CSE ATIP A-2015-00045

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

TOP SECRET
CANADIAN EYES ONLY

29

HISTORY OF CBNRC

VOLUME V

THIS DOCUMENT CONTAINS CODEWORD MATERIAL

TOP SECRET

WARNING

THIS DOCUMENT IS

CANADIAN EYES ONLY

IN ITS ENTIRETY

26

HISTORY
OF
CBNRC

VOLUME V

N.K. O'Neill

K.J. Hughes

AUGUST 1987

HISTORY OF CBNRC

VOLUME V

COMSEC TECHNIQUES & MATERIAL

Chapter 18

Provision of COMSEC Advice and Support

Chapter 18 - Provision of COMSEC Advice and Support

General

18.1 COMSEC is the protection resulting from the application of crypto security, transmission security and emission security measures to communications, and from the application of physical and personnel security measures to COMSEC information and material. Thus COMSEC intrudes upon the domain of authorities in five areas of security. Its purpose is to protect classified transmissions and emissions from unauthorized disclosure and exploitation. Because the measures and techniques of COMSEC are appropriate also to the protection of information treated by data processing equipment, COMSEC also finds its way into the field of computer security.

18.2 Although security protection in these areas was originally provided by various authorities, and in most cases by each department using its own resources, it became necessary to have experts in these areas as the authorities became more closely concerned with the protection of communications. World War II and the years that followed brought a tremendous explosion in the volume of communications and the attempts by foreign countries to exploit them. Unable to cope with the burgeoning problem of protecting communications, government agencies met together in committees to find an answer. Eventually the Director CBNRC was given responsibility in all these areas[1].

18.3 CBNRC provided COMSEC assistance to government departments in many ways; some of these will be discussed separately in specific Chapters, e.g. provision of keying material in Chapter 19; evaluation of codes and of crypto equipment in Chapter 21; ascertaining the level of security being maintained on communications links in Chapter 23; TEMPEST testing in Chapter 24; and COMSEC training in Chapter 28. There were many other ways in which CBNRC rendered

[1] See Annex 17.A

assistance. It is not intended that this Chapter should recount every service provided in addition to CB's major COMSEC roles discussed in the other Chapters, but an attempt will be made to give an indication of the variety of assists that came to be regarded as part of CBNRC's "back-up" role. Day-to-day advice and support on miscellaneous COMSEC matters were provided in accordance with the COMSEC mission of the Director, CBNRC. The duties and responsibilities of Test and Design (T&D), the original COMSEC section of CBNRC, as authorized in June 1948 are listed in Annex 17.A, and include (item vi): "To advise on all matters concerning communications security." Essentially the same responsibilities were reaffirmed in February 1975[2]. Thus it can be seen that not only in the formative years, but also on a continuing basis, CBNRC was charged with formulating policies, objectives and general procedures for the secure conduct of communications. CBNRC's terms of reference required the COMSEC staff to advise among other things on the types of ciphers to be used under varying circumstances and conditions. To do this, T&D, and later S Group, had first to acquire a specialized knowledge of cipher devices, both operational and technical, as soon as such information became available. In most cases one or more staff members were sent on maintenance training courses held at GCHQ and NSA, or at the plant in the UK or US where the crypto devices were being produced.

18.4 Prior to 1947 the Armed Services provided crypto support for themselves, External Affairs and the RCMP, and also for the CBNRC Communications Office. From that year onwards, T&D began to assume COMSEC responsibilities, first for CB, and then by gradually adding more and more communications/crypto/centres to its clientele, until it was recognized as the national COMSEC authority. Of course, other departments which had been engaged in communications before the existence of CBNRC resented this "upstart" organization presuming to set itself up as a source of expertise in the field of COMSEC. Nevertheless,

[2] See Annex 17.J

in time all came to realize that some one agency was needed which would devote all its time to the business of protecting sensitive communications from accidental or deliberate eavesdropping and exploitation, especially when it became obvious that unauthorized persons were indeed "listening". However, some resistance was frequently met from established departments, as in the case of the implementation of TEMPEST standards. Each department wanted to conduct radiation tests of its own facilities, but soon found that such a project was not feasible, that it was more economical and practical to have such surveys done by one agency because the detection equipment was very expensive and the expertise highly specialized.

