of the revised COMSEC structure, the new terms of reference of the CPC and the expanded communications security task assigned to the Director CBNRC, were set forth in CSB/45, which was approved by the CSB at its 17th Meeting, held on 24 May 1955, and is attached to Annex E. In the past, CBNRC and the COMSEC committees were responsible only for cipher (crypto) security; henceforth COMSEC (communications security) would be considered to include crypto security, transmission security and the physical security of classified communications equipment and material, and these were to constitute the responsibilities of the CPC, the CSG and CBNRC COMSEC (T Group). The JTC agreed in principle to the extension of CPC responsibility to include COMSEC matters generally, and to act itself on COMSEC matters as a "Service Device" to implement CPC decisions within the Department of National Defence.

4. See para. 2.13
5. See Annex E and para. 2.22

Liaison with NATO

16.12 A NATO Standing Group Memorandum (SGM-620-54, dated 14 September 1954) requested each member nation to "designate a communications security agency" authorized to communicate on COMSEC matters, both civil and military, with the NATO Standing Group Communications Security and Evaluation Agency (SECAN), Washington. The SECAN responsibility was exercised by NSA/COMSEC. After deliberation, the CPC decided at its 26th Meeting, on 5 November 1954, that it was the proper authority to be designated as the Canadian agency to communicate with SECAN on COMSEC matters, and so informed NATO.

COMSEC Awareness Increases

16.13

The CSPC and ELSEC

16.14 Until 1959, the responsibilities of the COMSEC committees could be summarized as: "formulating, recommending and maintaining comprehensive policies in the field of communications security, including transmission security, cryptographic security and the physical security of classified communications equipment and material." In that year,

"To meet the ever expanding requirements for good standards of COMSEC and to cope with the growing complexity of the art, which had come to involve the security of non-communications (electronic) as well as communications transmissions, the evaluation of security hazards associated with electromagnetic and acoustic radiation from cryptographic and communications equipment installations and other similarly complex technical matters", the CPC in 1959 put forward to the CSB certain proposals for further changes in the Canadian COMSEC organization. The revised COMSEC structure is set forth in CSB/82 (Annex F), which was approved by the CSB at its 25th Meeting held on 13 October 1959. The major changes effected by CSB/82 may be summarized as follows:

a) The terms of reference of the CSB were expanded to include responsibility for policy control of electronic emission security (ELSEC) as well as communications security (COMSEC);

b) The title of the "Cipher Policy Committee (CPC) was changed to the "Communications-Electronic Security Policy Committee" (CSPC), and that of the "Cipher Security Group" (CSG) to the "Communications-Electronic Security Group" (CSG); their terms of reference were revised to include responsibility for electronic emission security and the membership was extended to include representatives of the Defence Research Board (DRB) and the Department of Defence Production (DDP), as well as representatives of other departments and agencies of the Government on an "as required" basis; and

c) The COMSEC task assigned to the Director, CBNRC, was revised to include responsibility for providing technical advice and support on all ELSEC and COMSEC matters.

16.15 A significant change in the wording of the terms of reference of the CSPC was also made, which, while it apparently made no difference in practice, served to assuage the sensitivities of the Department of National Defence. The 1955 version, CSB/45 (Appendix B to Annex E), had given the CPC responsibility "to establish and ensure the execution of policies and procedures necessary to maintain high and uniform standards of COMSEC within all departments and agencies of Government concerned". The DND Deputy Minister questioned the propriety of the CSPC having executive responsibility over Service operating policies. This implication had obviously slipped past the critics when the original terms of reference of the CPC had been approved by the CSB in 1955. The new proposal had retained the exact wording of the particular paragraphs in the previous paper, with the simple addition of the words "non-communications transmissions". In CSB/82, the words were changed to read "to recommend policies and procedures ..." (Appendix A to Annex F). The CSPC was an advisory committee only, with no executive authority. Its responsibility was to formulate COMSEC policies and to recommend them to the CSB for consideration.

The IPC and ICSI, SAC and CSC

16.16 The authority and responsibility for coordinating and maintaining general policy direction of COMSEC in Canada passed to the Intelligence Policy Committee (IPC) which was formed in April 1960 as successor to the CSB[6]. The COMSEC organization outlined in CSB/82 (Annex F) was adopted without change and incorporated into IPC/1-60 and IPC/3-60. This hierarchy, IPC-CSPC-CSG, endured for 12 years, until reorganization resulted from a study of the Isbister Report (on intelligence operations) of 1970.

6. See para. 2.23

The new structure, instituted in 1972, was headed by the Interdepartmental Committee on Security and Intelligence (ICSI) at the Deputy Minister level[7]. The CSPC and CSG were disbanded in March 1972. Under the ICSI, COMSEC policy matters were handled by the Security Advisory Committee (SAC) which also took the place of the Security Sub-panel for security matters other than COMSEC. Under the SAC, a new COMSEC policy committee, the Communications-Electronic Security Committee (CSC), was formed with membership and terms of reference almost identical to those of the CSPC/CSG; the only significant changes were that the Director CBNRC became Chairman of the CSC, and provision was made with respect to the conduct of international arrangements, in which "policy" aspects would be referred to the SAC.

Canadian COMSEC Community

16.17 As more and more Government officials became aware of the vulnerability of classified communications, other departments were invited to send representatives to the COMSEC committees. These departments and agencies came to be known collectively as the "Canadian COMSEC Community". Members of the "Canadian COMSEC community" dealt directly with CBNRC on COMSEC matters, but other government departments were scarcely aware of the existence of a COMSEC organization. In most cases they would look to the RCMP or DND for communications security advice and guidance, and would in turn be referred to CBNRC and the CSC if substantial assistance was required.

Department of Communications (DOC) and COMSEC

16.18 In mid-1969 there was an attempt by the Department of Communications (DOC) to assume control of the COMSEC responsibilities of CBNRC. Richard Gwynn, Executive Director to Minister of Communications Eric Kierans, insisted that COMSEC be included in the DOC Telecommission's terms of

7. See para. 2.29

reference, as he wished to review COMSEC policy and operations in Canada. He called a meeting of representatives of the RCMP and of the Departments of External Affairs and National Defence, but excluded CBNRC. The Director CB drafted a letter for signature by E. R. Rettie, Chairman of the CSPC, to the Deputy Minister of Communications emphasizing the "sensitivity of the subject and the need to limit information on the policies, procedures and techniques utilized in Canada to the minimum number of government personnel possible and yet ensure an adequate standard of communications security". The letter pointed out that the Intelligence Policy Committee (IPC) was responsible for intelligence and security matters in Canada, that the CSPC was responsible to the IPC for all interdepartmental communications security matters, and that the executive agency was CBNRC. It suggested that the conflict might be resolved by having DOC name a suitably cleared and indoctrinated senior officer to attend CSPC meetings, and by having the Minister of Communications indoctrinated and briefed on the functions and modus operandi of CBNRC. The controversy continued for the next five years, however, and was only resolved after the Inter-departmental Committee on Security and Intelligence, at its meeting on 4 September 1974, recognized that there was a possible overlap between the mandate of DOC and that of CBNRC in the area of secure communi-cations. There followed discussions between DOC and CBNRC and Treasury Board officials "to resolve possible misunderstandings and to clarify the definition of COMSEC responsibilities". The statement of the respective mandates and responsi-bilities, which was accepted by the Deputy Minister of Communications and the Director of CBNRC in October, is given at Annex G; the stated COMSEC responsibilities of DOC are summarized below.

16.19 At their 6th Meeting on 26 September 1972 the SAC had agreed that the Department of Communications should represent the departmental interests of federal departments not having a formal COMSEC organization, in much the same way that the RCMP and the Department of Supply and Services (DSS)

interfaced with provincial and municipal police and Canadian industry respectively, on matters requiring COMSEC guidance. The COMSEC responsibilities of the DOC were approved by Treasury Board, and funds for the fulfilment of their obligations were approved by TB 726153 in April 1974. It was considered at that time that the DOC, "as part of its approved objective to 'foster, develop, and extend telecommunications services to obtain optimum benefits for Canada in the short term and long term' has a responsibility to participate in the formulation of federal government COMSEC policy". This responsibility was considered to be discharged through active membership in the interdepartmental committee structure which provided policy formulation and guidance, and through a close working relationship with CBNRC.

Excerpt from CRC/73 dated 5 June 1948 Concerning the Establishment of the Communications Security Group

C.R.C Cipher Security Organization

1. In accordance with decisions made by the C.R. Committee during the 29th meeting held on 6 May 1948, the cipher security organization as controlled by the C.R. Committee will be carried out as indicated below.

2. Communications Security Group

A sub-committee of the C.R. Committee will be formed to coordinate the cipher security problems of the three Services and the Dept. of External Affairs. This sub-committee will be known as Communications Security Group. The membership and the terms of reference of this group will be as follows:

Director Signals Division Navy (or his rep.)
Director of Signals Army (or his rep. and one other member)
Director of Signals R.C.A.F. (or his rep.)
Communications Officer, Dept. of External Affairs (or his rep.)
Director of CBNRC (or his rep.)
Head of Test and Design Section of CBNRC

The Chairman of this group should be one of the members on a rotational basis. The secretary could be provided from the "Test and Design" Section of C.B.

Terms of Reference of the Communications Security Group

(i) To co-ordinate and keep under review the security of the Codes and Ciphers used by the Services and the Department of External Affairs. In case of other cipher using Government Departments their cipher security problems will be passed from the Chairman of the Security Panel to the Chairman of the C.R. Committee for the necessary action.

(ii) To submit to the C.R. Committee important questions of Cipher Policy affecting the Canadian users of ciphers.

(iii) To implement the directives issued by the C.R. Committee on all matters of cipher security.

Terms of Reference of the CSG (as amended at the 36th Meeting of the CRC on 4 February 1949)

(i) Under direction of the C.R. Committee to coordinate and keep under review the security of the code and cipher systems used by the Services and the Department of External Affairs.

(ii) To submit to the C.R. Committee important questions of cipher policy affecting the Canadian users of ciphers.

(iii) To advise the Departments of National Defence and External Affairs on matters covered in (i) and (ii) above.

(iv) To refer, when necessary, recommendations concerning ciphers and cipher security through the C.R. Committee for consideration by the Security Panel.

(v) The CSG, less the External Affairs member, will also act as the Security and Cryptographic Sub-Committee of the JTC. As such, the group will report to the JTC, and will be guided by the terms of reference of the JTC Sub-Committee.

The SPCCC, at its first meeting, 31 March 1952, laid down the following terms of reference for itself:

(i) that the Committee should be called the Security Panel Committee on Codes and Ciphers, and noted that it would, from its general terms of reference under the Security Panel have authority for an interim period to deal with questions of cipher security in all Canadian government departments and agencies in Canada and abroad;

(ii) that the Committee should consist of representatives of each of the three Armed Services, the Department of External Affairs, the Communications Branch of the National Research Council, and the Privy Council Office;

(iii) that in matters of physical security arising indirectly from cipher security requirements, the Committee would have the advantage of easy reference to the Security Panel itself;

(iv) that to carry out the detail of its work the Committee would require a subordinate technical group, that such a group existed and should be given new terms of reference under the Committee;

(v) that the Committee should immediately take preliminary steps towards establishing liaison with equivalent organizations in the United Kingdom and the United States;

(vi) that at a later date the Committee would report to the Security Panel as to how the problems of Cipher Security might best be handled on a permanent basis.

Chapter 16/Annex D

7 April 1952

Terms of Reference of the Cipher Security Group

(i) Under direction of the Security Panel Committee on Codes and Ciphers to examine and keep under review all aspects of cryptography, crypto security, production and printing.

(ii) To submit to the Security Panel Committee on Codes and Ciphers important questions of general crypto policy affecting Canadian users of codes and ciphers.

(iii) To advise all Civil and Service Departments on matters covered in (i) and (ii) above through appropriate channels. This will be accomplished in the case of the Department of National Defence by liaison between the CSG and SCSC.

(iv) To refer when necessary, recommendations concerning cryptography and crypto security, production and printing to the Security Panel Committee on Codes and Ciphers for consideration.

(v) To secure the carrying out by all cipher-using departments of the directives received from the Security Panel Committee on Codes and Ciphers.

MEMBERSHIP

It is suggested that the regulation governing membership of the CSG be amended so as to permit more than one representative of each department. This is in accordance with UK policy in

regard to CSC and is considered advisable since it is difficult for one specific representative to be fully qualified on all the varied subjects that are likely to come up for discussion from time to time.

On this basis suggest membership be as follows:

- Chairman (as at present or Head of T&D Group)
- Representatives of Directors of Signals of each of the three Defence Services
- Representatives of Department of External Affairs, Communications Section
- Representatives of T&D Group, CBNRC
- Representatives of other Civil Departments (as authorized by SPCCC)
- Secretary (to be selected from staff of T&D Group, CBNRC)

Chapter 16/Annex E

18 May 1955

MEMORANDUM FOR THE COMMUNICATIONS SECURITY BOARD

Canadian Communications Security (COMSEC) Organization

The Cipher Policy Committee has reviewed the existing Canadian communications security (COMSEC) organization. As a result of this review, and after consultation with the Joint Telecommunications Committee, certain recommendations, which are intended to provide more effective security control of procedures and techniques employed on our national communications networks, are presented in the attached paper CSB/45.

2. The proposed changes are summarized as follows:

(a) Responsibility for general policy control over COMSEC matters should be transferred from the Security Panel to the Communications Security Board.

(b) The Cipher Policy Committee should undertake executive responsibility for all aspects of communications security under the authority of, and responsible to, the Communications Security Board (Appendix "B" to CSB/45 refers).

(c) The Joint Telecommunications Committee shall be responsible for co-ordinating and maintaining, within the Department of National Defence, COMSEC policies and procedures as approved by the CPC.

3. The change suggested at para. 2(a) above, which should provide more effective control of COMSEC matters from an operational aspect as the membership of the Board is more representative of the major cipher-using Departments, is in accordance with a proposal made by the Deputy Minister of National Defence at the 16th Meeting of the CSB. The changes proposed at para. 2, sub-paras. (b) and (c) above, are considered essential in order to provide unified policy control and to enable the designated COMSEC authority to take cognizance of all matters pertaining to crypto security, transmission security and physical security of classified communication equipment and material. The Joint Telecommunications Committee has indicated agreement in principle with these proposals and is prepared to seek the approval of the Chiefs of Staff Committee to amend the JTC terms of reference accordingly.

4. For your information, the communications security mission assigned to the Director, CBNRC, under the direction of the CPC, in Appendix "C" to the attached paper, does not constitute an actual change of policy. It merely provides confirmation of the duties and responsibilities now being undertaken by the Director, CBNRC, in the field of communications security.

(Signed by) G. G. Crean,
Chairman,
Cipher Policy Committee.

Attachment to Annex E

18 May 1955

CSB/45

CANADIAN COMMUNICATIONS SECURITY (COMSEC) ORGANIZATION

INTRODUCTION

1. Communications security (COMSEC) is defined as "the protection resulting from all measures designed to deny to unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such a study". Communications security includes, - transmission security, crypto security, and physical security of classified communication equipment and material. These terms are defined as follows:

(a) Transmission Security - "that component of COMSEC which results from all measures designed to protect transmissions from unauthorized interception, traffic analysis and imitative deception".

(b) Crypto Security - "that component of COMSEC which results from the provision of technically sound cryptosystems and their proper use".

(c) Physical Security - "that component of COMSEC which results from all measures necessary to safeguard classified communication equipment and material from access thereto or observation thereof by unauthorized persons".

2. This paper presents a brief review of the present Canadian COMSEC organization and makes

certain recommendations, which are intended to provide more effective control of procedures and practices employed on our national communications networks.

GENERAL REVIEW

3. The Cipher Policy Committee (CPC), as presently organized, functions as a committee of the Security Panel. As such, it derives its authority from the Cabinet. Matters which cannot be resolved at Committee level are referred to the Cabinet Committee on Emergency Measures through the Chairman of the Security Panel. The present membership and terms of reference are as shown at Appendix "A".

4. The Cipher Policy Committee constitutes a central authority for the purpose of formulating general policies and maintaining uniform and high standards and consistent practices in the field of crypto (cipher) security. It also exercises operational control of crypto production and security facilities established within CBNRC. The terms of reference do not include responsibility for the other two components of communications security, namely transmission security and physical security of classified communication equipment and material.

5. A somewhat parallel structure exists within the Department of National Defence, in that the Joint Telecommunications Committee (JTC), an advisory body of the Chiefs of Staff Committee, is charged with cognizance of telecommunications generally. This includes responsibility, within approved military cryptographic and security policies, to the Chiefs of Staff, for:

(a) cryptographic security,

(b) transmission security, and

(c) physical security of crypto equipment and material.

Attachment to Annex E

The directors of the communications branches of the three Armed Services are members of the CPC and the JTC.

6. In discussing this matter, the Cipher Policy Committee noted that the present organization involves some duplication of effort. As a result, inconsistencies in COMSEC policies, procedures and techniques have arisen. Investigation of incidents of compromise of crypto keying material, which have occurred recently and which have given cause for concern, indicates that the insecurities are attributable mainly to misinterpretation of or failure to maintain approved procedures. The Committee suggests, therefore, that full security of our national communications is dependent upon the unified control of COMSEC policies, to ensure the establishment and maintenance of uniform and high standards and consistent practices in regard to the three basic components of communications security. The Joint Telecommunications Committee has indicated agreement in principle with this proposal.

RECOMMENDATIONS

7. The Cipher Policy Committee therefore recommends that:

(a) responsibility for general policy control over communications security be transferred from the Security Panel to the Communications Security Board;

(b) the terms of reference of the Communications Security Board be amended to include the following:

(i) to maintain general policy control over all aspects of communications security (COMSEC), and

(ii) to exercise such control through the Cipher Policy Committee (CPC);

(c) the Cipher Policy Committee have responsibility, membership and terms of reference as shown in Appendix "B";

(d) the Chiefs of Staff Committee be asked to amend the terms of reference of the Joint Telecommunications Committee to indicate responsibility for the co-ordination and implementation, within the Department of National Defence, of policies and procedures approved by the Cipher Policy Committee; and

(e) under the direction of the Cipher Policy Committee, the Director, CBNRC, be designated to carry out the communications security mission and responsibilities as shown in Appendix "C".

Appendices "A", "B" and "C" attached.

Appendix "A"
to CSB/45

MEMBERSHIP AND TERMS OF REFERENCE of the CIPHER POLICY COMMITTEE

(A) Membership

Chairman: Representative of the Department of External Affairs.

Members: Director of Naval Communications,
Director of Signals, Army,
Director of Communications, RCAF,
Director, Communications Branch, NRC
Secretary of the Security Panel.

Secretary: Supplied by CBNRC.

(B) Terms of Reference

(i) To advise on questions of policy governing the security of all codes and ciphers used by all Canadian government departments and agencies;

(ii) to assess, evaluate and recommend the use of any new code and cipher aids, machines and devices proposed for Canadian use;

(iii) to obtain assurance that all Canadian government departments and agencies exercise adequate supervision in the use of codes and ciphers;

(iv) to recommend policy, and to advise on all matters pertaining to the manufacture of cipher aids, machines and devices in Canada; and

(v) to be responsible for dealing with appropriate US authorities and the Cypher Policy Board in the UK on all matters relating to codes and ciphers.

Appendix "B"
to CSB/45

RESPONSIBILITY, MEMBERSHIP AND TERMS OF REFERENCE
of the
CIPHER POLICY COMMITTEE (CPC)

The responsibility, membership and terms of reference of the Cipher Policy Committee (CPC) will be as follows:

(a) Responsibility

The Cipher Policy Committee will be responsible to the Communications Security Board for formulating, recommending and maintaining comprehensive policies in the field of communications security. Communications security (COMSEC) includes transmission security, crypto security and the physical security of classified communication equipment and material.

(b) Membership

Chairman: Representative of the Department of External Affairs

Members: Director of Naval Communications,
Director of Signals, Army
Director of Communications, RCAF,
Director, Communications Branch NRC
Secretary of the Security Panel

Secretary: Supplied by CBNRC

(c) Terms of Reference

(i) To formulate and recommend policies, procedures and plans for the security of government telecommunications;

(ii) to establish and ensure the execution of policies and procedures necessary to maintain high and uniform standards of COMSEC within all departments and agencies of Government concerned;

(iii) in order to discharge the responsibilities outlined in (ii) above, to analyze national communications for the purpose of studying COMSEC standards and practices of any department or agency in the field of COMSEC and to make recommendations, as necessary, to ensure compliance with approved policies in this field;

(iv) to recommend policy and to advise on all matters pertaining to crypto evaluation, crypto research and development, and the manufacture of crypto aids, machines, and/or devices in Canada;

(v) to assess, evaluate and recommend the use of any new code and cipher aids, machines and devices proposed for Canadian use;

(vi) to guide and keep under review the communications security mission assigned to the Director, Communications Branch of the National Research Council;

(vii) to collaborate with and assist departments and agencies in the preparation of the communications security portions of cover and deception plans; and

(viii) to be responsible for dealing with appropriate authorities of the United Kingdom, the United States and international organizations on policy matters relevant to COMSEC.