Need for COMSEC Support

18.5 It is understandable that departmental authorities would be sensitive about having personnel from another agency inspecting their premises, finding fault with installations and procedures, and finally telling them how things should be done. This sensitivity is particularly noticeable in areas involving classified information. Security officials consider COMSEC to be just one aspect of security. Security protection is expensive and, since security is a departmental responsibility under the control of each Deputy Minister, it must compete with other requirements for funding. It was not till the late 1950s that funds were provided to encrypt much of the Armed Forces communications. Even HF radio circuits (e.g. the RCN link from Esquimalt to New Zealand) still carried unencrypted traffic in 1957. Moreover, there have been instances reported where the security classification has been removed from messages in order that the messages might be transmitted in the clear, and occasions in missions abroad where the security classification was put on correspondence after it was typed because the typist was a "local employee" without a security clearance. The attitude in some cases has not been "we need security protection but cannot afford it now" but rather "if that is what security protection costs, then our traffic is not really classified". With the former attitude precautions would be taken until the department could arrange the funding necessary for crypto protection; with the latter, the information would be regarded as unclassified and no precautions taken.

18.6 The first major COMSEC project was the provision of secure cryptomaterial, principally one-time pads[3], and advice on their proper use. Keying material was made not only for the Canadian Government, but also in due course for CANUKUS and NATO use (codes, authentication tables and key cards) and for the UK and New Zealand (key tape). There was evidence of a lack of understanding of the principles involved in the use of ciphers, and CBNRC was able to instruct Canadian users on the proper procedures and explain the risks of careless usage. Often the prime cause of security weakness is that personnel involved in communications do not fully appreciate the reasons behind security regulations and the importance of their strict observance, e.g. using a "one-time" key only once. As well, in the 1940s CBNRC frequently had to remind government users of Category B[4] ciphers that the texts of messages which were later declassified had to be reworded or paraphrased before publication, or else the cipher system would be in danger of compromise. Even today, people feel they are protecting information by whispering sensitive words during telephone conversations and have to be reminded that an interceptor need only turn up the volume when playing back the recorded version. These were some of the minor but important ways in which CB was able to advise communicators, especially those new to the field.

18.7 It frequently transpired that even some of the most experienced communicators were unaware of or overlooked a vital reason for a particular step or would consider inconsequential a detail that, in fact, was quite important. This sort of situation developed, no doubt, because of the "mystique" surrounding crypto operations - users were told the "how" but not always the "why" or the "why not". As a result,

[3] See para. 17.18
[4] See para. 20.7

communicators often circumvented or even deactivated a restraining device because they thought it was a shortcoming in the equipment when, in fact, it was a component deliberately incorporated to prevent a compromise of classified information. The failure to understand some of the basic principles of cipher security was evidenced when long-time users of cryptography proposed codes or ciphers they had invented, without realizing that their system contained fundamental security weaknesses. Experience indicates that, if an amateur code system is adequate from a security aspect, it will almost certainly be too cumbersome and slow from an operational viewpoint. On the other hand, if the code is simple enough to allow for easy use while communicating, security will likely be non-existent, or, at the very least, inadequate. In the latter case, the false sense of security provided by the use of the code is apt to result in misuse of the communications system and leakage of information of intelligence value.

Preaching the Gospel

18.8 For many reasons, therefore, a series of COMSEC lectures was inaugurated. Until 1963, Canadian communicators, mostly from the Armed Forces, were sent to England to participate in COMSEC courses conducted by GCHQ. Continuous pressure from LCdr. W.D. Moyes of the RCN, both in the Cipher Policy Committee (CPC) and directly to CBNRC, resulted in the inauguration of COMSEC courses at CB, initially for communicators of the Services, the RCMP and External Affairs, but eventually also for senior officials of any department who needed convincing that COMSEC was essential, especially those who controlled the purse strings that had to be loosened to make good COMSEC a reality. The T Group Section Head responsible for COMSEC Doctrine visited GCHQ, and after participating in the communications security analysis of a British Joint Services exercise and attending a GCHQ COMSEC course, returned to CB and established a similar training program in Canada. The first Canadian COMSEC Course was held in mid-September 1963. More than fifty such courses had been presented by the end of the period covered by this History. Special abbreviated COMSEC Courses were given, for example, to Regional Supervisors at the Royal Canadian Corps of Signals School, Barriefield, in November 1966, and training in COMSEC monitoring analysis procedures given to Supervisors of Navy monitoring teams from Halifax and Esquimalt in February 1967. Two weeks training in COMSEC techniques was given in December 1967 to officers from Mobile Command HQ and CFHQ. Special lectures were also given to representatives of commercial firms, e.g. to engineers of Computing Devices Company, who had a contract to build secure terminals for DND in 1968. Additionally, special courses were held at CB several times each year for personnel of other government departments and agencies, to provide training in the logic systems of current crypto devices, the secure installation and maintenance of equipment and TEMPEST measures for all information processing systems. Courses on equipment (e.g. KW-26) and general COMSEC matters were given to Halifax Maritime personnel, and COMSEC lectures were delivered at the Forces training establishment in Kingston. Courses on Emission Security were given to DND personnel.