Appendix "C"
to CSB/45

COMMUNICATIONS SECURITY MISSION
OF THE
DIRECTOR
COMMUNICATIONS BRANCH, NATIONAL RESEARCH COUNCIL

1. The communications security mission and responsibilities assigned to the Director, Communications Branch, National Research Council, by the Cipher Policy Committee, are as shown below:

(a) to review and evaluate crypto principles incorporated or to be incorporated in any telecommunications equipments and systems and in any COMSEC equipments or systems used or proposed for use by the departments and agencies of the government;

(b) to review, evaluate and formulate crypto security rules, regulations and instructions applicable to the operation and use of COMSEC equipments and systems;

(c) to perform technical analyses of national communications for the purpose of determining the degree of COMSEC being provided by the crypto principles, materials and procedures utilized by the departments and agencies, as well as the effect on COMSEC of the communications procedures and practices being utilized, making arrangements through the CPC, as appropriate, to obtain the material required for such analyses;

(d) to review and evaluate COMSEC procedures used or proposed for use by any department or agency, as directed by the CPC, and to determine whether such procedures will provide and maintain transmission security, and to recommend revisions and additional rules as required;

(e) under the direction of the CPC, to assist in the preparation of the communications security portions of cover and deception plans;

(f) to co-ordinate and conduct COMSEC research and development, as directed;

(g) to produce crypto keying materials necessary to meet the requirements of departments and agencies of the government and to ensure that there are adequate production facilities to meet all approved requirements for crypto keying material;

(h) to prepare and to recommend minimum standards for the physical security of cryptomaterial;

(i) to provide technical guidance and support in COMSEC matters as required by departments and agencies of the government; and

(j) to conduct liaison on technical COMSEC matters with the communications security agencies of the United Kingdom and the United States.

Chapter 16/Annex F

CSB/82

22 September 1959

CANADIAN COMMUNICATIONS-ELECTRONIC SECURITY ORGANIZATION

The responsibility, membership and terms of reference of the Cipher Policy Committee, as organized at present, are stated in Appendix "B" to CSB/45, dated 18 May 1955. In general, the Committee is charged with responsibility to the Communications Security Board for formulating, recommending and maintaining comprehensive policies in the field of communications security, including transmission security, cryptographic security and the physical security of classified communication equipment and material. It is observed that, while the wording may be interpreted to include the security of all transmissions no specific reference is made to the security of non-communications (electronic) transmissions.

2. The widespread application of electronics to almost every phase of modern defence tactics presents a new field for which security must be provided. This aspect of transmission security is now generally referred to as Electronic Emission Security. The aim of electronic emission security can be defined as "the denial to an enemy of as much information as possible from the interception and analysis of non-communications (electronic) transmissions, while preserving to ourselves the benefits to be obtained from their use".

3. Non-communications systems, which may emit signals of potential intelligence value, can be grouped functionally under the following headings:

(a) Navigational Aids (C.W. and pulse) and survey devices;

(b) Surveillance Radars (search, ranging, tracking, and airborne bombing aids);

(c) I.F.F. (Identification Friend or Foe);

(d) Fire Control Gun Laying (surface and airborne);

(e) Missile Guidance Systems (including homing);

(f) Proximity Fuses; and

(g) Battlefield Aids.

4. The information which might be obtained from interception and analysis of non-communications transmissions falls generally under two headings:

(a) Technical details of the transmissions, thus permitting;

(i) development of electronic countermeasures (ECM),

(ii) enemy use of the transmissions for their original purpose, e.g. Navigational Aids,

(iii) development of similar equipment, and

(iv) deception;

(b) Deployment and operational use of the equipment, leading to revelation of;

(i) capability of our Defence Services,

(ii) recognition and location of our units,

(iii) order of battle information, and

(iv) our tactics and intentions.

In addition, communications circuits (voice or telegraph) associated with the control or steerage of non-communications transmissions are often prolific sources of collateral information concerning the function of such transmissions.

5. Two aspects are important in considering electronic emission security, namely:

(a) during development and production by industry, and

(b) during operational use by the Defence Services.

Under (a) the need, for purely technical reasons, to carry out functional tests during development, and on a sample basis during production, may reveal sensitive characteristics of the equipment before it is used operationally. Under (b) the problem is to carry out training in the use of the equipment and to maintain it at operational readiness during peacetime without nullifying its usefulness in time of war.

6. The problem of electronic emission security is very difficult. While it may be feasible in the not too distant future to apply cryptographic techniques to certain systems such as Identification Friend or Foe (IFF), other electronic systems, including primary radars, would appear at present to be beyond technical security treatment. In practice, therefore, complete security is impossible and a potential enemy will be able to intercept and exploit some transmissions. The amount and type of intelligence gained by an enemy will depend on the effort he expends on interception and analysis and the effort we expend on security measures. In

7. In view of these developments, it is proposed that the Cipher Policy Committee should also assume responsibility for electronic emission security. If this proposal is accepted, it follows that the composition and terms of reference of the Cipher Policy Committee, as stated in Appendix "B" to CSB/45, should be revised. The proposed new organization of the Committee is shown in detail in Appendix "A" to this paper. The changes involved are summarized as follows:

(a) the title of the Committee to be changed from "Cipher Policy Committee" to "Communications-Electronic Security Policy Committee" (CSPC);

(b) the terms of reference to be broadened to include responsibility for electronic emission security (ELSEC); and

(c) the membership to be extended to include representatives of the Defence Research Board and the Department of Defence Production.

8. If the reorganization of the "Cipher Policy Committee", as proposed above, be approved, it will be necessary to effect parallel changes in the composition and terms of reference of the Cipher Security Group. The proposed reorganization of this technical support Group is set out in Appendix "B" to this paper. The changes involved are summarized below:

(a) the title of the Group to be changed from "Cipher Security Group" to "Communications-Electronic Security Group" (CSG);

(b) the terms of reference to be broadened to include responsibility for providing technical advice on electronic emission security; and

(c) the membership to be expanded to include representatives of all departments and agencies represented on the CSPC.

9. Similarly, it is considered appropriate that the "COMSEC" mission assigned to the Director, CBNRC, in accordance with Appendix "C" to CSB/45, should be amended as proposed in Appendix "C" to this paper. While the major changes proposed involve the inclusion of responsibility for providing technical advice and support on electronic emission security matters, the opportunity has also been taken to clarify certain general responsibilities now being undertaken by the Director, CBNRC, in the field of communications security. The changes involved are summarized below:

(a) existing item (b) to be amended to include electronic, as well as communications, security equipments. This step is considered necessary in view of the likelihood of cryptographic treatment being applied to IFF and possibly other electronic systems;

(b) existing items (c), (d), (e), (f) and (i) to be amended to include electronic as well as communications security matters;

(c) new item (j), concerning cryptographic compromises and violations, to be inserted to define a responsibility now being undertaken by the Director, CBNRC, in accordance with CPC Paper No. 5, dated 4 June 1953;

(d) new item (k) to be included to provide for co-ordination of any monitoring/analysis effort which might be undertaken in the transmission security field; and

(e) item (l), formerly item (j), to be amended to include responsibility for technical liaison on electronic emission security matters as well as communications security matters.

RECOMMENDATIONS

10. The Cipher Policy Committee recommends that:

(a) the terms of reference of the Communications Security Board, as stated in CSB/56, be amended as follows:

FOR : "(c) maintain general policy control over all aspects of communications security;

(d) exercise such control through the Cipher Policy Committee",

READ: "(c) maintain general policy control over all aspects of communications-electronic security;

(d) exercise such control through the Communications-Electronic Security Policy Committee";

(b) the Cipher Policy Committee be redesignated as the Communications-Electronic Security Policy Committee (CSPC) and have responsibility, membership and terms of reference as set out in Appendix "A";

(c) the Cipher Security Group be redesignated as the Communications-Electronic Security Group (CSG) and have responsibility, membership and terms of reference as set out in Appendix "B"; and

(d) the communications-electronic security mission assigned to the Director, CBNRC, under CSB/45, be amended as proposed in Appendix "C" to this paper.

Appendices "A", "B", and "C" attached.

Appendix "A"
to CSB/82
CPC/P/25, dated
22 September 1959

RESPONSIBILITY, MEMBERSHIP AND TERMS OF REFERENCE OF THE COMMUNICATIONS-ELECTRONIC SECURITY POLICY COMMITTEE (CSPC)

The responsibility, membership and terms of reference of the Communications-Electronic Security Policy Committee (CSPC) will be as follows:

A. RESPONSIBILITY

The Communications-Electronic Security Policy Committee will be responsible to the Communications Security Board for formulating, recommending and maintaining comprehensive policies in the field of communications-electronic security. The security of communications and non-communications transmissions includes:

(a) the security of all systems, practices and procedures used in communications and non-communications (electronic) transmissions,

(b) the security of cryptographic systems, principles and procedures,

(c) the physical security of cryptographic material and equipment at all stages, and

(d) the standards of security applicable to personnel engaged on the development, production or use of cryptographic equipment or material.

B. MEMBERSHIP

Chairman: The Director of Communications Security, or his representative.

Appendix "A"
to CSB/82

Members:
- The Director of Naval Communications
- The Director of Signals, Army
- The Director of Communications, RCAF
- The Director, Communications Branch, NRC
- The Secretary of the Security Panel
- The Director of Communications, Department of External Affairs
- A representative of the Defence Research Board
- A representative of the Royal Canadian Mounted Police
- A representative of the Department of Defence Production
- Representatives of other departments and agencies of Government, (on a continuing or occasional basis), as required, (e.g. Joint Electronic Warfare Committee)

Secretary: Supplied by CBNRC.

C. TERMS OF REFERENCE

(a) To formulate and recommend policies, procedures and plans for the security of government communications and non-communications (electronic) transmissions;

(b) to recommend policies and procedures necessary to maintain high and uniform standards of communications-electronic security within all departments and agencies of government;

(c) in order to discharge the responsibilities outlined in (b) above, to arrange for the analysis of national communications and non-communications transmissions for the purpose of studying and assessing standards and practices of any department or agency in the field of communications-electronic

security and to make recommendations, as necessary, to ensure compliance with approved policies in this field;

(d) to recommend policy and to advise on all matters pertaining to crypto evaluation, crypto research and development, and the manufacture of crypto aids, machines and/or devices in Canada;

(e) to assess, evaluate and recommend the use of any new codes and cipher aids, machines and devices proposed for Canadian use;

(f) to guide and keep under review the communications-electronic security mission assigned to the Director, Communications Branch of the National Research Council;

(g) to collaborate with and assist departments and agencies in the preparation of the communications-electronic security portions of cover and deception plans; and

(h) to be responsible for dealing with appropriate authorities of the United Kingdom, the United States, and international organizations on policy matters relevant to communications-electronic security.

Appendix "B" to
CSB/82
CPC/P/25, dated
22 September 1959

RESPONSIBILITY, MEMBERSHIP AND TERMS OF REFERENCE OF THE COMMUNICATIONS-ELECTRONIC SECURITY GROUP (CSG)

The responsibility, membership and terms of reference of the Communications-Electronic Security Group (CSG) will be as follows:

A. RESPONSIBILITY

The Communications-Electronic Security Group will be responsible to the Communications-Electronic Security Policy Committee for providing technical advice and assistance, as required, on communications-electronic security matters, including the security of communications and non-communications (electronic) transmissions, the security of cryptographic systems and procedures and the physical security of cryptographic equipment and materials, and for implementing procedures, practices, and techniques in the communications-electronic security field as approved or otherwise authorized by the Communications-Electronic Security Policy Committee.

B. MEMBERSHIP

Chairman: Secretary of the Communications-Electronic Security Policy Committee

Members: A representative of each Service, Department and Agency represented on the Communications-Electronic Security Policy Committee. Any member may be accompanied by technical advisors.

Representatives of other Government Departments or Agencies as authorized by the Communications-Electronic Security Policy Committee.

Secretary: Supplied by CBNRC.

C. TERMS OF REFERENCE

(a) Under the direction of the Communications-Electronic Security Policy Committee, to examine and keep under review all aspects of communications-electronic security, including the production, processing and printing of crypto keying materials approved for Canadian use;

(b) to refer recommendations concerning communications-electronic security matters to the Communications-Electronic Security Policy Committee for consideration as required;

(c) to deal with such non-policy matters within the communications-electronic security field as may from time to time be referred to it by any member of the Group;

(d) to deal with communications-electronic security matters which may be referred to it by the Communications-Electronic Security Policy Committee; and

(e) to provide technical guidance and support, on communications-electronic security matters, to any government department or agency as required or as directed by the Communications-Electronic Security Policy Committee.

Appendix "C" to
CSB/82
CPC/P/25, dated
22 September 1959

COMMUNICATIONS-ELECTRONIC SECURITY MISSION OF THE DIRECTOR COMMUNICATIONS BRANCH, NATIONAL RESEARCH COUNCIL

The communications-electronic security mission and responsibilities assigned to The Director, Communications Branch, National Research Council, by the Communications-Electronic Security Policy Committee, are as shown below:

(a) to review and evaluate crypto principles incorporated or to be incorporated in any telecommunications equipments and systems and in any COMSEC equipments or systems used or proposed for use by the departments and agencies of the government;

(b) to review, evaluate and formulate crypto security rules, regulations and instructions applicable to the operation and use of communications-electronic security equipments and systems;

(c) to perform technical analyses of national communications and non-communications transmissions for the purpose of determining the degree of security being provided by the crypto principles, materials and procedures utilized by the departments and agencies, as well as the effect on communications-electronic security of the procedures and practices being employed, making arrangements through the Communications-Electronic Security Policy Committee, as appropriate, to obtain the material required for such analyses;

(d) to review and evaluate communications-electronic security procedures used or proposed for use by any department or agency, as directed by the Communications-Electronic Security Policy Committee, and to determine whether such procedures will provide and maintain transmission security, and to recommend revisions and additional rules, as required;

(e) under the direction of the Communications-Electronic Security Policy Committee, to assist in the preparation of the communications-electronic security portions of cover and deception plans;

(f) to co-ordinate and conduct communications-electronic security research and development, as directed;

(g) to produce crypto keying materials necessary to meet the requirements of departments and agencies of the government and to ensure that there are adequate production facilities to meet all approved requirements for crypto keying material;

(h) to prepare and to recommend minimum standards for the physical security of cryptomaterial;

(i) to provide technical guidance and support in communications-electronic security matters as required by departments and agencies of the government;

(j) to evaluate crypto compromises and violations in regard to national crypto keying material;

(k) to prepare programmes for and place requirements on any available Canadian monitoring/analysis facilities; and

(l) to conduct liaison on technical communications-electronic security matters with the communications-electronic security agencies of the United Kingdom and the United States.

Chapter 16/Annex G

October 1974

A STATEMENT OF DOC AND CBNRC MANDATES AND RESPONSIBILITIES IN THE COMSEC AREA

The mandate of CBNRC in the COMSEC area is outlined in the objectives and description of the COMSEC program as approved by Treasury Board in February 1974. A copy is attached.

In accordance with its objective of planning, developing, evaluating and promoting cost-effective COMSEC throughout the Federal Government, the national COMSEC agency, CBNRC, under the policy guidance of the interdepartmental committee structure, has responsibility for:

(1) meeting the requirements of the Federal Government for cryptographic keying materials, COMSEC devices, and documentation;

(2) the preparation and dissemination of COMSEC doctrine, including;

(i) establishment of criteria and guidelines for the installation and use of COMSEC systems by federal government departments;

(ii) the provision of advice to federal government departments on the planning, acquisition, installation, and use of cryptographic equipment and secure communications electronic systems.

Notwithstanding the mandate of the national COMSEC agency as outlined above, the Department of Communications, as part of its approved objective to "foster, develop, and extend telecommunications services to obtain optimum benefits for Canada in the short and long term" has a responsibility to participate in the formulation of federal government COMSEC policy, (Sub-paragraph 2, above). This responsibility is discharged through active membership in the interdepartmental committee structure which provides policy formulation and guidance, and through close working relationship with CBNRC.

In addition, insofar as the Security Advisory Committee agreed at its meeting on September 26, 1972 that the COMSEC interests of those federal departments not represented on the Communications Electronic Security Committee could most appropriately be handled by the Department of Communications, DOC has a responsibility for the preparation and distribution of COMSEC information and advice, and the dissemination of COMSEC doctrine and criteria to those departments (sub-paragraph 2(i) and 2(ii)), in consultation with CBNRC.

In April 1974, Treasury Board approved the allocation of resources to the Security and Communications Support Services Branch of the Department of Communications to permit it to carry out, among other activities, the responsibilities assigned by the Security Advisory Committee. (TB 726153). Treasury Board approval of these resources implies approval of a DOC mandate in the COMSEC area which must be carried out in consultation with CBNRC, and under the policy guidance of SAC, in a manner which should not result in overlaps or conflicts with the CBNRC mandate.

Att.

Attachment to Annex 16G
CBNRC Mandate

Communications Security Program

Objective:

To plan, develop, evaluate and promote cost-effective communications-electronic security (COMSEC) throughout the Federal Government.

Sub-Objectives:

(a) To meet the requirements of the Federal Government for cryptographic keying material and COMSEC devices and documentation efficiently and effectively.

(b) to ensure that planning, acquisition, installation and procedures for use of secure communications-electronic systems in the Federal Government are effective and provide maximum possible security at an acceptable cost.

Program:

The provision of COMSEC material, advice and services to meet the needs of the Federal Government.

Activities:

(a) Planning and Research -
The provision of advice to Federal Government departments on the planning, acquisition, installation and use of cryptographic equipment and secure communications-electronic systems; research, evaluation and analysis of COMSEC techniques, equipment and systems in support of the COMSEC program.

(b) Operations -
The establishment of criteria and guidelines, and the provision of monitoring capability and inspection services in the field of emission security; the production of cryptographic keying material and COMSEC devices and documentation as necessary to meet the needs of the Federal Government.

(c) Administration -
The management and administration of the COMSEC program.

Terms used in the above submission are defined below and are simplified versions of those definitions agreed between Collaborating Agencies.

Communications-Electronic Security

The term communications-electronic security, commonly referred to as COMSEC, is defined as the protection resulting from the application of all measures taken to prevent unauthorized interception and/or exploitation of communications and non-communication electromagnetic emissions. (COMSEC includes crypto-security, transmission security and emission security and the physical security of COMSEC information.)

Cryptographic Keying Material

Material used directly in the encryption and decryption process, i.e. material used alone or in conjunction with crypto-equipment to convert plain text into unintelligible form or to reconvert the latter into plain text.

Emission Security

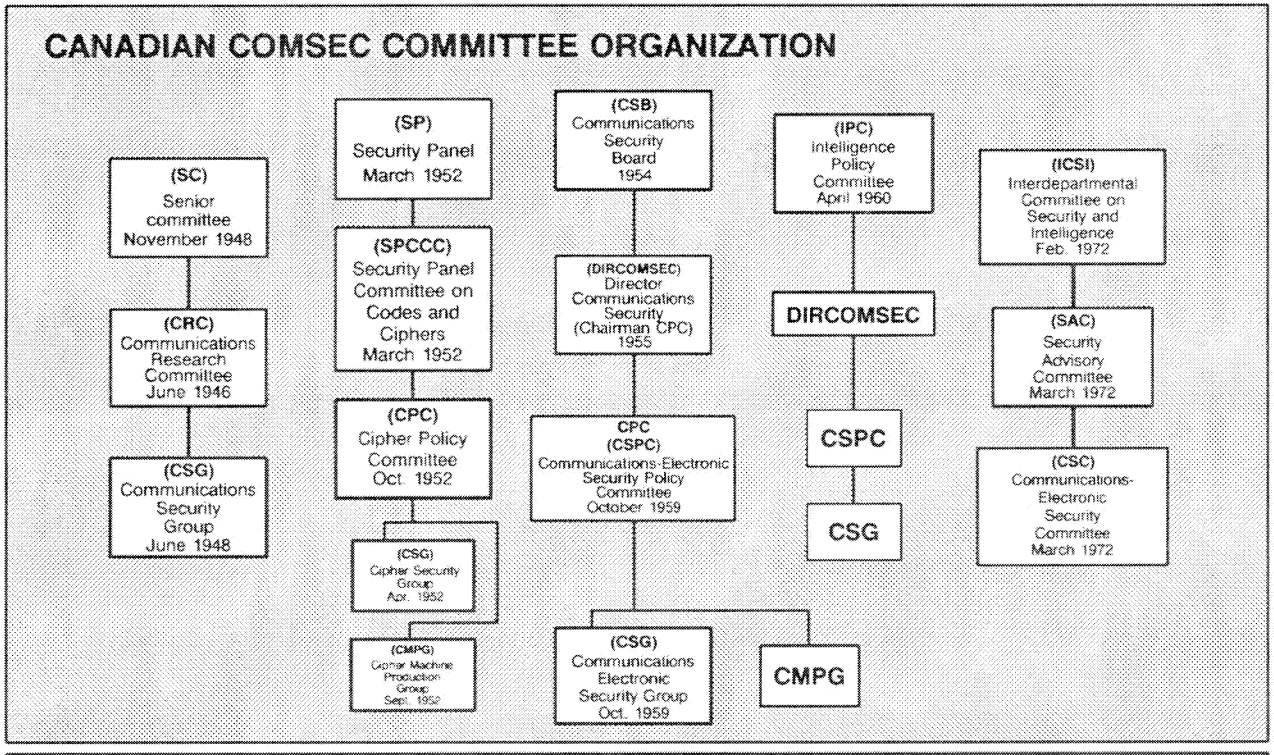
That component of COMSEC which results from measures taken to deny unauthorized persons information of value which might be obtained from intercept and

analysis of compromising emanations from equipments and systems involved in the processing of classified information.