Advice re Ciphers

18.9 By 1951 CBNRC was able to begin providing support in all aspects of cipher usage. At the request of the RCMP, a survey of the Force's cipher systems and crypto requirements was carried out and a report rendered, with an evaluation and advice for the future. The ciphers used between Ottawa, London and Washington gave high grade security. Within Canada, however, the RCMP had a long subtractor system using Bentley's Code (a one-part commercial code) with a "special RCMP appendix" (also a one-part code, i.e. significations and code groups in alphabetical and numerical sequence). It was assessed as "providing marginal security only" because of the indicator procedures followed and the non-random characteristics of the subtractor tables. Recommendations were made for improving the system. The COMSEC Doctrine Section also devised a scheme to minimize the risk of "spoofing" in CANUKUS authentication procedures. It was accepted and adopted by the

UK and US. One-time pads were provided in 1952 to Eldorado Mining and Refining Limited, a Crown Company.

18.10 In 1952 T Group undertook a major study aimed at providing secure communications for the National Meteorological Service, to be instituted in the event of a nation-wide emergency. Provision was to be made for possible intercommunication between any two of the 110 stations concerned. The use of General Area "OUT" pads or Area Reciphering Tables was considered impracticable in view of the geographical location of the stations. The Department of Transport (DOT) was extremely reluctant to use stencil systems such as they had had in World War II, and which they had found cumbersome and the cause of garbles and frequent delays. Fortunately fifty percent of the meteorological information transmitted was spot weather and not long-range forecasts (any forecasts transmitted would be for a limited area and limited time, and therefore would be of little advantage to an enemy). CBNRC made up cipher systems ranging from 2-way to 120-way one-time pads for DOT operational-type messages, with General Reciphering Tables for "Request-and-Reply" type messages. Here again, the financing of COMSEC requirements posed a problem. DOT feared that the Treasury Board would oppose the expenditure by DOT of funds for encryption of meteorological information, because they considered that to be a DND commitment. The Cipher Policy Committee, however, felt that the need for security of meteorological information in an emergency was a national concern.

18.11 The Services regularly reviewed their cipher systems, attempting to simplify their codes and authentication methods and to make them more efficient. These efforts occasionally resulted in the introduction of short cuts which CB would study and either approve or reject. Operational codes and authentication systems were developed by CB to provide short-term protection for perishable information in tactical situations; frequently field officers would seek to extend the cryptoperiod of these systems, and would have to be warned against such action. Assistance was also given to the Services and other government departments in planning for and acquiring crypto equipment. CBNRC prepared technical reports to indicate the advantages to be sought for, stressing factors such as operational reliability, stability of components and ease of maintenance - in short, all the desirable technical and operational aspects of equipments. Throughout the 1950s and 1960s, CB obtained from NSA every six months a status, availability and cost listing of all US crypto equipment. Summaries of UK cipher developments were also obtained as they became available. As the COMSEC Agency for Canada, CBNRC was the channel through which such information was provided, and all interested departments and agencies were kept informed either directly or through the COMSEC committees. In furtherance of this role, CB in 1963 began publication of CID/09/4, a "Technical Summary of Cryptographic Equipments Under Development or Currently Available for Use in Canada, United Kingdom, United States and NATO". Because of rapid advances in the crypto field this proved to be a tremendous undertaking. Frequent revisions were required - in November 1963, and in January and August 1965. The second edition was published in March 1966 and the third in April 1973. It was intended to provide basic details of crypto equipment for staff planning, but the equipment summaries were not designed for detailed engineering of communications systems. Before any Canadian orders for crypto equipment were placed, CBNRC would do an operational evaluation of the system. Copies of the device would be obtained, tested in the CB laboratories, and demonstrated to potential users. Field trials would be conducted by a Service or department, with CBNRC staff providing training and remaining on hand to render assistance. T Group would write up a consolidated trials report, including any recommended modifications to cater to proposed Canadian use of the equipment. CBNRC would then coordinate the Canadian orders for the equipment.