Collaborating Agencies

The COMSEC agencies of the United States, United Kingdom, Australia and New Zealand with which Canada has agreements or arrangements for collaboration and exchange of COMSEC information.

CANADIAN COMSEC COMMITTEE ORGANIZATION



1948-1975

Chapter 17

Development of COMSEC in CBNRC

Chapter 17 (Cont'd)

Chapter 17(Cont'd)

Chapter 17 - Development of COMSEC in CBNRC

The Problem

17.1 The establishment of a communications security (COMSEC) organization in Canada grew out of a need to protect sensitive information transmitted by various agencies of the government, especially by the Department of External Affairs, the National Defence Services and the RCMP. Unlike in the case of SIGINT, there existed no established agencies whose mission was to study the vulnerabilities of classified information during transmission, let alone to provide the means of protecting such communications. COMSEC is the total of all measures used to protect communications from exploitation by unauthorized persons. In practice complete security is impossible - a potential enemy will be able to intercept and exploit some transmissions. The amount and type of intelligence gained by an enemy, therefore, will depend on the effort he expends on interception and analysis and the effort we expend on security measures to thwart his endeavours. It is realized, of course, that security protection is expensive. As a consequence, the need for taking precautions has always had to be substantiated before funds would be forthcoming for COMSEC measures.

17.2 Security is a departmental responsibility in the Canadian Government, and each Deputy Minister must compare the need for security against other requirements; he/she must be thoroughly convinced of the vulnerability of classified information and of the existence of a threat in the prevailing conditions. After World War II many defences were let down in the belief that the threat had been

eliminated; the Gouzenko affair should have made it obvious that this was not so.

17.3 Even in the UK, however, long lists were prepared of "subjects which no longer needed to be treated as secret for telegraphic transmission purposes". This caused the British Cypher Security Committee to declare at its 106th meeting on 6 June 1945 "that cypher must be used if the interests of the United Kingdom or any associated Government are likely to be prejudiced by disclosure, through interception of code or plain language (P/L), to a foreign or unauthorized Government". At a special meeting a week later the Committee observed "until recently the bulk of Departments' traffic was passed in cypher, whereas now it was likely that the proportion of P/L would rapidly be increased until it was equal to or had exceeded that of cypher ... principal risk to be guarded against was that of a reference to a cypher message which would link the two in such a way as to give a clue to the contents of the cypher message".

The Canadian Solution

17.4 Prior to 1947 the cryptographic keying material requirements of the Department of External Affairs and the Canadian Military services were supplied by the United Kingdom without cost to Canada[1]. This arrangement did not guarantee the privacy of Canadian government classified communications. A distinctly Canadian code or cipher was frequently suggested, but there were no experts in this field in Canada and wartime conditions were not suitable for training such experts. During a Commonwealth Signals Intelligence Conference convened in London in February, 1946[2],

At that time, however, there existed no Canadian Government

1. See para. 15.7
2. See para. 11.16

organization under whose aegis such a function could be placed.

17.5 But then, as related in paragraph 1.1, a proposal for a "Communications Research Centre", as it is called in the P.C. reproduced in Annex 1.A, was made in the form of a submission to Council over the signature of the Ministers of National Defence, External Affairs and Trade and Commerce (for NRC), and was approved by the Prime Minister in April 1946. Order-in-Council P.C. 54/3535, dated 21 August 1946, and Treasury Board Minute No. T307012B, dated 22 August 1946, authorized the establishment of the new Communications Research Centre, with 179 positions, of which thirty[3] were set aside for "cypher making". A description of the proposed "Communications Research Centre", dated 29 March 1946, had included among its functions "code and cypher making, and cypher security". It had also stated "the authority for the Centre should be an Order-in-Council, approving of a Centre for the purpose of producing codes and cyphers and related material, to be used by all Canadian code and cypher-using departments, including regulations for controlling the use of such cyphers".

Policy Control

17.6 As late as the end of October 1946 no final decision had been made as to what Canadian Government authority would be responsible for cipher security policy. Then, at the 12th Meeting of the Communications Research Committee (CRC)[4], held on 5 December 1946, it was agreed that the CRC should control Cipher Security Policy for the Services and the Department of External Affairs[5], and that CBNRC "should be in a position to give advice re equipment, tapes, maintenance, etc. of all cipher machines used by these Departments".

3. See Annex 3.N
4. See para. 2.4
5. See para. 16.3

The COMSEC Organization

17.7 Basically, the objective of all COMSEC work is to ensure the establishment and maintenance of adequate standards of communications security within all departments and agencies of government. It is considered most important to be able to provide cryptographic materials, as well as advice on dangers to the security of communications transmissions, on a national basis, rather than to rely on material and advice from abroad. For these reasons, a cipher materials production component was created in CBNRC on the recommendation of the CRC with the mandate to produce cipher books and keying material for use with machines of United Kingdom or United States origin. For the next 18 months it was referred to as the "Make Section". In this way there was established a national COMSEC organization under the Director CBNRC.

17.8 Early in 1947, CB hired four people to form the nucleus of the COMSEC organization: E. (Ed) de Grey, an electronics engineer from the NRC atomic energy plant at Chalk River, S/L W.J. (Bill) Trowbridge, a graduate of Dalhousie University and an experienced code-and-cipher staff officer with the RCAF; and G.S. (Gord) Thomson and D.A. (Doug) Rodgers, both wartime members of British Security Coordination, employed in the crypto equipment Research and Development (R&D) laboratory. To provide these neophytes with the knowledge necessary to produce codes and ciphers, arrangements were made for them to visit Government Communications Headquarters (GCHQ), Eastcote, England, to study background, theory and techniques for several months. The cooperation and assistance of GCHQ staff contributed greatly to the early development of COMSEC in CB. T. (Tim) Burton-Miller, Chairman of the Cipher Policy Board (CPB), M. (Monty) Davenport, Captain Wilson and Brigadier J. (Jim) Straight provided support for several years. Two Canadians who also assisted greatly in the initial stages were Sir William Stephenson, Director of British Security Coordination in Rockefeller Center, New York City,

and his engineering and development officer, Colonel B. de F. Bayly, formerly a professor of electrical engineering at the University of Toronto.

17.9 As might be expected, the formation of an organization to establish minimum security standards and exercise a measure of control over communications activities of government agencies, even when such control would result merely from the provision of advice to enhance security, led to conflict with other government agencies over responsibility and jurisdiction. As mentioned above, security is a departmental responsibility and always entails considerable expense. When large scale expenditures are dictated by advice from an external source, complaints of unwarranted interference sometimes arise. Most often the conflict is due to different interpretations of stated COMSEC objectives.

17.10 On 5 February 1947, CRC/28 outlined what was probably the "cover story" for CBNRC in which the objectives of COMSEC were stated:

> "The Communications Branch was created in July [sic] 1946 to deal with the very heavily increased commitments which Canada faced both during and after the war (World War II) in the field of communications. New techniques of communication are examined and tested for security, speed and efficiency with a view to keeping Canada completely up-to-date in every aspect of world communications."

A more accurate alternative was then suggested, pointing out "It will be realized that most of the Government and Service authorities in Canada have security means whereby they could exchange confidential messages internally or with external authorities. To preserve the security aspect of such communications some form of ciphering or encoding devices are used. It is the duty of this Branch to analyse such devices from a security point of view and recommend improvements where need be to ensure that the devices are safe to use ...."

COMSEC Responsibilities

17.11 Even the governing bodies had difficulty defining accurately the boundaries of COMSEC responsibilities. In the formative years, as the Communications-Electronic Security Group (CSG)[6] tackled various problems, the CRC felt that the junior body ventured into areas that were "ultra vires". CSG Paper No. 2, for instance, was entitled "Physical Security of Cipher Material". The CRC objected that physical security was not the responsibility of the CSG. Eventually, however, it came to be recognized that cipher material required special handling, and that certain aspects of its physical security had to be dealt with by specialists in those areas. Indeed, Government departments relied very heavily on the CSG and CBNRC, as the years unfolded, for advice and assistance on physical security protection for cipher material in operational environments - e.g. External Affairs in missions abroad, and DND in tactical situations. CB's Make Section in October 1947 assumed responsibility for accounting for all COMSEC publications, materials and equipment, a task previously handled by the Cipher Office. The following month, the Cipher staff moved into the Teletype Office and the vacated room was taken over by the Make Section as a workshop. The shortage of space was becoming acute, especially since supplies of cipher materials were beginning to accumulate. UK-produced one-time key tapes were sent to the CB Make Section for distribution to Canadian users, as well as to ASA[7] and SLO[8] Washington.

17.12 Towards the end of his training period in England, Bill Trowbridge was unfortunately taken ill. After being flown back to Canada, he was hospitalized until early in December 1947. The others, returning to Canada, set about the task of organizing what was to become the "COMSEC side" of

6. See para. 16.3
7. US Army Security Agency
8. GCHQ Senior Liaison Officer

CBNRC. Ed de Grey resigned in May 1948 to return to Chalk River. The first order of business was the recruiting of staff, a difficult assignment when one considers that the tasks ahead had never before been performed in Canada. Of the 39 positions now assigned to COMSEC, eleven had been filled by August 1948. The total had climbed to 21 by July 1949 and to 23 by December of that year; about half of the latter figure were technical, the remainder administrative and operating personnel. The technical strength received a considerable boost in January 1948 with the arrival of F.L. (Ferdy) Laporte, an ex-army radar technician, and again a month later with A.V. (Al) Joyce, a former British Army communications technician.

17.13 At its 26th Meeting on 5 March 1948 the CRC agreed that the Make Section of CBNRC should be known in future as the "Test and Design Section" (T&D). The Committee also approved the original terms of reference and the scope of duties and responsibilities of T&D which were published in CRC/73 of 5 June 1948 and are listed in Annex A. By July 1948 T&D had taken over full responsibility for maintenance of the teletype and cipher equipment in the CBNRC Comcentre. New teletype equipment purchased by the Branch had arrived to replace that on loan from the Army, but setting it up had to be delayed till October because of the lack of space for testing and installation.

17.14 Although scarcely prepared for the responsibility, T&D was called upon even as early as 1947 and 1948 to evaluate many codes and cipher systems proposed by individuals and submitted to the Government. With assistance from SIGINT cryptanalysts assessments were made. The proposals varied from childish to ridiculously unwieldy, but any that had practical applications were found to offer little security. One of the better ideas was a non-synchronous on-line cipher device proposed in March 1951. It had been developed by an American civilian and an application had been filed with the Canadian Patent Office. A detailed technical report was drawn

up for the Directorate of Naval Communications. Evaluation of inventions is discussed in more detail in Chapter 21.

17.15 With the overall mission of providing support in the security protection of classified government communications, the new organization would have to develop a COMSEC doctrine to provide advice and technical assistance, and would have a second responsibility of furnishing the means whereby such advice could be followed. Some members of the staff would have to acquire expertise in protection techniques, while others would have to begin producing keying materials and other COMSEC aids to be used in concealing classified information.

17.16 As several departments had ordered ROCKEX cipher equipment, Gord Thomson and Doug Rodgers, who had participated in the development of ROCKEX, were called upon to provide working-level advice and assistance, including training. They literally set up the system for the Department of External Affairs, conditioning and installing the equipment, and training technical and operating personnel. Bob Murray, an assistant to John Manson in C Group, was seconded to External to serve as Acting Communications Officer until a suitable replacement could be hired (he was succeeded by Joe Bélanger following the latter's discharge from the RCN). Until the military established ROCKEX training facilities some time later, T&D also provided them with advice and assistance. COMSEC Advice and Support will be covered in Chapter 18, and COMSEC training is treated in Chapter 28.

Radiation

17.17 At about this time, CBNRC, as well as our UK and US counterparts, began to evince a growing interest in compromising emanations detected in the vicinity of communications and cipher equipment. The subject, originally called Radiation, is discussed briefly later in this Chapter and covered in detail in Chapter 24, under the title "TEMPEST", incorporating the measures that can be taken to

eliminate or at least minimize the risk of such emanations being exploited for intelligence purposes. This became a heavy responsibility for T&D, not only on behalf of CB, but also of all government agencies that processed classified information. The T&D technicians began in 1948 and 1949 to install protective measures on CBNRC's crypto and communications equipment to prevent intelligence-bearing emanations from radiating out to distances where they could be detected and exploited by unauthorized persons. ROCKEX equipment parts and leads were grounded and shielded, and special enclosures were constructed to suppress these radiations. Soon CB was also providing advice and assistance to other departments.

Beginnings of Production

17.18 As operating staff came on board, a crypto key production capability was established. First efforts were devoted to producing one-time pads (OTP). Bill Trowbridge had concentrated on methods for producing printed keying material. Although he was in hospital, some production of this material was undertaken, and first deliveries to users were made in January 1948. Settings for TYPEX inserts and plugboards, produced by hand methods, were delivered to External Affairs two months later. (Production of Keying Material is the subject of Chapter 19.) By January 1949 Canadian-made COMSEC materials were coming into more general use in External Affairs and National Defence communications. CB had set up key generating equipment and was supplying ROCKEX key tape for External's communications between Ottawa and its missions in London, Washington, New York and Paris, and between London and Paris. In addition, CBNRC's SIGINT communications with Coverdale, Whitehorse, ASA and SLO required a million groups of ROCKEX key tape per month. Canada's diplomatic and other classified communications were now being secured for the first time with an automatic electronic encryption process operating at telegraph speeds, in a way which ensured that only authorized Canadians had access to the information. Canada had grown up a little.

17.19 In addition to producing paper keying material - OTPs, cipher machine settings and reciphering tables - the T&D Reprographics subsection did reproduction on duplicating equipment for the whole of CBNRC; a typical month's production was 200 photostat sheets, 9,000 sheets of Ditto and 30,000 sheets of Multilith copy.

17.20 The responsibility for coordinating COMSEC requirements for Canadian government departments and agencies gradually fell to CBNRC. At the 17th CRC Meeting on 8 May 1947, and later that year on 6 November at the 23rd Meeting, the Director CB requested the Service Departments and External Affairs to submit an "approximate estimate of their requirements for key tape, one-time pads, basic code books, etc. ... partially for supply of their needs ... and partially as guidance in the development of the Make Section". The Chairman CRC noted that UK authorities had suggested that CB should become the distributing authority for all cipher material used by Service and Civilian Departments. Nevertheless, as late as 4 February 1949 there was still some doubt as to where responsibility lay for the coordination of requirements[9]. The CRC Chairman, Bill Crean, observed that coordination of requirements for new editions of TYPEX inserts "did not strictly fall within the terms of reference of the CSG", but "the CR Committee would instruct the CSG to coordinate all the requirements, both for supply from the UK and for eventual local production". The RCAF order for TYPEX inserts in March 1949 was placed through CBNRC, but External Affairs the following month requisitioned inserts in a letter to the Commonwealth Relations Office, with a copy to CBNRC. Orders for UK-manufactured inserts were placed by CB for the Canadian Army and the RCAF in 1950 and 1951. Thereafter CBNRC was the supplier of all crypto keying materials.

17.21 The pressure continued on CBNRC to expand production of keying materials. The original proposal

9. 36th Meeting of CRC

by UK authorities was that Canada, Australia and New Zealand should set up production centres to satisfy their own internal cipher requirements, and so relieve the UK organization of some of the responsibility and costs of production.

Space Constraints

17.22 During the early period, while the Section was cutting its teeth, the most serious problem was the shortage of space. Bill Trowbridge shared an office 8 feet by 14 feet with four ladies making

s.15(1) - DEF

s.15(1) - IA

keying material. Another little room which had formerly housed a few cipher machines was scarcely able to meet the needs of a workshop, let alone provide space for keying material production equipment. Operations soon spread into office areas. Even the Director's office was not sacrosanct: when Mr. Drake was absent in September and October 1948, space was required for a fourth key tape generating station; it was set up in his office and production increased by 25 percent. By June 1949 arrangements were made to use a portion of the second floor of the Lasalle Academy, and the tape generators and workshops were moved there. Four other generating stations, which had been stored in the Justice Building for the previous nine months, were retrieved and were set up and adjusted in preparation for operation after the expected move to new quarters in the Rideau Annex took place.

17.23 As mentioned above, the first COMSEC aids produced were those that could be fabricated by hand methods. These involved labour-intensive processes, building up random data and assembling code and cipher hand systems and cipher machine settings. There was a great need to develop automated methods. This was thwarted by the shortage of space. Development of a random alphabet card file (for the production of manuscript, key lists, settings, one-time pads, authentication systems, etc.) had to be deferred until the move to larger quarters, because there was insufficient space in the IBM machine room.

Construction of Automated Production Equipment

17.24 Between mid-1948 and December 1950 T&D was faced with the enormous task of providing equipment to produce keying material.

it was necessary for T&D to build many intricate devices on its own. Fortunately CB was able to obtain advice from GCHQ and to benefit from the latter's experience, and in many cases T&D

would build an electronic device where GCHQ had used mechanical equipment[10]. In any event, T&D designed, developed and constructed, by the end of the year 1950, several items required in the production of ciphers, as reported by the section:

"(i) Electronic scrambler for IBM sorter (recognized by UK authorities as being superior to their mechanical scrambler);

(ii) Relay operated Tape Checkers (superior to UK checker as it counts the actual characters on the tape and, in addition, the Delta count); nine of these units constructed here and instruction manuals prepared;

(iii) Tape Winders (UK Authorities have taken drawings etc. as considered much superior to their winder);

(iv) Electronic Discriminators to scrutinize and check faults in tape - considered to be practically foolproof by Group Head;

(v) Electronic unit to control page production from tape;

(vi) Numerous types of "test" equipment to facilitate fault finding on various equipments in use;

(vii) Prototype electronic distributor for ROCKEX machines (now being tested);

(viii) Plans for early construction of electronic production equipment;

(ix) Multiple tape checkers."

17.25 Construction to meet special needs became an essential function of T&D - whether it was an

10. See para. 19.27 and following

electromechanical device for production purposes, a specialized tool or a wooden or metal enclosure. An expressly designed "tape humidor" was built, with a capacity of 180 rolls of tape, to control the amount of humidity present in the tape just prior to punching; this requirement arose because of perforating difficulties encountered. Staff members quickly gained expertise in judging tape quality, and soon were advising tape manufacturers regarding paper content and other tape specifications essential to CB's unusual application (multi-tape punching).

17.26 One of the main tasks at this time was the construction of tape checking equipment (devices to verify the randomness of key) and comparison checkers to handle 3-way to 6-way ROCKEX tape. The T&D technicians were very innovative. They designed and built a device to enable ROCKEX-generated key tape to be used in the production of TYPEX message settings. When space limitations inhibited some normal technical operations (such as setting up and testing equipment), they would turn their hands to other occupations in preparation for the move of the Branch to the Rideau Annex. They built a new "patch-panel" for distribution of teletype circuits at the Annex. They made wooden boxes for shipping key tape and even engaged in carpentry work and other installation duties at Rideau Annex in the weeks prior to the move. During this period, the technicians were also responsible for the maintenance and repair of communications and cipher equipment. This responsibility, moreover, involved the modification of teletype and crypto equipment for TEMPEST protection. Monthly technical meetings were held to coordinate operations.

17.27 Key tape production equipment was set up and put into operation in the Rideau Annex in November and December 1949. T&D technicians also installed the cipher and communications equipment in the Com-centre's new quarters during the latter half of December, as the other parts of CBNRC prepared for the move in early January 1950. New teletype equipment had to be set up for two new circuits (to Edmonton and Leitrim).

Expansion in Rideau Annex

17.28 On arrival at the Rideau Annex, Sections in CB became Groups and Subsections became Sections. Bill Trowbridge was now Group Head; G.A. (Art) Browness joined the staff to become Deputy Group Head. T&D also came to be known as T Group. The organization of the Group in 1950 is shown at Annex B. With adequate space in the new quarters, T&D was now able to direct its efforts to meeting the full Canadian requirement for COMSEC materials. This emphasized the need for additional staff. The Cipher Production Section asked for more personnel for the production of key lists, authentication tables, etc. Setting up new key tape generators created a requirement for more operators and more technicians for servicing and repair. Overtime was instituted for tape operators. By October 1951, with the T&D establishment set at 78 persons, 54 were engaged full time on cipher production. Approximately 60 to 65 percent of Canadian Government cipher requirements were now being met. The CB Communications Office, which had relied on T&D Group for technical planning, installation and maintenance since mid-1947, was greatly expanded and fitted out with more ROCKEX equipment and the new 5UCO on-line crypto and teleprinter ancillaries; this increased the need for technical staff. The 5UCO equipment was set up in July 1950, and the training of technicians to maintain it tied up several staff members. Unlike off-line equipment, the 5UCO crypto was operated by T&D technicians, while the operator was concerned only with the teletype ancillaries. A GCHQ expert came to CB in August, and testing of the system over RCAF-RAF single sideband (SSB) radio commenced.