18.12 Frequently professional COMSEC support was sought in obtaining some required financing. In 1960 the Treasury Board withheld funds provided in RCMP estimates to replace TYPEX Mark 22 by NOREEN. To bolster the RCMP case, Bill Trowbridge, as Secretary of the Communications-Electronic Security Policy Committee (CSPC), wrote to the Force informing them that the Committee was of the view that there would be considerable risk to Canada's security if the RCMP were not permitted to upgrade their cipher equipment. The letter suggested that the RCMP request the Treasury Board to reconsider the matter. The difficulty in obtaining funding for security, especially COMSEC, was a recurring theme at committee meetings. The DND representative at a 1971 Communications-Electronic Security Group (CSG) Meeting claimed that security was often ignored until after the study on a project had been completed, by which time no funds were available for the incorporation of security measures. He said there appeared to be a widely-held belief that crypto security was unnecessary because communications equipment could be operated without it, and he added that loopholes in contracts and agreements were used to downgrade the importance of security. The Committee deplored the excessive demands often levied on government departments to justify costs where security was concerned; they acknowledged that such costs could not be ignored, but felt that all factors were not viewed in the proper perspective and in relation to the value of the information being protected. They noted that the "indoctrination" given officials attending the Senior Officers COMSEC courses had proved most fruitful, and agreed to do their utmost to have more senior officials enrolled in the course.

Installation

18.13 Installation practices formed a basic part of CBNRC's COMSEC support. This ranged from guidance on the physical security parameters for cipher offices (e.g. at the Canadian Joint Staff Building, London, in 1960) to the correct configuration of cipher systems. CB's expertise was sought, for instance, regarding mortice deadlocks in consultation, of course, with RCMP security experts. Also in cooperation with the RCMP, T Group in March 1955 revised UK specifications for a secure door lock for crypto centres. From time to time the RCMP physical security experts would request CB assistance; for example, in January 1962

T Group provided them with information on a "coded door control unit" so that they could furnish advice and support to other departments. S Group developed an electronic door lock control device for O Group. It will be apparent that the benefits to be derived from the use of good crypto can be nullified if the equipment is installed in a physically insecure environment or is operated by careless or untrustworthy persons. The safeguarding of crypto resources and the personal integrity of cipher operators are of paramount importance. The physical protection for COMSEC material must be more stringent than for other material because, like a list of combinations of locks on security vaults, it can be the key to much more than its own essence; loss of crypto keys can mean the loss of all classified information encrypted with those keys. Thus CBNRC was responsible for physical security as it applied to crypto centres and other areas that contained COMSEC material - including providing specifications regarding location, layout, access control, windows, doors, wiring and plumbing conduits, and secure perimeters. In July 1955, for instance, CBNRC submitted a proposed layout for destruction facilities intended for classified material at NDHQ. Assistance with crypto installations was therefore a major responsibility of CB COMSEC. In many instances the CBNRC technicians actually installed the equipment; they set up the External Affairs ROCKEX cipher office and trained the staff in the operation and maintenance of the equipment in the late 1940s; and in 1953 they assembled and adjusted 32 ROCKEX equipments for the RCAF. T Group technicians also installed power cables in floor raceways at Beaver Barracks for the RCAF in June 1961, and set up KW-26C and KW-37 equipment so that communications would be able to start up as soon as Service personnel were moved into their new quarters. A TEMPEST field survey which they conducted immediately afterwards ensured that the installation was secure. Similarly, T Group lent technical assistance to the RCN during shipboard installation and testing of crypto equipment. One CB technician joined the Fifth Canadian Escort Squadron in New York in November 1962, and remained aboard providing technical assistance with KW-7 trials until the squadron reached Halifax.

Special CB Capabilities

18.14 Frequently the need for CBNRC's assistance was due to the fact that some regulation and fault correction of crypto equipment demanded very fine adjustments which could be made only by special instruments and techniques possessed by CBNRC. For example, in June 1962 T Group conducted tests for the Army "to ascertain the effects of varying degrees of increased clutch tension on a ROCKEX V unit equipped with a ("TOOTHPICK") security modification to determine the frequency of lubrication necessary and the increased degree of maintenance required for units equipped with this modification". Other agencies would invite CB inspection of their crypto equipment after they themselves had modified them. CB technicians conducted distortion tests on British (Creed) teleprinter equipment for the Army, converted Teletype reperforators from low to high speed for the RCN, modified crypto (KW-26) equipment for the RCAF, assisted External Affairs and the RCMP with crypto on TELEX circuits and adapted various UK crypto devices (e.g. ALVIS and DOGATE) for use with error detection and correction (EDC) equipment. The S Group Calibration Laboratory was set up to cater to the need for "super fine" measurements. It developed state-of-the-art calibration facilities to verify measurements up to a few parts per million over extended periods of time. All measurements were directly traceable to the ohm, volt and nanofarad reference standards maintained for Canada at the Division of Applied Physics of the National Research Council.

Quick Reaction Facility (QRF)

18.15 As will be explained in Chapter 22, cipher devices are not always readily available when a need arises, as is the case with on-the-shelf items such as teleprinters, word processors or duplicating machines. A requirement for cipher machines, nevertheless, can occur suddenly and unexpectedly and often must be met without delay. For years CB had endeavoured to obtain authorization to establish a small "bank" of crypto equipments to be drawn upon by any department which, without warning, was faced with an urgent requirement. Financing was, of course, often an insurmountable obstacle. From its inception, T&D, and later S Group, had been pressed into service to meet such needs in any way possible. Equipment would be borrowed from other departments or from the UK, or most often from the US Services. When this was not possible, CB technicians would once again form a "Make Section" and devise a temporary solution. By cannibalizing, adapting and improvising, they were often able to provide a workable alternative, which would serve until a more suitable equipment could be acquired. The need was not always for a complete cipher equipment. More often a replacement part or a security modification would be required, sometimes even on one day's notice. The CBNRC Model Shop built up a reputation for being able to rise to almost any occasion.

18.16 Many requests, however, involved considerable expense, e.g. the fabrication of COMSEC devices, modification kits, authentication grilles and low level keyers. Each request was considered on its own merits, and prior approval of the Director obtained. The time arrived when it was considered necessary to formalize a procedure which had been followed for twenty years or more. The CSG Equipment Working Party proposed in 1971 that a Quick Reaction Facility (QRF) be established. As with other suggestions, this would imply a need for more personnel and therefore, although many projects were requested of "CBNRC's QRF" and promptly completed, no specific facility was brought into existence. The Director agreed that CBNRC COMSEC laboratories and workshop facilities, whenever possible and available, could be utilized to meet the COMSEC requirements of customers, provided any undue expense likely to arise in connection with the project was borne by the customer. All aspects of each request would be considered: the magnitude of the task, its impact on current CBNRC workloads, the financial implications, and contact with commercial firms if necessary. The CSG Members accepted these conditions, and whenever an urgent COMSEC requirement arose, whatever parts of S and T Groups could respond - usually T Group's Model Shop and circuit board wiring unit - would pool their facilities and provide the needed assistance. Any borrowed crypto equipment would be repaid as soon as equivalent items could be ordered and received - sometimes two, three or more years later.

18.17 Although never a specific facility per se, the QRF as envisaged and approved by the Director CB consisted of all facilities which could be made available to other government departments on short notice to provide unique and especially classified items. This service was used by the RCMP and External, but mainly by the military to provide special security modifications, printed circuit boards and electronic gadgetry. Laboratory facilities were installed at CB for the manufacture of printed circuit boards - for processing the art work and photo etching - for R, S and T Groups. The wiring of circuit boards was done by the rotor production unit for the whole COMSEC Community. T Group constructed two keyboard-operated numeric counting units for O Group in 1958, and a card-scrambling device for M Group in 1959. The T Group and S Group technicians were occupied much of their time in developing and constructing fittings, fixtures or other apparatus, either for CB or another government agency. They made equipment to produce keying material: for instance, T Group designed and built their own key tape generators and high speed checking equipment in the 1950s[5] and key card production systems in the early 1960s[6], and in 1974-75 T4 were developing a minicomputer approach to cryptoproduction using a key generator they had designed and constructed, a computer and a phototypesetter. In 1966 S Group made and installed a transistorized intercommunication system for the CB Security Office and a public address system for the Training Office.