17.29 Other demands were made on the staff. Unable to obtain parts and equipment from IBM and Teletype Corporation, T&D technicians had to design and make special tools and construct devices such as card sorters, comparison checkers for scanning multi-way tape, and a machine for the automatic production of one-time pads. Two T&D technicians were trained at the local IBM Centre to overhaul Electromatic typewriters. In addition, the Group was embarking on

a new program, the production of TYPEX inserts. The technicians were also engaged in the testing of various new crypto devices, notably the 5UCO and the ASAM-2. A study was made of a non-synchronous on-line cipher machine.

TYPEX Inserts - Machine Shop

17.30 The Senior Committee had now given its approval for the production of inserts, and recruiting for the Insert Machine Shop could get under way. By December 1950 Mr. Drake was able to promise the 64th Meeting of the CRC that delay in the production of inserts would not result from lack of personnel, but might be caused by the time required to obtain and install equipment which had to be imported from England. He realized that the shortage of inserts might become acute in the ensuing months, but pointed out that acquisition of equipment had had to await approval of the program. A contract was let in March 1951 for the renovation of an area in the basement to house a TYPEX Insert Machine Shop. Noah Gauthier was despatched to the UK to study production methods for TYPEX inserts. Three lathes, two drill presses, a bench grinder, a shaper, and other machine shop tools were purchased for the insert production shop, which in time took on various responsibilities and was expanded into a precision model shop. Special parts required by other sections of CBNRC and classified areas of other Government agencies were machined in the workshop. Insert production was initiated in August 1951. More detail on production is contained in Chapter 19.

17.31 Recruiting of technical personnel continued - 86 were interviewed in June alone, and a dozen were hired as quickly as security clearance could be arranged. T Group organization in 1952 is given at Annex C. As the Branch grew, plans were soon under way to extend operations to the fourth floor of the Rideau Annex, and this involved T&D staff in various special projects. They planned the power and lighting requirements for the elements to be moved to the top floor, including the Comcentre, and designed and constructed for the latter a panel to safeguard

against plain language being transmitted to line. T&D moved the Comcentre equipment on a weekend in February 1952 without a break in communications.

Requirements for Keying Material

17.32

17.33 T Group Head, in a memorandum to the Director on 1 June 1951, said that in view of the small production staff (41 persons) and limited facilities, it would be difficult at that time to commit T&D to a firm undertaking. He suggested delaying any decision, "except to agree in principle until work is actually commenced" on manuscripts for Canadian material, since CB "would then be in a better position to estimate the scope of any additional commitments"[11].

11. See also para. 17.62

17.34 The efficiency with which CBNRC produced ROCKEX cipher tapes inspired the Members of the CRC (at their 75th Meeting on 2 August 1951) to consider the possibility of selling key tape as a "revenue producer" for CBNRC. It was thought, however, that the allotment and transfer of funds for this purpose would elicit enquiries as to the nature of the operation and would create a security problem. Nevertheless, finances continued to occupy the attention of the CRC, and Mr. Drake told the 77th Meeting on 5 October 1951 that of CBNRC's overall Estimates of $1,487,068 for 1952-53 approximately 30 percent was indented for cipher production, and that some $100,000 would be expended on paper stock alone, with $10,000 requested for the construction of a storage building. He explained, too, that the Estimates had included a revenue item of $40,000 to be derived from TYPEX inserts "on a repayment basis". The Chairman expressed the opinion that the question of repayment for cipher production by users should be reviewed, and that as long as the President NRC did not object to the existing financial arrangements there was no need to ask for repayment of cipher production services. Mr. Drake agreed providing that the Treasury Board raised no objection. There is no record of any Canadian Government agency ever compensating CBNRC for cipher production despite the following entry in the Minutes of the 13th Meeting of the Senior Committee, held on 12 February 1953:

> Para 2 a) "After examining CRC/177 the Committee agreed with recommendations of the C.R.C., namely, that each Service and Department obtaining cipher materials from Communications Branch should pay for this material on the basis of financial encumbrances. It was noted that these arrangements would go into effect for the financial year 1954-55."

17.35 The main obstacle to initiating the production of keying material in Canada for Combined or NATO use was the lack of facilities, mainly printing facilities, for such large-scale projects.

Canada was eager to share part of the load with its Allies, and had given favourable consideration to the proposal when it was first made by the UK in 1949. The CR Committee had agreed (at its 42nd Meeting on 15 August 1949) "that it might be useful experience for Canada to undertake some further cipher production task, as long as the cost was not prohibitive". Only the King's Printer had facilities capable of handling printing projects of the order of magnitude involved. At the 46th CRC Meeting on 24 November 1949 the Members had noted that under the Printing Act the King's Printer had sole authority for all Government printing, but could not meet the necessary security requirements until his new plant was ready, which might not be for five years. Security printing for the RCN had to be done by the Canadian Bank Note Company. (In Britain in 1947, the majority of COMSEC items, such as Basic Books, Call Sign Books, and SS Frame Tables were printed by commercial firms from manuscript produced at GCHQ. During World War II, Canadian firms had undertaken printing projects for the British Government.)

Security Printing

17.36 Discussions were held with the King's Printer, and by January 1950 it was learned that a Security Printing unit could be set up within six months in temporary quarters leased by the Printing Bureau on Nicholas Street. The CRC agreed to the undertaking, stressing the physical security problems involved. Five months later, however, little progress had been made. Mr. Drake wrote to Mr. Glazebrook on 6 June that the "Senior Committee has now approved ... setting up ... specialized security printing plant by the King's Printer to take care of the Canadian cipher requirements". Nevertheless, even by 7 September 1950, at the 60th CRC Meeting, "The Chairman reported that the Secretary of the Security Panel and the King's Printer were endeavouring to find a building which would conform to the security requirements of the CRC". At the previous meeting, a suggestion had been made (by the Directorate of Military Intelligence (DMI) representative) that the large-scale security

printing plant be set up in CBNRC, but this solution was considered "undesirable". As the search continued for quarters for a secure printing establishment, the Chairman CRC wrote on 13 September 1950 to the President of NRC, seeking his approval for an increase in the establishment of CBNRC by ten positions for the production of manuscript in the Test and Design Group. Pointing out that the Senior Committee had recently approved a plan for the printing of Canadian cipher material in a special security printing plant to be operated by the King's Printer, he said that in order to provide material for printing, T&D would have to prepare and check approximately thirty-five types of random manuscript - twelve editions per item - and complex basic code books constructed in large part by hand. Six weeks later (on 24 October 1950) the CRC Chairman wrote again to the NRC President requesting a further increase in CB's establishment, this time by eleven persons to enable T&D to manufacture TYPEX inserts for Canadian users on a repayment basis. He reminded the President that the Senior Committee had approved on 13 October the plan to set up a small workshop for the purpose, and said the Services regarded the project as urgent since there were no replacement or emergency reserve inserts in Canada at the time. A compromise of the inserts in use would deprive the Services of a secure means of communication.

17.37 The Security Printing Plant was eventually established in the Mortimer Building (premises owned by Mortimer Printers Limited) on Nicholas Street. The 70th CRC Meeting (5 April 1951) noted that the plant was considered secure for printing material up to the SECRET level; CBNRC used the facility for the printing of large projects, e.g. to make proforma sheets for TYPEX indicator books and manuscript of 5-letter groups produced at CB on tape; but the CRC Members expressed uneasiness about security until a comptroller should be appointed. (A controller/ comptroller was appointed on a temporary basis in October.) Later that month, the Communications Security Group (31st CSG Meeting on 23 April) "noted with some concern that certain 'published' references to the new security printing plant technically

constituted a breach of security ... the Acting Shop Superintendent apparently has advertised the new plant to certain commercial firms as a 'security printing plant' and has displayed signs to the same effect about the Mortimer Building, including the main entrance". The Members agreed that "such a procedure is prejudicial to the maintenance of sound security ... and invites attention". The Cabinet Secretariat, in a letter dated 1 May 1951, decreed that "no signs identifying this unit as a security printing plant should be posted either inside or outside the establishment" and that "employees should be cautioned not to discuss ... the functions ... other than ... on a 'need-to-know' basis. Special functions ... should not be drawn to the attention of commercial firms or individuals". The Secretary added: "I am informed that ... the plant will be identified merely as the Nicholas Street unit of the Government Printing Bureau."

17.38

12. The King's Printer became the Queen's Printer on 6 February 1952, on the death of King George VI

arrangements were being made to provide 24-hour watch shortly, and it was agreed that responsibility for production of the ACPs should be accepted. Mr. R.G. Robertson, the Clerk of the Privy Council, observed that it would be appropriate for money for this purpose to be made available from Mutual Aid Funds, and suggested in a letter to the Minister of National Defence that the sum of $40,000 be transferred to the Directorate of Publications and Printing of the Naval Service, which would then make the necessary requisition to the Queen's Printer. Order-in-Council P.C.4704, dated 30 December 1952, granted approval for Canada to share in the production of certain Combined and NATO cryptomaterial.

17.39 During the next few years, concern was expressed in the various COMSEC committees over the obviously indifferent and perfunctory attitude toward security shown by officials involved in setting up and maintaining the secure printing plant. Pressure was exerted on various authorities to join in the selection and appointment of suitable staff and guards. At the 12th CPC Meeting on 10 April 1953 Peter Dwyer of the Privy Council Office (PCO) observed that a maintenance man at the Plant, who occasionally manned the incinerator while the RCN TYPEX Message Setting Book was being printed, had been shown to be a member of the Communist Party. Because the man was involved only in disposing of waste, it had apparently not occurred to those in charge that he was handling copies of "live" keying material discarded perhaps for some printing fault or imperfection. It was not until September 1954 that correspondence between the Secretary to the Cabinet and the Queen's Printer indicated acceptance of the security measures drawn up by the CPC for the operation of the Secure Printing Unit, and that crypto manuscript held by the Director CBNRC could therefore be released for printing.

17.40 While these seemingly endless discussions were taking place to arrange for adequate printing facilities, AFSA in May 1952 sent an urgent request for assistance in the production of keying material at other than the printing stages, especially in the

preparation of manuscript. This T Group was able to do, and thenceforth material was prepared each year for several NATO codes and authentication systems.

Canadian National Distributing Authority

17.41 Possibly the bitterest debate in the history of the development of COMSEC in the Canadian Government occurred in 1953, as authorities vied for responsibility in handling and distributing NATO cryptomaterial. The NATO Standing Group had put out two memoranda, SGM 2631-52 and SGM 303-53, outlining a "Plan for the Production, Distribution, Accounting and Security Control of NATO Cryptomaterial". Each member nation was asked to establish a National Distribution Authority (NDA) "for the purpose of receiving, distributing and accounting for NATO cryptomaterial issued to that nation". The main contenders for the job in Canada were the Navy and CBNRC. (Curiously, the main proponent of the latter was not CB itself, but the Army, possibly motivated by inter-service rivalry.) The main factors to be considered in selecting an agency to assume the duties of the Canadian National Distributing Authority (CNDA) were: the volume of material involved (and, of course, which organization was the largest customer); the storage space required (5,000 square feet); accounting procedures which would have to be established; additional personnel required to handle the tasks involved; and payment for the material. Two proposals, one by the Navy that its Directorate of Publications and Printing (DPP(N)) be named CNDA, the other by the Army that CBNRC assume the role, were embodied in CSG Paper No. 6/53, which was considered at the CPC's 13th Meeting on 18 April 1953. The acrimonious nature of the discussion was, of course, not reflected in the Minutes.

17.42 The Navy, as the major user of NATO material, already had facilities for storage, distribution and accounting for such material, and consequently would need to recruit fewer additional personnel to take on the job. Also, although the Canadian Services received NATO cryptomaterial free of charge when it was produced by their opposite numbers in the UK,

certain other material, crypto and non-crypto, was procured and paid for by the RCN. These factors made a good case for the Navy proposal. However, the Army felt that a National Distribution Authority, responsible to all Canadian users of NATO cryptomaterial, "should be free from all operational defence problems" and "the Services should be required to devote their full effort to the direction and operations of crypto communications within their respective Services, without the hindrance of acting as distributing authority for all other users". The Army regarded the CB Test and Design Group as the ideal agency for CNDA because it was already involved in producing NATO cryptomaterial, worked in conjunction with NSA and GCHQ, and would likely undertake further production for NATO. The Army offered storage space at the Royal Canadian Signals Cipher Depot, Kingston, for use by CBNRC, and insisted that "The National Distribution Authority, under the sponsorship of CBNRC would be free from all Service entanglements to act as the one and only Canadian Distribution Authority (NATO) to all Canadian users". As for funding, the Army observed that current arrangements involved no charge for cryptomaterial, but if this should change, the cost could be shared on a percentage basis by the Canadian users, the funds being transferred from Service appropriations to CBNRC for application as required. The Army proposal was quite detailed. The RCAF supported the RCN's bid, and External Affairs played mugwump, agreeing to accept the majority decision.

17.43 CBNRC agreed that it could be regarded as the logical choice for CNDA, since civil as well as Service requirements were involved. At the same time, CBNRC recognized that serious problems would arise in regard to the provision of adequate space and facilities. CB also pointed out that the NATO Standing Group had authorized direct communication between the National Distribution Authorities and the Standing Group Security Evaluation Agencies and Distribution and Accounting Agencies. This direct communication channel would be used for promulgation by the Standing Group of cryptographic policy and procedures, and by all other agencies and authorities

"listed" for the exchange of information and directives concerning cryptomaterial, procedures and policies. While it was realized that the procedures and policies referred to would be concerned with NATO cryptomaterial only, the possibility existed that such policies and procedures might, on occasion, be at variance with national policy. CBNRC felt, therefore, that the CNDA selected should function, as far as policy matters were concerned, under the jurisdiction of the Cipher Policy Committee. Thus CBNRC was of two minds, believing that it should have the responsibility for cryptomaterial, but realizing at the same time that it did not possess the personnel, facilities and space to cope with the job; also, once again aware of the "requirement to maintain a low profile" - which might be difficult when dealing with nationals of other NATO countries assigned to the NATO agencies - CB hesitated to press its case too strongly.

17.44 The CPC Chairman expressed the opinion that, in view of the nature of the duties involved and the lack of space to accommodate any personnel over and above the existing CBNRC establishment, he would be reluctant to have CB accept additional responsibilities. He suggested, therefore, that the Navy proposal be accepted. No shots were fired, no blows were struck, and agreement was reached that DPP(N) would act as CNDA, and would operate under the authority of the CPC. The operation of CNDA was carried on under the same roof as the NDA for national material, but separate lockers and books were maintained. The responsibility for the direction of CNDA gradually fell to the authority who paid the bills, i.e. Naval Communications, and became part of the function of the RCN Directorate of Communications Security, working in close cooperation with T Group CBNRC.

Growing Pains

17.45 T Group's problems in recruiting personnel, and in dealing with Government agencies which were not part of the COMSEC community, were aggravated by what was called the "need to maintain a low

profile". The CRC gave consideration to the possibility of allowing CBNRC to advertise for staff with qualifications that would be useful in crypto operations. At the 97th CRC Meeting on 10 April 1953 the Chairman said he "personally was of the opinion that security regulations dealing with cipher production by CBNRC could be relaxed somewhat". The Cipher Policy Committee (CPC) and the Communications Security Group (CSG) took the opposite view. The CPC considered the subject of unclassified references to crypto duties and "agreed that, since unclassified information of this nature provided disloyal persons with an opportunity for penetration into cipher offices, such advertisements were prejudicial to security and should be prohibited". At the 14th Meeting of the Senior Committee, now called the Communications Security Board (CSB)[13], on 19 October 1953 "the question was raised as to whether recruiting was so seriously hampered by the secrecy which prevailed in connection with SIGINT work that some consideration should be given to publication in general terms of the nature of the work of the Branch. It was suggested that one possibility might be to make public the fact that the Branch was engaged in the production of ciphers. No decision was reached on this general question".

17.46 Meanwhile, the responsibilities of the Test and Design Group continued to expand. Production of book ciphers, key settings

TYPEX inserts

and ROCKEX tape was progressing apace. Preparations were under way for the generation of 5UCO tape. Along with their routine maintenance and fault-finding and correction routines, T&D staff were required to build five random signal generators, a timer and five isolators. In preparation for the move of the Comcentre to the fourth floor of the Rideau Annex, T&D built new control racks and prefabricated jack panels, connecting blocks and cable assemblies. Overtime was necessary, and five more technicians were sought, as well as a draftsman.

13. See para. 2.13

The Mechanical Design and Drafting element was established in August 1952.

17.47 Mr. Drake told the 79th Meeting of the CR Committee on 2 November 1951 that information had been received that the checkers built into the 5UCO key tape generators were not too effective, and that the UK authorities were of the opinion that it would be necessary to manufacture new high-speed electronic checkers in order to ensure that complete randomness was being obtained in the tape produced. The UK would not be in a position to supply Canada with this device until 1953 or later, and suggested that Canada build a checker for its own use. One such checker could handle 40 punches - the output of 8 generators.

17.48 The heavy workload continued throughout 1952. Transmission difficulties on the RCAF-RAF SSB circuits, coupled with record traffic levels in the Comcentre which put greater strain on the communications and cipher equipment, resulted in extra demands on maintenance staff. Fortunately the requirement for ROCKEX key tape diminished slightly for a short period, allowing operators to be shifted occasionally to the production of printed keying material, where orders were accumulating. Soon, however, the tape operating staff was faced with new commitments - the production and security sealing of 5UCO key tape. Duplicating requirements were on the increase, including microfilming, developing and printing. Insert production was expanding but could not keep up with the demand. In addition, an extensive technical stores unit was set up in T&D in July 1952, to serve the entire Branch. Items that could not be obtained commercially were made in the Group's Machine Shop. By the end of 1952, T&D staff reached a strength of 79 persons. Activities varied from the standard tasks to unusual ones such as changing some transcribing positions from Latin to Cyrillic type. For other departments, the Group held COMSEC training courses for Naval technicians, and assembled and adjusted several dozen ROCKEX machines for the RCAF. A new UK-developed cipher device (ROLLICK I) was tested in T&D laboratories and on a circuit to NSA.

17.49 At this point, by a stroke of good fortune, the UK were able to relieve some of the strain on T&D technical staff. Earlier, GCHQ had said it would be unable to manufacture a high-speed tape checker for Canada, and had suggested that T&D build one. Subsequently, the staffing situation in the UK had improved, and GCHQ were able to manufacture a checker, with technical assistance and partial payment from CBNRC.

17.50 Bill Trowbridge resigned to take a position in industry in May 1953, and was succeeded on an acting basis by Art Browness. He returned to CBNRC in September 1954, and once again took on the responsibilities of T&D Group Head[14].

17.51 After discussions with NSA representatives in August 1953, CBNRC began a month later producing

for NATO. Thereafter, production of keying material for and NATO use increased. By this time, too, the Branch was producing 5UCO key tape for Canadian Army and Navy use, and within nine months was also supplying 5UCO key tape to the UK.

17.52 As production expanded, working and storage areas seemed to shrink. The Senior Committee in October 1953 expressed concern about the circumstances in which the keying material production centre was situated - the crowded conditions, and the risk of fire and even of air attack, either of which could destroy the sole source of key; the Committee considered whether T&D should remain in the Rideau Annex or move to another location, or whether a small building should be erected nearby. No action was taken. More space was found by eliminating the need for some filing cabinets by microfilming their contents. Another microfilm camera was added. Production staff was rotated from job to job to cope with the workload as backlogs developed. Staff strength stood at 87 at the end of 1953, and recruiting continued.

14. See para. 3.9

17.53 The Comcentre invested in new Teletype equipment (upgrading from Models 14, 15 and 19 to Model 28) and added more 5UCO racks. These, of course, had to be installed and maintained by T&D. The technical staff required reinforcement.

17.54

17.55

Research and Development (R&D)

17.56 Design and development continued unabated. To prevent reuse of ROCKEX six-hole key tape (double

employment of key would provide an interceptor with a depth of two and enable him/her to exploit the encryption) the UK had developed a tape-slitter, but this mechanical device was plagued with problems. T&D designed the 7th Hole Perforator, nicknamed "TOOTHPICK", which accomplished the same purpose with a simpler modification; they provided samples to the UK and constructed sufficient copies for all Canadian users.

17.57 Two production devices were designed and developed by T Group in 1954: one, named "POKERFACE", was used to produce codes; the other, "PINEAPPLE", was developed for manuscript production. They are described in more detail in Chapter 19. In addition, a random generator was designed to work in association with PINEAPPLE. As an indication of the state-of-the-art in the commercial arena at the time, it might be noted here that T&D invested, in October 1954, in what was called an "Instant Copier"; it required 45 seconds to produce one copy.

17.58 The Communications Security Board at its 15th Meeting on 10 August 1954 considered CSB/35 "dealing with Canadian cryptographic policy and recommending the establishment in Canada ... of cipher machine production facilities, a cipher evaluation group and a cipher machine development group". The history of cipher evaluation is told in Chapter 21, and events related to the development and production of crypto equipment are recounted in Chapter 22.

CANCOMSLO/W

17.59 At the 27th Meeting of the Cipher Policy Committee on 14 January 1955 the Chairman tabled a letter from DIRNSA (Director NSA), dated 20 December 1954, which proposed that consideration be given to the establishment, in Washington, of an officer to represent Canada on COMSEC matters. The Committee agreed to the proposal. Although it had earlier been thought that an engineer would be most appropriate for the position, it was later concluded that an officer with a general cryptographic and COMSEC

background would be more suitable. The Committee unanimously approved the appointment of Art Browness as the first Canadian COMSEC Liaison Officer to Washington

Gord Thomson assumed the responsibilities of Acting Deputy Group Head as well as Technical Assistant to the Group Head.

17.60 By the beginning of 1955, the COMSEC staff had grown to 93 bodies. The Branch's 5UCO circuits were operating on a 24-hour basis, putting a severe strain on maintenance staff. T Group Organization on 1 November 1955 is shown at Annex D.

High-Speed Generating Equipment

17.61 Communications levels continued to climb and the requirement for ROCKEX tape increased to the point where the existing production system was no longer adequate. High-speed gearing was introduced and the output was increased by 20 per cent. Even this was insufficient to meet the burgeoning demand for ROCKEX key. CBNRC had to call on its creative resources to invent some high-speed generating equipment. Unfortunately, the quest for an engineer for COMSEC work had produced short-lived results; although one had been hired in May 1954, he resigned in October 1955, after having been sent to the UK for training. The existing technical staff, however, was not found wanting. A system was designed and built, and soon key tape was being produced faster than it could be used. The new six-unit tape generator called BALLERINA, developed by T&D in the mid-1950s, produced ROCKEX key tape at twelve times the speed of the earlier equipment[16]. In all, six BALLERINA generators were constructed and set in operation, and production of ROCKEX key tape caught up with requirements in April 1956. Another high-speed generator known as BEAVER was designed and built to

15. For COMSEC Liaison, see para. 11.100 and following
16. See para. 19.29

meet the rising demand for PYTHON key tape (5-unit tape without format), used in 5UCO, ETCRRM and SIGTOT cipher equipment.

COMSEC Production for NATO

17.62 The Director of Communications Security (DCS) told the 17th CSB Meeting on 24 May 1955 that the US and UK were unable to supply all NATO cryptographic needs themselves,

T Group Moves

17.63 Operations in CB continued to expand. Key tape demand was growing - both for 5-unit (5UCO and SIGTOT) and for 6-unit (ROCKEX) tape. Basic code-books for use with one-time cipher pads were in preparation, with diplomatic vocabulary for External Affairs, and with military terminology for Canadian Forces. Insert production was in full swing and rotor production was getting under way. One-time pads, with series ranging from two-way up to 300-way, were being made for various departments. Overtime was instituted in ROCKEX tape production to meet rising commitments. Tape was being supplied for two 5UCO circuits to NSA. A second high-speed checker was being constructed, as was a photo-electric reading head for the checker and a timing pulse generator for a ROCKEX tape reperforator unit. A special timing unit was under construction for indicator insertion, to satisfy a requirement for SIGTOT tape specified by the RCAF. A second POKERFACE equipment was under development (for producing codes). Meanwhile, the Development Section had designed and built a prototype model of a proposed miniature ROCKEX cipher device[17]. All of CBNRC was growing, but T&D was expanding at such a rate that new quarters were essential. Construction of an addition to the Rideau Annex was considered and rejected. Early in 1955, as CB cast about for additional space, NRC was in the initial stages of planning the construction of a new building for its Pure Physics Division. CB was able to convince the Council to erect a wing of the planned structure ahead of time, and to allow it to be occupied by

17. See para. 22.8

T Group for two years (but the occupation actually lasted five years), and for it to be specifically designed and built to accommodate T Group operations. The building, known as M-36 Montreal Road Laboratories, was completed in the fall of 1956, and T Group moved in during November. Being on its own, the COMSEC part of CBNRC had to assume added responsibilities such as physical security, plant engineering and various other administrative functions. The planning continued for new quarters for CBNRC, however, and T Group technical and drafting personnel were regularly involved. Various sites were studied, such as the Radio Field Station on the Albion Road. After months of discussion and redrawing of plans, a number of new sites would be considered, until a satisfactory one could be found.

17.64 As indicated earlier, T&D had from the beginning been responsible for the installation and maintenance of the communications and cipher equipment in the CBNRC Comcentre. As plans were taking shape to move T&D out to the Montreal Road complex, it became obvious that the maintenance of Comcentre equipment would have to be done by technical staff resident in the Rideau Annex. Accordingly, eleven communications/cipher technicians were transferred from T&D to C Group in May 1955. (The T Group organization in 1957 is shown at Annex E.) A further divesting of responsibility occurred in April 1958 when all four members of the T&D Microfilm Unit were transferred to L Group. The unit had been organized originally by T&D because that was where the requisite technical expertise resided, but over the years the microfilming of records had become mainly a support function for SIGINT. All associated equipment and other resources were also turned over to L Group. T&D continued to be responsible for the maintenance of the equipment. Yet another responsibility was relinquished in April 1959, when the T Group Duplicating Section (T5) was dissolved and that function was taken over by L Group, which then became responsible for duplicating work for the whole of CBNRC with the exception of COMSEC requirements; the latter were supplied by the Book Production

section of T Group (T1), which also continued to do special printing jobs for other groups. T&D staff had climbed to 113 persons in February 1959, but fell back to 110 as personnel were transferred to L Group. Also in 1959, Bill Trowbridge was named Coordinator COMSEC[18]; Art Browness became T Group Head, with Ken Hughes as Operational Assistant and Gord Thomson as Technical Assistant. The organization of T Group in 1959 is shown at Annex F. The last staffing change in 1959 occurred when the Cipher Policy Committee at its 39th Meeting on 9 February 1959 approved the appointment of Mr. T.A. (Tom) Chadsey to succeed Art Browness as CANCOMSLO/W, effective July 1959.

Canadian Crypto Equipment Policy

17.65 The Communications Security Board, at its 24th Meeting on 27 February 1959, considered CSB/79. This paper was the outcome of a study by T Group, the CSG and CPC. In October 1957, the CSB had directed the Cipher Policy Committee to prepare recommendations for its consideration concerning a long-term Canadian cryptographic equipment policy. CSB/79 contained the results of this study. It reviewed in detail the latest developments in the UK and US in off-line and on-line cryptographic equipment and also in voice, facsimile and data protection devices. In response to a query regarding the type of personnel required to operate the on-line equipment, T Group Head told the CSB that the emphasis would shift from crypto operators to crypto technicians, since with on-line operation the encryption process was automatic; in view of the more complicated nature of on-line crypto equipment it would not normally be possible to train existing operating personnel up to the necessary technical standards. The equipment policy presented in CSB/79 coincided with NATO, US, UK and CANUKUS policies, and the equipment which would be acquired would be a combination of both UK and US developments, depending on the Canadian requirement. The Chairman of the CSB emphasized that in addition to reducing transmission time,

18. See para. 3.11

conversion to on-line would also result in a significant increase in security, not only because all the equipment provided high grade protection, but also because of a large-scale reduction in the use of plain language. Procurement of new on-line equipment was expected to be phased over a five-year period at an estimated cost of 33-million to 43-million dollars. There would, of course, be some savings if certain of the CSB/79 recommendations were effected. Employment of automatic key-generating on-line cipher equipment, where feasible, would result in a considerable downward adjustment in the commitment for Canadian produced key tape; at the time, key tape production constituted a rather extensive and costly undertaking. (By way of illustration, one 5UCO-equipped duplex circuit required a minimum of twelve editions - 24 reels - per 24-hour period, entailing a production cost of $54. The same circuit, equipped with KW-26 or other automatic equipment, would require only four to eight IBM cards, the production of which would involve a maximum expenditure of one or two dollars.) The most vulnerable and insecure communications are undeniably voice transmissions, and the greatest offender is the telephone. The CSB expressed regret that the recommendations in CSB/79 regarding the protection of telephone lines could not be implemented. The Secretary to the Cabinet, R.B. Bryce, spoke of the danger of serious leaks occurring in Ottawa as a result of the insecurity of telephones, and enquired concerning the cost of telephone speech secrecy devices. Air Marshal Campbell replied that the cost per unit was approximately $123,000, but expressed concern that failure to procure a speech secrecy device would preclude Canadian participation in discussions which the US authorities were able to hold by means of this device. Vice Admiral de Wolf emphasized the necessity for Canada to operate the same kind of equipment as that employed by our allies. CSB/79 recommended adopting cryptographic equipment wherever feasible, especially conversion to automatic on-line transmission, but acknowledged that progress in the field of speech secrecy must await further development of equipment within a price range that could be considered. The CSB approved the conclusions

and general policies of CSB/79, and agreed that each Service, Department and Agency should implement the policies insofar as they affected each individual user.

Calibration Laboratory

17.66 Because T Group performed many unique functions - e.g. detecting and measuring electrical, electronic or acoustical emanations - it required various highly sensitive devices of sophisticated design, often special-to-type, and occasionally of a kind that had to be developed and built in its own laboratories. These devices also had to be maintained in a fine state of adjustment, and this resulted in the setting up of a Repair and Calibration Laboratory, which in time became so expert that it was given the responsibility of repairing and calibrating instruments and equipment not only for all of CBNRC but also for some other departments. This became part of the new Crypto Equipment Requirements and Logistics Section (T5). The "Cal Lab" would do acceptance checks and routine inspection and recalibration of 50 to 75 instruments and devices each month.

ELSEC

17.67 As related in Chapter 16, concern was growing about the security risks presented by "non-communications transmissions". The signals emitted by such devices as radar and navigational aids when under development and test

Responsibility for formulating a policy for protecting such emissions (electronic security or ELSEC) was given in 1959 to the COMSEC community; the name of the CPC was changed to Communications-Electronic Security Policy Committee (CSPC), the CSG became the Communications-Electronic Security Group, the Director CBNRC's COMSEC mission was expanded to include ELSEC, and

17.68

Page 1141

is withheld pursuant to sections

est retenue en vertu des articles

15(1) - IA, 15(1) - DEF

of the Access to Information

de la Loi sur l'accès à l'information

17.69 A paper was drafted by CBNRC - CSPC/P/27, CSB/90 - entitled "An Investigation into the Security of Telephone Circuits", describing the situation and setting out several possible solutions. Among the options suggested were:

19. See para. 2.23 for the IPC

Pages 1143 to / à 1144

are withheld pursuant to sections

sont retenues en vertu des articles

15(1) - IA, 15(1) - DEF

of the Access to Information

de la Loi sur l'accès à l'information

Departmental opposition to having "outsiders" inspect their premises was finally overcome by the concern about radiation security, and CNBRC was given responsibility for TEMPEST. A Canadian Policy Paper, CSB/91, was approved by the CSB; it detailed the need for surveys of government telecommunications facilities to determine their vulnerability to the radiation hazard and to identify the appropriate protection measures required. The paper recommended that the Director CBNRC should assume responsibility in Canada for carrying out field tests and providing government departments with technical advice and assistance on radiation problems, and that he be authorized to acquire the resources required to carry out these tasks. CSB/91, therefore, was the mandate for CBNRC activity in the TEMPEST field. In addition, a CSG Radiation Working Party was set up in March 1960 to coordinate planning for the TEMPEST testing of government communications installations across Canada and at Canadian embassies and missions abroad.

17.74 To implement its mandate, T Group at first borrowed and later bought a truck, filled it with very sensitive detecting and measuring devices, and set out on surveys across Canada, in the US, and in Europe to ensure that Canadian government crypto-communications installations operated in as secure a manner as possible. The Mobile Survey Laboratory (MSL - a new truck and trailer) was received in April 1961, and brought into operation after being fitted with the necessary equipment. This was the beginning of what was to become one of the most important and most costly of CBNRC's COMSEC responsibilities, an activity which is dealt with in more detail in Chapter 24.

21. See Chapter 24 for TEMPEST activities

The Move to the Tilley Building

17.75 After more than four years of separation, the COMSEC part of CBNRC was reunited with the rest of the organization when CBNRC moved into the Sir Leonard Tilley Building in June 1961. The months preceding the move were marked by feverish activity on the part of T Group technicians. They were involved not only with the dismantling and reassembling of T Group production equipment, but also with many facilities for the Branch as a whole, such as the installation in the new building of an intrusion alarm physical security system with ultrasonic sensors, door detectors, a central guard communications system, a fire alarm system and a secure internal telephone system. The internal telephone system was not "secured" by the use of a crypto device, but was considered "secure" by virtue of the fact that the system was enclosed entirely within the building, with all cabling and exchange apparatus under the control and operation of T Group. They designed and built a coded door control for the Communications Centre. They also participated in the planning of the electrical wiring (with metal conduit and raceways) and plumbing and air conditioning installations, because these are all potential conductors of classified information signals originating within the building, and must be strategically located and protected so as not to carry such signals beyond the secure perimeter of the building.

Out with the Old - In with the New?

17.76 The requirement for keying material never stopped growing. As on-line equipment was introduced, it was expected that the need for key for off-line systems would all but disappear. Such was not the case, however. When newer and more

sophisticated systems became available, the older devices were allocated to lower echelon or back-up duties. The COMSEC aim was to see crypto applied to all transmissions of the Departments of National Defence and External Affairs and the RCMP - and any other government agency handling sensitive information - even unclassified communications, because these, although when viewed in isolation might be quite innocuous, when examined collectively usually reveal intelligence. Consequently, as cipher equipment was upgraded on circuits carrying highly classified information, the displaced device was usually not retired but moved to circuits on which transmissions had heretofore not been encrypted. The TYPEX equipment, for instance, which had been used during World War II, would see thirty years of service before being melted down and reformed into manhole covers. As well, keying material for use with KL-7 (ADONIS cryptosystem) was still being produced thirty years after that system was inaugurated. Because of the huge quantities of key tape necessary to support ROCKEX and 5UCO operations, every effort was made to replace these systems with non-tape-using devices. As a result, the 5UCO was replaced by KW-26 after less than nine years use (1950-1959) on the CB-GCHQ and CB-NSA circuits, and after less than three years (1959-1962) on CB circuits to the intercept stations. On the other hand, ROCKEX continued in use for 35 years (in fact, in the miniature version, NOREEN, it was just being inaugurated in 1984-85 as a cryptosystem for communication between Buckingham Palace and the Governors-General in Ottawa, Melbourne and Wellington). It will be realized that appropriate key had to be produced as long as a particular crypto device was in use. Even if key generating equipment was required to operate only occasionally, it had to be kept available. There were instances when production equipment was mothballed because no further requirement was foreseen, but then had to be set up again because a department had a recurring need for key.

17.77

Page 1148

is withheld pursuant to sections

est retenue en vertu des articles

15(1) - IA, 15(1) - DEF

of the Access to Information

de la Loi sur l'accès à l'information

Further Developments

17.79 Fortunately the use of key cards with KW-26 brought about a reduction in requirement for 5UCO tape, but unfortunately an increase in world tensions created a greater need for ROCKEX tape, especially multi-way tape for large nets. The spiralling requirement for multi-way editions of ROCKEX key tape in 1962 soon exceeded the capability of the existing

tape production equipment. Modifications were made to the high-speed generators and reperforators to enhance their capacity. Such stop-gap measures served the purpose for a while, but improvisation can only be effective for so long, and eventual replacement was necessary. The demand for other types of keying material was also increasing. CBNRC was lagging behind the state of the art in methods of production involving the use of manuscript. Many processes were labour intensive, including numerous manual procedures. The only automation in this area had been the introduction of an MP-2B, an NSA device, used with an IBM 407 tabulator to scramble cards containing random alphabets and numerals for the production of one-time pads, key lists and other crypto settings. Much of the checking was still done visually - for example, every character in the TRITON authentication tables was individually checked for correctness and readability. More detail on these processes is given in Chapter 19. Various means of improving the situation were studied, and in August 1963 it was decided to build a Canadian version of a GCHQ development called DAUPHIN. T Group converted the design from vacuum tube to solid state operation. The transistorized version was put into operation in October 1966. The development of DAUPHIN is covered in greater detail in paragraphs 19.38 and following. DAUPHIN not only gave added capability and flexibility, but also enhanced security because of various checks built into the production programs.

17.80 The research and development effort occasioned by the continuing need to update production methods had to compete for T Group attention with other high priority projects. The operational evaluation of new crypto devices (KW-37, KW-7, KL-4, KL-15, KG-14, KY-8, etc.) demanded considerable time and effort almost on a continuing basis. In addition, an important part of the COMSEC responsibility of CBNRC, although it engages fewer people than the production of keying materials, is the evaluation of the level of security attained on various Canadian communications facilities. Such

assessments are made either by reviewing the principles and rules employed by the communications authorities concerned, or by analysis of actual traffic provided for the purpose. For years, certain departments had been endeavouring to establish their own monitoring capability in an effort to discover and eradicate COMSEC weaknesses. After discussing the problem since 1955 in the CSG, they finally agreed in 1963 that the undertaking could be more efficiently handled by the National COMSEC Agency. The setting up of a monitoring and analysis section in T Group is treated in Chapter 23. During this period of increasing awareness of the vulnerability of communications, the Canadian COMSEC Community had become increasingly frustrated by the lack of success in reinforcing the security consciousness of persons with access to communications equipment. They eventually prevailed upon the Director CB to inaugurate a COMSEC Training Program and this responsibility was given to T Group. The account of the First Canadian COMSEC course and subsequent sessions is given in Chapter 28. Another function thrust upon T Group, after other departments had found themselves unable to cope with it, was the monitoring of cipher offices and other information-processing installations for electronic and acoustic radiation, evaluation of the risk arising from such radiation, and providing remedies to correct such TEMPEST problems[22]. Several TEMPEST documents were prepared by T&D and distributed to various departments, and in most instances "hands on" assistance was given in the installation and even operational training to ensure minimal compromising emanations from information-processing equipment. Screened enclosures were designed and frequently built upon request. These responsibilities, together with the recently imposed ELSEC task of assessing the threat to security resulting from the possible interception of Canadian non-communications electronic transmissions (e.g. radars, IFF, proximity fuses, etc.), mentioned in paragraph 17.67, enabled CBNRC to

22. See Chapter 24

obtain CSB approval to add a small number to the overextended technical and engineering staff on the COMSEC evaluation side. Authorization was given (IPC/5-61) to add three positions to the establishment to perform the added duties anticipated in connection with the planned production of ALVIS equipment. Not approved, however, was the request for five technicians to staff a mobile radiation facility.

Formation of S & T Groups

17.81 The campaign to produce crypto equipment in Canada gained in tempo, and the Test and Design Group became more and more involved. As the overall load increased on T&D, it was decided to divide the major responsibilities into separate groups. Since his return from duty as Canadian COMSEC Liaison Officer in NSA, Art Browness had been lobbying to organize CB COMSEC according to the three basic functions of Doctrine, Production and Engineering, the pattern used at NSA. COMSEC Doctrine, the whole body of knowledge of the procedures, processes, techniques and practices essential to the maintenance of security in communication, being more abstract than the other two functions, tended to be submerged, to lose its identity in one of the other two. T&D was divided on 3 February 1964 into two groups, S (Engineering) and T (Production)[23]. COMSEC Doctrine was first ensconced in T Group and some years later moved to S, never fully at home with either, its effectiveness always limited by the practical requirements of the technical and production operations.

17.82 S Group was responsible for all technical and engineering aspects of the Canadian COMSEC mission as assigned to the Director CBNRC. It was composed of three sections: S1, R&D, responsible for, among other tasks, construction of DAUPHIN and operation of the Calibration Laboratory; S2, Crypto Equipment and Communications Systems, charged with providing assistance and support to all Canadian Government users of crypto and communications systems and

23. See Annex 3.I

maintenance of the CBNRC secure (internal) telephone system; and S3, Electromagnetic and Acoustic Detection, responsible for conducting TEMPEST tests on crypto and other information-processing equipment and installations and designing protective devices to remedy TEMPEST weaknesses (such devices/enclosures/ modification kits were normally constructed in the T Group Model Shop). A fourth section, S4, Crypto Systems Evaluation, was set up in theory, intended to come into existence when personnel and facilities became available; in truth, the functions of S4 were performed by staff members borrowed from the other sections when evaluation projects required it and section workloads permitted it. For further discussion of Crypto Systems Evaluation, see Chapter 21. During the next few years, many S Group staff members were deeply involved in the production of a Canadian version of the ALVIS crypto equipment[24].

17.83 The new T Group was responsible for COMSEC Doctrine and for the production of Keying Materials. It consisted of five sections: T1, Book and Key Card Production, which also produced key lists and did all the production printing; T2, Key Tape Production; T3, Rotor and Insert Production, which also managed the Model Shop; T4, Technical Installation and Maintenance, which was responsible for servicing all crypto production equipment, the microfilm equipment in L Group and the Branch fire and instrusion alarm system; and T5, COMSEC Analysis and Procedures, which monitored Government communications and provided COMSEC evaluations thereon, gave COMSEC doctrinal support to government departments and managed the COMSEC Training Program for government departments. COMSEC Monitoring and Analysis is treated in Chapter 23 and COMSEC Training is covered in Chapter 28. The CBNRC COMSEC organization in 1964 is shown in Annex G.

17.84 The succeeding years found CBNRC COMSEC providing more and more support and assistance to members of the COMSEC Community. Every type of

24. See Chapter 22

crypto equipment used or proposed for use by Canadian Government agencies had to be operationally tested and TEMPEST-approved in S Group laboratories (see Chapter 21). Every crypto installation had to conform to regulations and standards provided by CBNRC. In addition, user departments called on CBNRC for assistance in installing and repairing crypto equipment, and security modifications were provided and often fabricated and sometimes even installed by CB technicians. T Group was the only authorized source of keying material for cipher devices used by Service or Civilian Departments. The Canadian position on COMSEC matters presented in CAN/UK/US, AUS/CAN/NZ/UK/US and NATO discussions was formulated in CB's COMSEC Doctrine Section (T5). S Group designed TEMPEST enclosures for computer installations for the Privy Council, the RCMP, Statistics Canada and M Group in CBNRC; for T Group's phototypesetters; and for an electronic translation system installed in the Government Conference Centre in Ottawa. In each case, S Group specialists were required to monitor construction, providing advice and direction, and then to conduct TEMPEST tests afterwards to ensure that the installation was secure[25]. Much travelling was involved. The TEMPEST teams conducted surveys of Canadian Government information-processing installations (crypto, communications, computer) in the Ottawa area and across Canada from Halifax to Vancouver, in Washington and London, and even in Lahr, Germany. COMSEC analysts participated in Canadian Forces exercises on the east and west coasts, in ships in the Atlantic, Pacific and Caribbean, at army bases in Alberta, and at Northern NORAD Headquarters, North Bay. Technicians travelled to intercept stations, even as far as Alert, and went aboard ships and aircraft, to assist with crypto installations. Personnel attended CAN/UK/US meetings in Washington and NATO COMSEC Agency meetings in the various Allies' capitals. COMSEC courses were set up at CBNRC for Service and Civilian Government employees grouped into three categories: Communications

25. See Chapter 24 for details

Officers, Senior Officers, and Warrant Officers (and corresponding level civilian personnel). The Head of the COMSEC Analysis Section travelled to Halifax and Kingston to give COMSEC lectures to larger groups of Service personnel than could be accommodated at CBNRC.

17.85 The expanding responsibilities which forced the restructuring of CBNRC COMSEC into two Groups also required major changes in facilities and extensive remodelling of S Group laboratories and the T Group Model Shop. More staff was added to the Mechanical Drafting and Design element of S Group. Requests for radiation testing of various equipment -- crypto devices, printers, typing reperforators -- signalled the need for a larger, more complete TEMPEST laboratory. Tenders were put out for a new screened room. As work progressed on the Canadian version of ALVIS, not only did S Group staff members have to visit the manufacturer's plant to provide basic COMSEC guidance, but as the various model stages were reached testing and demonstrations were carried out at CBNRC. Putting prototypes and production models through their paces at CB, described in Chapter 22, necessitated more space and more test equipment. Special jigs and TEMPEST enclosures built in the T Group Model Shop also required more specialized tools.

Quick Reaction Facility

17.86 The formation of a "Quick Reaction Facility" (QRF), to provide COMSEC support and assistance to government departments on short notice, had been advocated for years. As related in Chapter 18, the QRF was never formally established because no additional personnel could be obtained. Nevertheless, CBNRC COMSEC had begun in 1948 to provide quick reaction assistance to other departments, and this service was expanded as years passed. Subsidization could not be obtained for building up a small inventory of crypto devices or ancillaries to meet a sudden, unanticipated requirement by a government agency, but S and T Groups were often able to fabricate a temporary substitute until the most suitable solution could be found. This required

additional laboratory equipment and specialized tools and, over the years, T Group Model Shop and Device Fabrication Unit built up an excellent collection of power tools and special instruments, and developed an enviable reputation for being able to meet almost any request in short order. Some years later (1969), facilities were set up for the laboratory manufacture of experimental printed circuit boards.

Crypto Requirements for Telephone Circuits

17.87 In 1962 the CSPC had directed the CSG to examine the Canadian requirement for crypto in the speech, facsimile and data fields. This was in reaction to the growing concern about the amount of sensitive information being transmitted by insecure means.

CBNRC prepared a questionnaire to be completed by CSG Members in order to determine Canadian requirements. At about the same time (LCSA) London Communications Security Agency asked CB's A/D, during a visit by him there in August 1962, about Canada's position on speech secrecy. He replied that the Prime Minister and Cabinet were considering a proposal to buy the UK-developed PICKWICK system for certain fixed telephone circuits - an Ottawa area net to include 13 or 14 subscribers. Finances were, however, a major obstacle in view of the high initial capital costs of secure speech (ciphony) equipment and high recurring costs involved in renting special wideband Bell Telephone wire circuits. While it was hoped to have a decision before the end of the year, the outcome was expected to be unfavourable because of the current austerity program. There was also the problem of compatibility between such a local secure telephone net and future secure long distance telephone circuits. It was possible, therefore, that the TSEC/KY-3 (the US short-haul speech security equipment) might be used on the local net, in lieu of PICKWICK, to facilitate tie-in to long distance circuits employing US ciphony equipment which might be established later.

17.88 When it was learned that some speech equipment would become available earlier than expected, the CSPC directed that a separate paper dealing only with speech protection be prepared. The CSPC specified that the paper should indicate that "local and long distance telephone circuits, regardless of method of routing, are vulnerable to exploitation; that their protection is now technically feasible and that the costs of ciphony equipment are gradually decreasing". The paper was not to be a comprehensive work on the subject of secure speech networks, but rather was to serve as a guide for higher level consideration. The paper as prepared presented facts and figures regarding the availability and use of speech equipment, estimated costs for a typical secure network, and cost and availability data regarding suitable telephone circuits. The estimated costs for the Ottawa area net dismayed Canadian authorities, who asked that another study be made and another paper drafted. This, of course, served as a delaying tactic, and nothing further developed for two years. In the meantime, the campaign was also being waged to provide security on tactical voice networks.

17.89 In the late 1950s and early 1960s both the US and UK were developing crypto devices for protecting radio telephone transmissions. Two units of the UK DELPHI equipment were received at CBNRC in the summer of 1960 in order to undergo Canadian trials. DELPHI was a single channel, half-duplex, push-to-talk speech secrecy equipment suitable for protecting all classifications of information, up to and including TOP SECRET, transmitted on VHF, UHF and SHF radio channels, but not on HF or line circuits. Unfortunately the device was not compatible with either the Army or RCMP radio equipment. Laboratory tests were conducted at CBNRC, where modifications were developed and incorporated into the relevant radio equipment to achieve compatibility with the DELPHI cryptosystem. The Canadian Forces ordered eleven copies of DELPHI in 1965, and while awaiting delivery received eleven equipments on loan from UK authorities. They were used by the Fourth Canadian Infantry Brigade Group (4CIBG) operating within the

BAOR (British Army of the Rhine) in Germany. T Group obtained production criteria and developed techniques for producing DELPHI key cards, but was never called upon to produce them. Since 4CIBG worked with the British Army, UK-produced keying material was used exclusively.

17.91 Canada progressed more slowly, however, toward protection of its strategic networks. At the Tenth Meeting of the Intelligence Policy Committee (IPC) on 12 November 1964 the Chairman observed that the head of the US COMSEC Agency had visited Ottawa, and had outlined the large scale installation of speech security equipment in Washington and throughout US military commands. He had also expressed the opinion that as US Cabinet Ministers became accustomed to the use of crypto equipment amongst themselves, they would inevitably think twice before discussing classified matters on unprotected telephone circuits with their Canadian colleagues. Secure discussion between London and Washington had already been made possible using British crypto equipment,

As related above, Canadian authorities preferred to delay inauguration of a system until assured that it would be interoperable with future systems. As a result, the UK early achieved a measure of secure communications, whereas it would be many years before Canada would have even a small secure telephone net.

17.92 The CSG prepared another Secure Speech paper, IPC/2-64, whose aim was to postulate a hypothetical speech secrecy system for costing purposes, but to leave it up to the departments concerned to take the initiative in establishing their individual requirements. The Chairman IPC informed the Committee that speech secrecy was now available at a price, and that both the US and UK governments had already invested heavily in it. He said there was an increasing number of situations when it was practically impossible to avoid using the telephone to discuss classified matters with London and Washington, as well as within Canadian Government circles. The members were asked to make a list of officials requiring a secure terminal, starting with the Prime Minister and the Ministers of External Affairs and National Defence. The Committee discussed the paper, noted its conclusions, and agreed to ask the US and UK how they had gone about establishing priorities and standards for the introduction of their speech secrecy systems.

17.93 The Chairman CSG, in a letter to the Chairman CSPC in April 1966, expressed the concern of CSG Members over the apparent lack of progress in the task of providing secure speech facilities on certain local and long distance government telephone circuits. The response of the CSPC was to have the CSG prepare yet another draft of the Speech Secrecy paper. Again in May 1969, the CSPC directed the CSG to re-draft the paper, including, as was the case with the 1964 version, a hypothetical secure communications network for the Ottawa area, with the approximate costs of both narrow band and wideband speech security equipments updated. Problems were

encountered in determining the type of circuit to be recommended for the Ottawa area. Firming up proposals was also complicated by the range of crypto equipments available to fill the requirement. The major obstacle continued to be funding, as the new devices, particularly secure speech equipment, which were to become available in the 1970s, carried high price tags, and this made it difficult to sell the need for such expenditures to senior financial authorities in DND and the RCMP. External Affairs representatives, on the other hand, reported "little difficulty in obtaining funds for communications equipment and associated crypto equipment owing to the support of their Foreign Service Officers who were aware of the importance of secure communications". In order to assist departments in justifying a more appropriate share of funds for communications security measures, a policy paper was proposed to show the extent of the threat to the security of national communications, and ways and means of overcoming the threat through the use of appropriate cryptosystems and defensive measures.

MALLARD - TRI-TAC - SAMSON

17.94 As the various government agencies, including the Armed Services, sought to build up their communications facilities, each would give primary attention to its own basic needs, striving to eliminate superfluous items in order to avoid what might be considered unnecessary expenditures. This frequently led, for instance, to the nation's Armed Forces being unable to engage in secure communications with each other because each had a different cryptosystem. Usually, however, they insisted on having compatibility with the corresponding Service in allied countries. The Director of Supplementary Radio Activities (DSRA), Captain G.A. "Sam" Worth, had told the 76th Communications Research Committee (CRC) Meeting on 12 September 1951 that there was a need for greater coordination in the selection of cipher machines by users. Twenty years later, the Canadian Forces were still using a variety of systems, although a move had begun in 1965 to work toward interoperability.

17.95 Don Fairley of CB attended a Quadripartite Conference of the ABCA (American, British, Canadian, Australian) Armies in London in June 1965, at which NSA representatives made a presentation on secure speech facilities planned for tactical net working and point-to-point VHF/FM communications systems for the 1970-75 time period. Also presented was a proposal by senior US and UK scientists, who had been requested to look into the tactical communications systems being used by field armies and to recommend measures to offset the lack of flexibility, efficiency and interoperability of these systems. They proposed the cooperative development of a new secure tactical communications system to meet the expected needs of users after 1975. There followed a series of Quadripartite Meetings which led to agreement on the objective of Project MALLARD, which was "to produce a combined development plan for a secure tactical trunk communications system, with single channel access thereto, for the ABCA Armies together with the associated Air Force formations and where applicable, the Navies". The MALLARD system was to be fully automatic and primarily a radio system, providing subscriber to subscriber security, particularly for voice transmissions, but also embracing data, facsimile and telegraph circuits. Canada became an active participant in MALLARD in August 1965, when the basic Memorandum of Understanding (MOU) was signed by the Chief of Defence Staff (CDS) on behalf of Canada after Cabinet approval was obtained by the Minister of National Defence. The MOU designated MALLARD as a joint (ABCA) development effort with a shared cost/work program at a projected cost of thirty to forty million dollars (later increased to $126M). On the basis of her contribution of five percent of the cost, Canada was assigned five percent of development/production tasks (US - 62%, UK - 30% and Australia - 3%). Because of special considerations applicable to crypto equipment, the design, development and production of MALLARD were to be the responsibility of the national COMSEC agencies of the participating governments. Further, the development, testing, evaluation, procurement and production of communications security techniques, logic, technical

arrangements and equipment were to be as agreed among the national COMSEC authorities. The MOU specified that the provision of COMSEC advice to the national MALLARD Project Office, the PMB (MALLARD Program Management Board), the JEA (MALLARD Joint Engineering Agency), and to contractors engaged in R&D work for MALLARD, would be the direct responsibility of the four national COMSEC Agencies, i.e. NSA, CESD (now GCHQ/CESG), DSD and CBNRC. The national COMSEC Agencies were to provide representatives to the JEA to ensure the proper integration and compatibility of COMSEC equipment with the MALLARD system. Various S Group staff members participated actively in the formulation of basic COMSEC guidance (during Phase I), conducting studies and attending meetings in Washington and London and at Project MALLARD headquarters, Fort Monmouth, N.J., as operational and technical requirements were defined. CBNRC hosted a meeting of the MALLARD COMSEC Agencies in June 1970.

17.96

Page 1163

is withheld pursuant to sections

est retenue en vertu des articles

13(1)(a), 15(1) - IA, 15(1) - DEF

of the Access to Information

de la Loi sur l'accès à l'information

17.98 CBNRC had made a considerable contribution to the MALLARD Project. Two senior staff officers and several working level personnel had attended frequent meetings in London, Washington and elsewhere; and a senior technical officer had been committed to full time attendance for a period of twelve weeks in 1969 as a member of the International System Selection Board at Red Bank, N.J., determining the technical parameters and specifications intended to be applied in the MALLARD system, including crypto components. In particular, the time involved in studying R&D material, in order to provide COMSEC engineering advice to the Canadian firm developing the subset, engaged three to four senior COMSEC officers for at least fifty percent of their time. There followed a 'phase-out' operation involving CBNRC and ITTC. A 'stop-work' order from the Department of Supply and Services (DSS) on 18 January 1971 ended the firm's right to hold classified items associated with the project and brought S Group in to wind down the operation. CBNRC's involvement in MALLARD ceased in June 1971 with the completion of disposal action respecting the documents and model sub-assemblies held by the Canadian MALLARD contractor.

17.99 All the work was not in vain, however. The effort was reoriented to meet the requirements of the US Tri-Service Tactical Communications Program, to be known as TRI-TAC. The MALLARD organization would remain intact at Fort Monmouth, but would be

augmented by the participation of USAF, USN and the Marine Corps. The Canadian Forces Liaison Officer assigned to TRI-TAC insisted that TRI-TAC was not a replacement nor a follow-on to Project MALLARD. TRI-TAC would not design, develop or produce equipment, but would sponsor such equipment as met TRI-TAC specifications. Individual Service require- ments would be acknowledged and accepted, so that equipment need not be standard but would have to be interoperable. Communications would be digital because the existing inventory of analog equipment did not provide for the rapidly expanding require- ments of the Services, Canadian as well as US, in terms of capacity, quantity, speed of service, reliability, security or joint service interoperability. While primarily concerned with tactical communications, TRI-TAC also aimed at interoperability with other government communications and international telecommunications systems. The program covered the spectrum from desk telephones to satellites. The COMSEC system to be used with equipment developed under the TRI-TAC program was known as TENLEY. The TENLEY family and ancillary equipments included key generators, loop encryption devices, trunk encryption devices, automatic key distribution centres, circuit switches and store and forward facilities. New switches were to be introduced in the mid-1970s to facilitate the transition from an analog to a digital system in the early 1980s. TENLEY offered improved security and reliability, while at the same time reducing size, cost, weight and power requirements when compared with existing equipment of similar capability. Probably the most significant advantage of TENLEY was the elimination of keying material; key variables were electronically generated and distributed. With the collapse of the MALLARD Project, Canadian authorities too realized that they would have to lay their own plans for the development of a national secure switched communications system to replace the network in use in the Canadian Armed Forces in 1971. Thus was born SAMSON.

17.100 SAMSON is an acronym for Strategic Automatic Message Switching Operational Network. It was the Canadian program to develop a national strategic

communications net to provide secure data and telegraph circuits for operational and administrative communications between DND bases. It involved seven automatic relay centres joined by 2400 b.p.s. communications links and protected by crypto equipment of the KG-30 family as well as by ALVIS. SAMSON was roughly equivalent to the US AUTODIN (AUTOmatic DIgital Network), a high-speed four-wire, non-blocking switching system for use with automatic digital message switching centres designed to provide a rapid, store-program-controlled, store-and-forward method of handling digital traffic. A project was initiated to consolidate all US/CAN cross-border circuits and to automate as many as possible into a SAMSON/AUTODIN automatic interface.

17.101 DND proceeded on the assumption that the SIGINT network would be integrated into SAMSON. CBNRC were not enthusiastic about the prospect, partly because they were not consulted in the early planning, and so were not familiar with the program and what was involved. NSA were also cautious about the integration of SIGINT traffic into AUTODIN. In an internal DND letter to the Director of Communications Requirements and Support (DCRS), the Director General of Intelligence and Security (DGIS) had agreed that supplementary radio activities traffic should, in principle, be handled by SAMSON. As a program change was in any event going to boost the overall cost of the project from 70 million to 90 million dollars, 2.2 million dollars could also be included for SIGINT traffic handling. On 26 August 1971 LCdr. W.D. (Bill) Moyes and his staff from NDHQ briefed CBNRC officials on the SAMSON system. They said a high-speed terminal was planned for CBNRC, which would be fed via Valcartier. A concentrator at Lahr for Canadian national use would provide an international interface to the US, UK, Australia and New Zealand. Coordinator of Technical Development (Coord/T) (Bob Grant) indicated decreasing opposition from CBNRC, and acknowledged that SAMSON could "take a big load off CB and save the government money". At a meeting of DND and CB officials in Mr. Grant's office on 6 November Mr. Moyes requested a firm indication by 16 November on whether the extra 2.2

million dollars should be included in the submission to the Treasury Board. Mr. Grant replied that a study of long-term SIGINT communications requirements was currently in progress, but that the report was not expected until mid-1972. He outlined some of the changes that were envisaged, and noted that there would be considerable reduction in message format traffic. There would be a trend to data entry and remote querying of computers by customers, and the "probe" concept would be developed whereby remotely operated control computers would be located at intercept sites.

17.102 However, CB eventually agreed to the DND proposal, and funds for the inclusion of SIGINT communications were included in the submission to Treasury Board. Preliminary investigations got under way to determine the "best Canadian communications posture within SAMSON for the transmission of intelligence traffic (including CRITICOMM) commensurate with adequate security". CBNRC accepted that DND/DCSE was the design authority for SAMSON, but retained responsibility for monitoring and signing off for intelligence communications aspects. Although financing was basically provided by DND, some of the engineering was done by CBNRC. Bob Grant insisted that CB continue to have a substantial input because of tripartite relationships and operational considerations. Since CBNRC would be required to maintain and support an LDMX (Local Distribution Message Exchange), CBNRC should have a voice in equipment selection and some managerial responsibility. CBNRC liked the concept of placing the LDMX at Carp instead of the original assumption that it would be located at CBNRC. The latter arrangement would demand a substantial increase in manpower, equipment and floor space at CB, whereas this burden would be transferred to Carp if the switch were situated there. Other advantages would accrue from the Carp location: a "no break" power supply; a physically and electronically secure site (which would be costly to provide at CB); a hardened site and hardened cables; and the availability of emergency communications. Location of the switch at CBNRC would require supplementary physical and electronic protection and the

addition of a fifth floor to "A" wing of the Tilley Building. Discussions on the pros and cons of each location continued till the mid-70s, when it was finally decided to establish the LDMX, by then called OSAX (Ottawa Semi-Automatic Exchange)[26], at Carp, with a concentrator at CBNRC. The SAMSON schedule had called for Final Program Approval in September 1972 and activation of the initial system in November 1975. There was considerable slippage, however, and SAMSON was not inaugurated during the period covered by this History.

Reorganization of COMSEC in CB

17.103 Bill Trowbridge's death in July 1971 was followed by a reorganization in September. Art Browness was named Assistant Director COMSEC[27] and Gord Thomson succeeded him as T Group Head. At this time it was decided that T would be concerned only with Key Production, including responsibility for the development and fabrication of equipment to produce keying material. This was made possible with the transfer of Herb Bergen and Al White to T Group. COMSEC Doctrine would continue to be handled by Ken Hughes, who moved to S Group, taking with him the responsibility for directing the COMSEC Courses which soon were being given four times per year. COMSEC Analysis also moved to S Group. The CB COMSEC organization in 1972 is shown at Annex H.

More on Secure Speech

17.104 In 1971 the decision was made to undertake another revision of the speech secrecy paper in view of renewed emphasis on the need for telephone security coupled with improvements in telephone "attack" techniques. This time it was thought that the most effective approach would be a short paper reiterating the need for ciphony equipment, and directing the departments concerned to prepare a list of actual requirements. The CSPC approved the new

26. See para. 14.106
27. See para. 3.14

approach, including replacement of the "typical network" in the appendix to the paper with a realistic coordinated departmental plan for a secure telephone network.

17.105 An article by a USAF Sergeant, printed in Ramparts magazine in August 1972, claimed that the US Government could and did read Canadian Government encrypted communications because Canada used cipher machines designed by NSA and built in the US. He said that this applied to all US allies, despite agreements made between the countries: "... the treaty is a one-way street. We violate it even with our Second Party allies by monitoring their communications constantly ... we also monitor their diplomatic stuff constantly ... These allies can't maintain security even if they want to. They're all working with machines we gave them. There's no chance for them to be on a par with us technologically." This, of course, was very disturbing to officials of the Canadian Government. The Director CB was able to assure members of the Cabinet Committee that the US was not likely to be reading our enciphered messages. He made the point that the integrity of an encipherment is based upon the keying material used and, as Canada has produced her own keying material since COMSEC production was inaugurated in CBNRC in 1948, government classified information enciphered with properly used high grade crypto systems is considered to be secure from cryptanalysis. Nevertheless, during the next few years the struggle continued to convince federal officials of the need to protect all government communications, particularly telephone conversations, and to persuade them that the large expenditures involved were warranted. As mentioned at the end of paragraph 17.93, a "Threat" paper was in preparation. The Security Advisory Committee (SAC), at its Sixth Meeting on 26 September 1972, considered and approved CSC/P/1/72, "The Threat to the Security of Canadian Government Communications". SAC also approved at the approved at the same meeting, CSC/P/2/72, "Cryptographic Security Policy for the Protection of Canadian

Government Communications". Both papers were forwarded to the Interdepartmental Committee on Security and Intelligence (ICSI)[28]. The "Threat" paper was intended to provide background and support for the "Policy" paper, and also to furnish departments with valid and persuasive arguments when seeking financial approval for the procurement and installation of crypto equipment. The "Policy" paper reviewed and updated CSB/79, the policy paper of 31 December 1958 which had been mainly concerned with telegraphic systems[29]. The new policy paper recognized the increased importance of securing other modes of transmission, e.g. speech, data and facsimile.

17.106 A Secure Speech Working Party was formed, chaired by Don Fairley of CBNRC and made up of representatives from DND, External Affairs, RCMP and the Department of Communications. It was a time of great development in crypto, especially in the ciphony field. Progress with some devices was halted as newer, improved ideas came on the scene, and as problems with bandwidth were overcome. Don Fairley visited the UK and US, and briefed the Working Party on developments in tactical and strategic voice equipment. In particular, he described for the members a new US project code-named BELLFIELD, which could provide high quality speech over 3 KHz bandwidth using normal lines, and which was the forerunner of equipment acquired years later for the secure telephone network in the Ottawa area. BELLFIELD was a program to develop a high-grade narrow band secure voice system designed for switched telephone networks, employing a complex arrangement of keying variables. The objective was to move from an all-analog to an all-digital system. GOLDWINE/CARLOS was the telephone subscriber unit which included a speech processor, key generator, control unit and modem. The system was designed to work through a key distribution centre which was to be a computerized distributor of keying variables on a per

28. See para. 16.16
29. See para. 17.65

call basis. Within CBNRC, R Group was responsible for coordinating the requirements of the Branch, and for ensuring that sufficient funds were included in the estimates at the appropriate time.

17.107 The plan was to implement the program in two phases: Phase I would be based on a Central Processing Unit (CPU) version of the Telephone Subscriber Unit (TSU) as an interim system by 1977; and Phase II, involving an LSI (Large Scale Integration) module version by 1981. R Group proposed that CBNRC acquire two GOLDWINE TSU's which would have up to three extensions each. The units were to be located one in the Directorate and one in L Group. Although Phase I for the Ottawa area considered the possibility of establishing two networks, one at the ministerial level and the other at the operational level, the CBNRC terminals would access only the operational network. As each department or agency was responsible for purchasing its own TSUs and associated equipment, R Group proposed the inclusion of a budget item of $70,000 for two GOLDWINE terminals in the CB FY 76/77 Program Planning. Once again, the cost of the program was the cause of its downfall, and no GOLDWINE terminals were ever procured.

17.108 CBNRC had purchased two TSEC/KY-3 equipments in June 1968 for laboratory evaluation and demonstration, when it was thought that this might be the device around which a network would be established. The equipments cost less than $6,000 each, and many times in the next fifteen years Canadian departments wished they had bought a hundred or more. The impediment, however, was the need for conditioned telephone lines for use with the equipment, imposing a heavy recurring cost. Before long (August 1968), the two KY-3s were pressed into service between CBNRC and RCMP Headquarters; one KY-3 was loaned to O Group, the other to RCMP HQ. When problems were encountered at the RCMP terminal, special installation criteria had to be developed by S Group to use the KY-3 with multi-gauge instead of conditioned telephone lines. Later relocation of the RCMP terminal resulted in reconversion to conditioned lines. The arrangement

worked so well that CBNRC had great difficulty in reclaiming the KY-3 from the RCMP ten years later, when it was needed for a CSE-NDHQ secure telephone link. (In 1985, the two KY-3s were still rendering yeoman service between the Tilley Building and NDHQ as CSE's link to the Secure Ottawa Area Network and the US AUTOSEVOCOM.) When secure telephone communications were established between the Prime Minister in Ottawa and the President in Washington, KY-3 equipment was made available on loan from the USAF to Canada. Other than these instances (and a few very temporary hook-ups), Canada had no secure telephone service until after the period covered by this History.

Use and Security of Computers

17.109 It became clear that automation would supplant manual operation in the SIGINT process, and CBNRC personnel felt the need for experience with a computer, even one of limited capability. In July 1960, the Mechanization Committee[30], on which all CB Groups were represented, agreed unanimously to recommend that CBNRC should rent an IBM 1401 computer system. It was to replace some of the machinery currently rented by the Branch, and the increased speed of operation would largely pay for the extra expenditure, which was relatively small. The 1401 could be ordered on a building block principle, so that, if requirements demanded, advanced computer equipment, such as tape drives, could be added. The 1401 operated on a "stored program principle" and was, in fact, the first machine with any computer capability (except for the random key generators and checkers used by T Group) which it had been practical for CB to consider. It was a variable word length machine with some magnetic core storage, but since CBNRC's SIGINT tasks required a very large storage capacity for a relatively small volume of material, it would be necessary to add magnetic tapes before large "memory" projects could be tackled. The other

30. See para. 13.3

Centres were experimenting with various types of computers, not all of which were compatible with the IBM 1401, but it would be possible to set up peripheral operations to increase compatibility. For one thing, there was the possibility of an attachment to the 1401 to change it from a "binary coded decimal" to a "binary" machine.

17.110 The first project scheduled to be undertaken on the 1401 was the checking of key cards produced by T Group for KW-26 and KW-37 crypto equipment, which at that time had to be sent to NSA for checking. Having to send the material to Washington was not only a slow and awkward arrangement, but it also meant that national keying material was available to another country. In fact, this was one of the strongest arguments used in seeking authorization to acquire the 1401: Canadian COMSEC policy provides that foreign-made cipher machines will be accepted for Canadian national use only on the condition that Canada produce and control the keying material for such machines; under existing conditions it would be possible for a foreign power to read national classified communications enciphered by the KW-26 or KW-37 key cards; acquisition of the 1401 would eliminate that potential security risk[31]. After serious consideration of all the options available, it was decided that the most practical and economic course of action would be to buy the equipment rather than to rent it. In July 1961, Chuck Hellyer reported to the Mechanization Committee that CBNRC had formally placed an order to buy an IBM 1401 machine. It would have an 8,000-character core memory and four magnetic tape units; in addition to the 1401 Processing Unit, there would also be the 1402 Card Read Punch and the 1403 Printer. The machine operated in sequential fashion, searching at 20,000 characters per second, and had a read-out speed of 600 lines per minute. For CBNRC's special purposes, of course, the equipment was modified from the regular version: it had a "space suppress" device,

31. See para. 17.105

a cyrillic chain and certain unconventional symbols. It was standard in other ways, e.g. the input was by cards, but then the record could be transferred to magnetic tape if necessary. The IBM 1401 was delivered in March 1962 and was operated by M Group for ten years. After it was replaced by an IBM 370/145 in March 1972, the IBM 1401 was transferred to T Group in August of that year[32], and continued its key material production functions for another twelve years.

17.111 Although much was said about the risks associated with interceptible emanations from information-processing equipment, very little attention appears to have been paid to the security of computer installations in Canada before 1965. CBNRC COMSEC had its hands full with the concern for crypto and other communications-associated equipment. Computers that were involved with communications systems were gradually regarded by COMSEC authorities to be within their jurisdiction - as for example, a computer used as an "intelligent switch"; whereas even this would often be regarded by computer security people as being subject to their authority. In June 1965, a Canadian military representative at an ABC Armies Working Party meeting was surprised to learn that "a major difference existed between Canada on the one hand and the USA and the UK on the other as to the requirements for security in computer work". The regulations within which US and UK agencies operated required that programs containing secret data be run on computers physically located within secure areas. The Canadian view, he understood, was that as long as the program involved purely quantitative or logical symbols, with no indication as to their meaning, the classified data would receive sufficient protection. This, of course, engendered a false sense of security, which often led to people taking more risks than they would have if they had known that there was no security protection. He concluded, therefore, that "in this

32. See para. 13.12

matter, Canada is, and has been violating the basic standardization agreement which calls for the provision of security arrangements by a recipient similar to the security afforded in the country of origin". He requested guidance. An enquiry was made of the DND Directorate of Scientific Intelligence (DSI) who in turn requested the Defence Research Member of the Canadian Joint Staff in Washington to seek information from US authorities on the subject of computer security. The Defence Research Board (DRB) representative referred the matter to John Lewis, CANSLO/W, in the hope that NSA might have information on the subject. Although Mr. Lewis felt that computer security was not within his terms of reference, he made enquiries at NSA and was rewarded with two copies of an excellent paper entitled "A Summary of TEMPEST Characteristics of Computers". One copy was given to the DRB Liaison Officer and the other sent to CB. (In fact, the US Government had not delegated responsibility for computer security to any agency; each interested party began assembling information on the subject; because of its operations in TEMPEST and related fields, however, NSA soon developed an expertise and fund of knowledge about computers, and most agencies turned to them for advice and assistance.)

17.112 Three months earlier, Don Fairley had visited NSA where he learned that the Agency computer installations were contained in rooms with screened walls, that spatial radiation of a compromising nature from the IBM 1401 computer might be picked up at distances of 500 to 600 feet, and that conducted radiation might be available at much greater distances. This caused consternation at CBNRC because the Branch's secure perimeter was no more than 50 feet, and the TEMPEST hazard had not been considered when the 1401 was being installed in M Group. S Group's TEMPEST facilities had been acquired as needed, and since field surveys were conducted on a "request" basis and only crypto centres had availed themselves of the service, the detection equipment was of a type designed to respond to emanations from crypto-communications equipment. Nevertheless, using the mobile laboratory, a radiation evaluation of the

M Group IBM 1401 computer installation was undertaken, including the 1403 printer and the 1402 card read punch, as well as the power mains leads and other conductors in the area. As expected, the detection capability was found to be inadequate, but what results were obtainable were found to parallel NSA's findings, with the worst offenders being the ancillaries, such as the output during punch card operations. As in the US, the responsibility for the security of Canadian Government computers had not been delegated to any specific agency. Five more years would pass before federal authorities would become sufficiently concerned, and actually take steps to minimize the risk of physical and electronic access to automatic data processing equipment. S Group obtained more detection devices, and in 1966 and 1967 conducted radiation tests of M Group's IBM 1401 computer. In 1971 and 1972 DND and the Privy Council Office (PCO) had S Group survey their computer installations[33].

17.113 The use of computers with magnetic tape gave rise to additional security problems. Tapes could be reused if the information stored thereon were completely removed. Degaussing, the process of demagnetizing the tape and erasing the stored data, was considered successful if no residual information could be detected. Tapes which had been used to store classified information could then be declassified and returned to a central supply bank. Unfortunately, more sensitive detection equipment somesometimes could pick up information from tapes that were returned as "clean". The fear was that even more sensitive detectors would be developed, until no assurance could be given that information could not be obtained from a tape after degaussing. T Group was first involved in studies in this field in 1959, but limited facilities forced the Director CBNRC to inform the Vice-President (Scientific) of NRC that we were unable to engage in research projects involving non-communications equipment. S and T Groups were

33. See Chapter 24 for TEMPEST activities

caught up in later investigations and discussions which ensued - S Group in the laboratory tests and T Group in the physical protection of magnetic tapes used in the production of keying material. In the final analysis, it was decided that magnetic tape used to store classified information should be segregated, even after degaussing, according to the level of classified information which had been stored thereon. Tape used in key production would be destroyed by burning. A related function that involved S Group personnel was the investigation into the deterioration of information stored on magnetic tapes subjected to magnetic fields. Test jigs were developed, and a variety of permanent magnets and electro-magnets were acquired for tests to ascertain the effects of magnetic field strength on the degradation over time of information (chiefly digital information) stored on magnetic tape, to a point where it could not be recovered by any standard system.

Protection of Mobile Voice Communications

17.114

17.115 The search for voice communication protection for the RCMP was not an easy one. Canadian Government policy, arrived at after exhaustive study of the pros and cons, had been to undertake development of crypto devices only when a particular need could not be satisfied by cipher equipment produced or planned by the US or UK Governments. D/CANSLO/C asked NSA to investigate the possibility of adapting a secure voice module they had under development, the TSEC/KYV-2, for use with the Motorola radio used by the RCMP. After several months study, NSA concluded that the modifications that would be required would render such a project impractical. No other US or UK crypto development was found to provide the required answer. A Canadian development seemed to be the only solution. As a result, the RCMP asked CBNRC to participate in a feasibility study which was given the nickname NADIR. The NADIR Project developed into a joint endeavour undertaken by CBNRC, the RCMP and the Communications Research Centre (CRC) of the Department of Communications (DOC), to investigate the feasibility of developing a secure digital speech system that could be fitted to RCMP mobile units and hand-held radios. The division of tasking amongst these agencies was that RCMP/CRC would study and/or develop the analog-to-digital converter and the frequency shift keying elements of the system, while CBNRC would investigate the feasibility of developing the cryptologic element.

17.116 S Group, with its staff bolstered by one cryptanalyst, undertook the cryptological study, beginning in November 1973. The design approach was to have the crypto element based on an electronic key generator of a type similar to that used in approved official crypto equipment. In examining the underlying mathematics necessary to the development, S Group conducted in-depth studies of key generation, particularly in the area of characteristic generating polynomials for linear recursive sequences; of complement register generators of the KOKEN type; and of cipher-text auto-key systems. Subsequent studies involved combinatorial logic, key variables and key changing methods, all with the aim of selecting the most satisfactory approach. Elements of S Group worked full time on the project during the next ten years as related in Chapters 21 and 22. Many events in the development of NADIR took place after the period covered by this History.

Fibre Optics

17.117 In 1973 an S Group engineer began an experiment in Video Voice Data Transmission, using light emitting diode sources, fibre optic cable transmission media and pin photo detectors. The experiment was intended as a familiarization exercise in the field of fibre optic transmission. A make-shift video system, using equipment borrowed from areas where it had non-video processing applications, was set up to ascertain whether video information could, in fact, be passed through the system. Only marginal transmission quality was achieved, but the results were sufficient to warrant further experimentation and the acquisition of better facilities, including an improved fibre optic waveguide and the fabrication of more suitable peripheral electronics for the bench-top system. Further redesign was necessary, and the development of devices to transmit and receive a synchronized signal from equipment under test to other equipment used for analysis by means of a fibre optic tube continued beyond the period covered by this History.

17.118

Jurisdiction Over COMSEC Matters

17.119 As mentioned in Chapter 18, members of the Canadian COMSEC Community had direct contact with CBNRC for COMSEC advice and support. The Branch had no authority to dictate or prohibit in matters of security, but was empowered to provide guidance and assistance in COMSEC activities. Unfortunately, departments and agencies who were not part of the COMSEC Community were not aware of the existence of a COMSEC organization. Some, not knowing of a source of guidance, and having no expertise in this area, unwittingly indulged in insecure communications practices. Others sought and obtained assistance from the RCMP or DND or were referred to CBNRC. The Department of Communications (DOC) had been established in 1969-70 and, after obtaining membership in the interdepartmental COMSEC committees, was able to provide a channel for non-COMSEC-Community agencies

to CBNRC[34]. At first, there had been a move by the Department of Communications to absorb all Federal Government communications functions, but as External Affairs and National Defence communications had been established by separate statute, they were able to maintain their autonomy. CBNRC, however, being a Branch of the National Research Council not protected by its own statute, was for a time a candidate for absorption into the DOC. The special nature of CBNRC was finally realized and it remained a separate entity. To provide a "front" for CBNRC with non-COMSEC-Community agencies, a COMSEC cell was formed in DOC.

By Any Other Name

17.120

34. See para. 16.19

The awkward situation in which CBNRC COMSEC had existed for years - not being able to identify itself, but needing to advertise its ability to provide essential communications security assistance - was resolved to some extent when CBNRC became part of DND in 1975 and had its name changed to the Communications Security Establishment (CSE). At last its function was legitimate, at least as far as the "COMSEC side" was concerned. The need for a low profile was no longer so great. It was on 15 January 1975 that the Cabinet Committee on Security and Intelligence agreed that CBNRC should be designated the Communications Security Establishment, should become a distinct entity within the Department of National Defence, and should continue as the national agency responsible (inter alia) for the Canadian COMSEC program. Order-in-Council P.C. 1975-95 of 16 January 1975[35] gave effect to the changes by transferring "control and supervision" of CBNRC to the Department of National Defence, effective 1 April 1975. While DND would be responsible for administrative arrangements for CSE and would be accountable for it to Parliament, operational policy guidance and direction would still

35. See Annex 2.F

come from the committee structure under the Cabinet Committee on Security and Intelligence. CSE COMSEC operations and objectives were the same as those of CBNRC, viz. on behalf of the Government of Canada, to direct, supervise and administer the Canadian communications-electronic security program: "to meet the requirements of the government for cryptographic keying material, COMSEC devices and documentation efficiently and effectively; and to ensure that the Federal Government is advised on the planning, acquisition, installation and procedures for use of secure communications-electronic systems so as to provide an appropriate level of security at an acceptable cost." The Director CBNRC was renamed Chief CSE, and was designated Manager of the Canadian COMSEC program, accountable to the Chairman ICSI. This accountability is delineated at Annex I. The responsibilities and functions of CSE as the Canadian COMSEC Agency, as approved by the Security Advisory Committee on 11 February 1975, are listed at Annex J.

Chapter 17/Annex A

Extract from CRC/73
June 5th 1948

3. Test and Design Section of C.B. - Terms of Reference

The Communications Branch of N.R.C. which functions under the jurisdiction of the C.R. Committee will organize a Test and Design Section whose scope of duties and responsibilities will be as follows:

(i) To provide and be the channel for clearing of secure cipher systems for the Services and the Dept. of External Affairs when facilities become available.

(ii) To print and produce all ciphers which could be produced in Canada for own use by the staff and machinery authorized for such purposes.

(iii) To examine and report on the security of codes and ciphers used by the Services and the Dept. of External Affairs. This service could be made available in other cipher using Government Departments upon the request of the C.R. Committee.

(iv) To examine and keep under review the various procedures applied to the different cipher systems and to ensure that the maximum degree of standardization of systems and procedures is achieved.

(v) To ensure that the directives of the C.R. Committee and the Communications Security Group are carried out by all cipher using Departments.

(vi) To advise on all matters concerning communications security.

(vii) To give the best possible security advice to the traffic handling authorities, so that they are aware of risks involved, if due to operational requirements, security regulations are relaxed in any way.

(viii) To advise on types of ciphers to be used under varying circumstances and conditions.

(ix) To advise re policy concerning the safeguarding of cryptographic material. The aim should be to achieve the highest possible standards of safe custody.

(x) To assist in the training of cipher operators and maintenance personnel by preparing or procuring the necessary training data and to provide lectures on various aspects of security in the use of ciphers.

(xi) Assist in the drafting of rules and regulations to ensure proper security supervision re handling of cipher messages, especially by non-cipher using Departments.

(xii) To investigate incorrect use of ciphers and cipher settings and suspected compromise.

(xiii) The collection and analysis of cipher returns.

(xiv) Advise re disposal of obsolete or surplus ciphers.

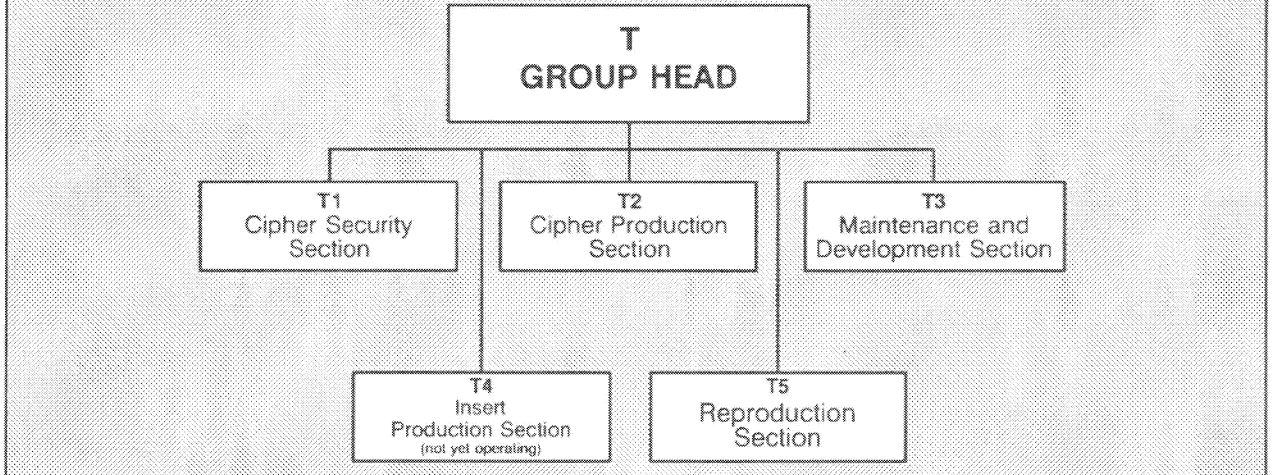
(xv) To operate an accounting service for all ciphers used in Canada supplied by C.B.

(xvi) To report on and carry out research into the design and development and production of cipher machines, cipher systems and other security devices.

G.G. Crean,
Chairman, C.R.C.

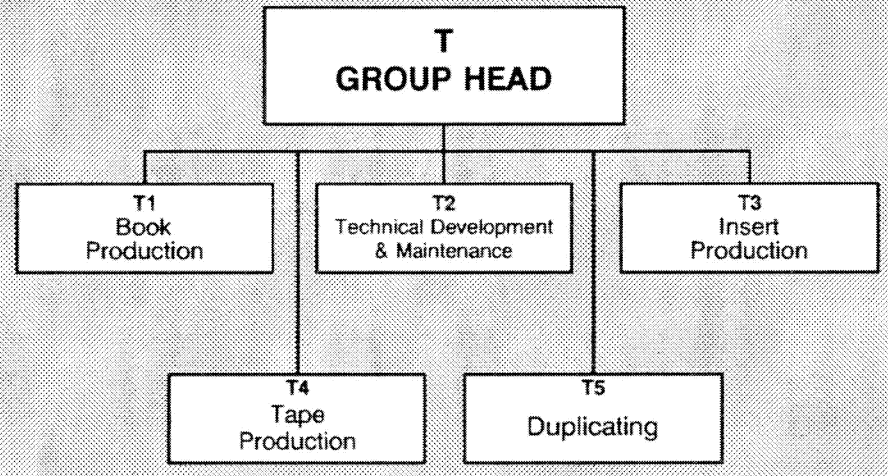
1950

CB COMSEC ORGANIZATION



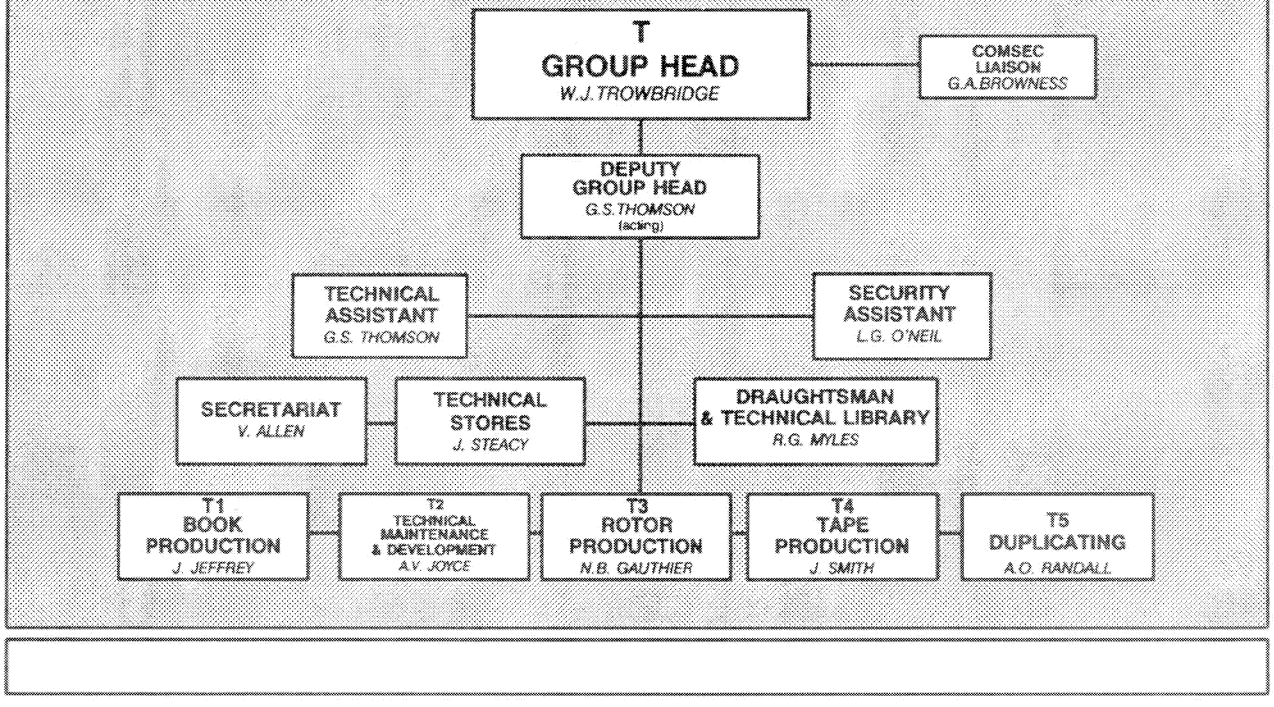
1952

CB COMSEC ORGANIZATION



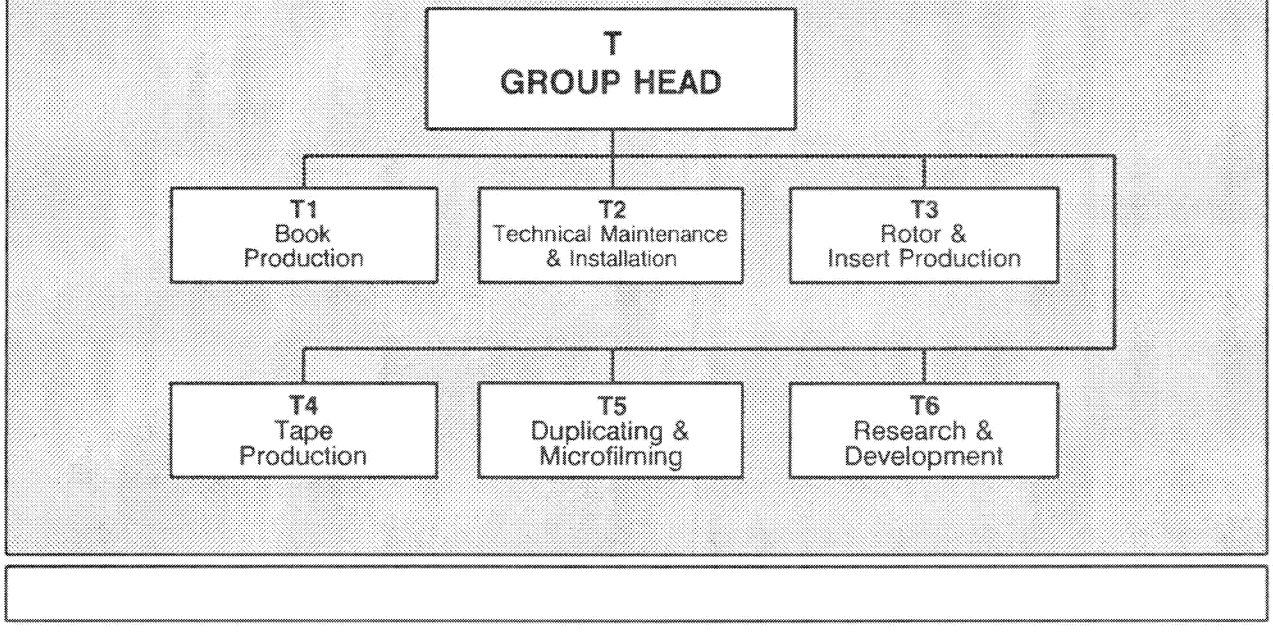
1955

COMSEC ORGANIZATION



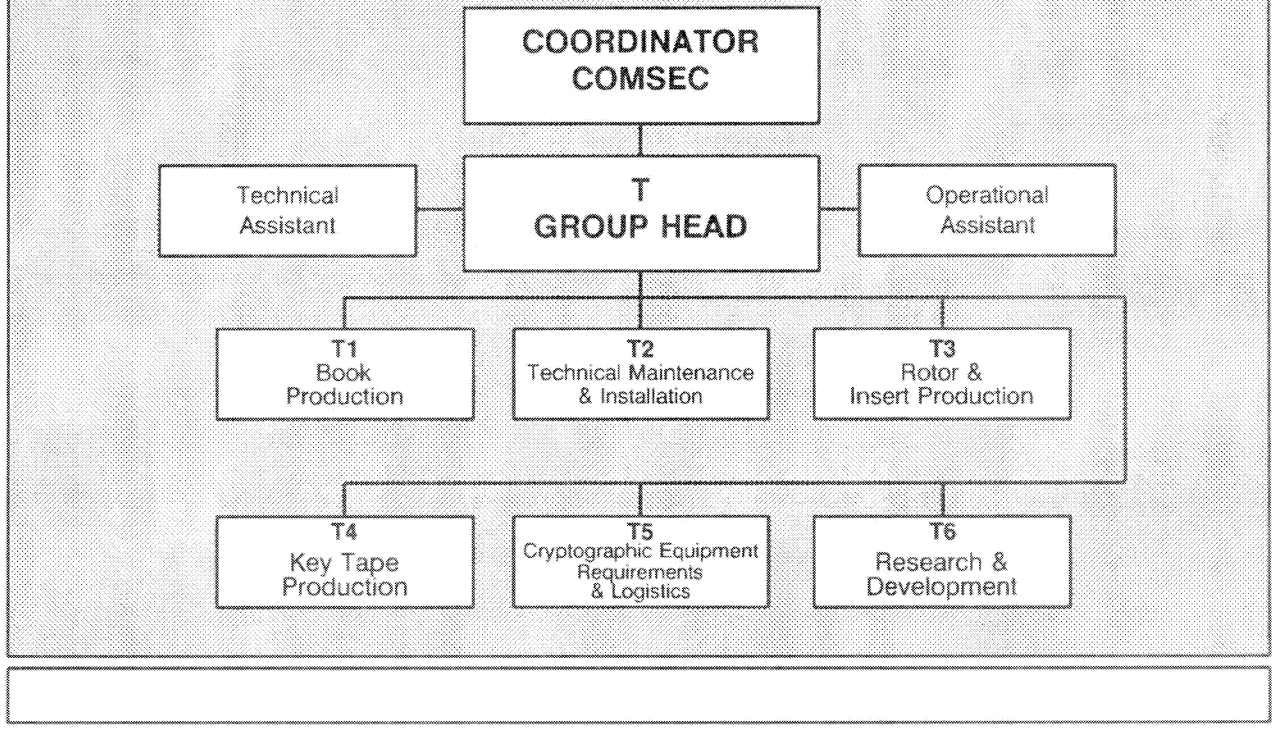
1957

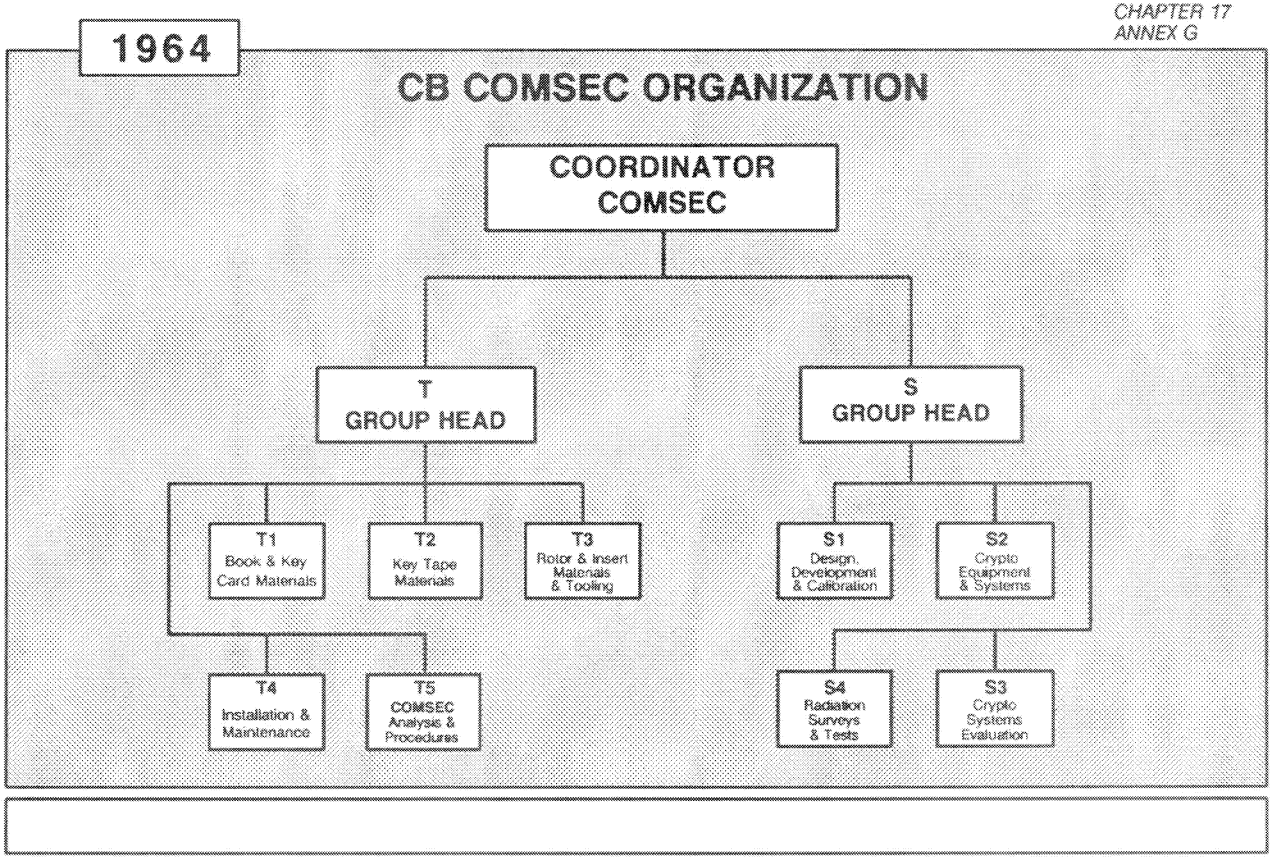
CB COMSEC ORGANIZATION



1959

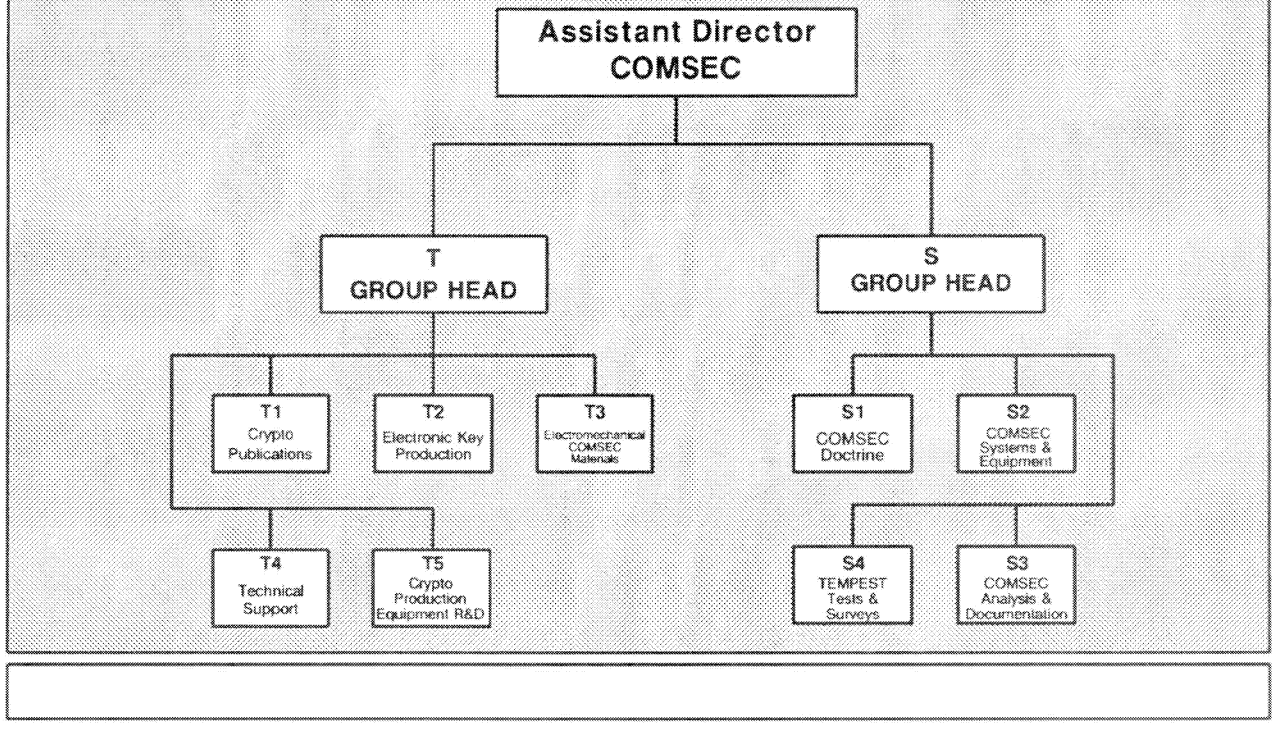
CB COMSEC ORGANIZATION





1972

CB COMSEC ORGANIZATION



Chapter 17/Annex J

February 1975

Responsibilities and Functions of the Communications Security Establishment (CSE)

COMSEC

(a) To advise federal departments and agencies on the planning, acquisition, installation and use of cryptographic equipment and secure communications-electronic systems;

(b) to review and evaluate the cryptographic principles incorporated or to be incorporated in any communications-electronic system used or proposed for use by federal departments or agencies;

(c) to evaluate as required commercially produced cryptographic equipment and assess the degree of security provided for specific areas of use;

(d) to produce cryptographic keying material, COMSEC devices and documentation to meet the requirements and priorities of users;

(e) to analyze on departmental request governmental communications and non-communications transmissions in order to determine the existing standard of COMSEC and to provide technical guidance and advice as appropriate;

(f) to carry out tests and surveys as required in the field of emission security, and to develop techniques to protect against compromising electromagnetic and acoustic emanations equipment and systems that may be used to process classified information;

(g) to coordinate and conduct research and development of techniques, equipment and systems to improve the effectiveness of national COMSEC;

(h) to formulate guidelines, and to review and evaluate the procedures involved in the installation, operation and maintenance of secure communications-electronic equipments and systems, and to conduct such training courses as may be required;

(i) to conduct liaison on COMSEC matters with collaborating agencies so as to effect the fullest possible exchange of technical information;

(j) to undertake such additional COMSEC responsibilities as may be delegated by the ICSI.

Chapter 17/Annex I

February 1975

ACCOUNTABILITY OF CHIEF, CSE FOR THE COMSEC PROGRAM

The Chief, CSE, is hereby designated Manager of the Canadian COMSEC Program. In this capacity, he is accountable to the Chairman of the Interdepartmental Committee on Security and Intelligence for the following substantive COMSEC matters:

a. with advice from the Communications-Electronic Security Committee, establishing COMSEC policies and plans for Security Advisory Committee review where appropriate; and their submission for consideration by ICSI or CCSI as appropriate;

b. planning and implementing effective, efficient and economical COMSEC activities to meet the COMSEC objectives;

c. conducting relations with foreign collaborating COMSEC agencies;

d. responding to COMSEC requirements as stated by Security Advisory Committee and its members;

e. preparation and coordination of COMSEC Program resource documentation, in accordance with ICSI and CCSI requirements and Treasury Board directives.

THIS DOCUMENT CONTAINS CODEWORD MATERIAL