TEMPEST

18.18 As will be recounted in Chapter 24, one of CBNRC's most important responsibilities to other

[5] See para. 19.27 and following

[6] See para. 19.35

departments was in the TEMPEST field. Not only did they provide advice on radiation of crypto and communications systems, conduct tests of equipment and surveys of installations, and prescribe remedies, but they also designed and constructed devices such as transmission line isolation units, low to high level signal converters, and screened enclosures for the suppression of unwanted emissions discovered at government offices in Canada and around the world (e.g. Service installations in Europe, and External Affairs missions in various national capitals). S Group designed and T Group built TEMPEST security enclosures for all and sundry: e.g. for an electronic formatting device being adopted by R Group; for detection devices used by the RCMP; and for electromagnets contained in teletype and crypto equipment used by all government communications offices. For security reasons these devices could not be manufactured commercially. In 1958 T Group fabricated a screened cage and shipped it to Resolute Bay to shield ROCKEX equipment.

18.19 Many other contrivances were invented and fabricated in S and T workshops to provide security features: e.g. the "springset device", a modification to ROCKEX to prevent decrypt key tape being used for encryption (which would make it possible for double employment of key, providing a depth of two and enabling a compromise); tape slitting devices and "7th-hole perforating devices" which would spoil encrypt key tapes as they were used so that they could not be used again; and special aids to speed up the setting of keys for various crypto machines such as ALVIS and KW-7. Secondary variables were also made up in T Group. In August 1967 S Group devised for sensitive RCMP locations an off-line tape preparation and "run-off" system with low TEMPEST characteristics. They also conducted reliability tests of multiple transmitter-distributors in low level circuits with various types and shapes of contacts in tungsten, gold and other metals. In 1968 they made security modifications to Teletype equipment at 704 Squadron, Rockcliffe, installed miniature teleprinter equipment in maritime patrol aircraft and "transportable radio communications stations", and added traffic flow security features to DND equipment.

COMSEC Tours

18.20 In addition to the TEMPEST surveys of communications/crypto installations recounted in Chapter 24, CBNRC officials also conducted tours of such centres to make general COMSEC inspections. Bill Trowbridge discovered COMSEC weaknesses in operations at RCAF bases at Marville, France, and Zweibrucken, Germany, during such an inspection in 1960[7]. In April 1967, a similar inspection was made of the "hardened" underground operational centre at Northern NORAD HQ, North Bay, to survey COMSEC facilities; in addition, exercise communications in and out of North Bay were monitored and analysed on several occasions, and COMSEC reports written. In one particular instance recommendations were made regarding public address procedures and telephone acoustic coupling, and changes were made to improve security.

Vulnerabilities

18.21 The need for protection of communications began to be better understood in the late 1950s. CBNRC was involved in studies of the vulnerability of most of the Government's classified transmissions and the threat from overt and covert snooping by other countries. Surveys were made of military and even industrial complexes whose communications and non-communications emissions could be exploited by unauthorized persons. Plants engaged in developing fuses, radar equipment or other devices whose emanations during testing could be detected were warned of the risk, because hostile parties could monitor these emissions and develop countermeasures.

Limited precautions could be taken, and CB was also involved in the warning arrangements.

[7] See para. 17.71

18.22

18.23 In March 1971 CBNRC received an urgent request to design a low cost enclosure to contain the emanations from an electronic translation system installed in the Government Conference Centre (the former Union Station) in Ottawa. CB was required to provide advice and direction on the construction of the enclosure during the rebuilding of the room and to test the shielding effectiveness of the completed installation. The entire project monopolized the time and talents of several technicians for a considerable time. CB personnel had also participated in the installation of screened rooms at other locations for crypto equipment and especially for computers.

Human Factor

18.24 Because "in the early days" few checks or safety features could be incorporated into the cipher systems, the human factor played a much greater role in the amount of security provided. True, the cryptographer was given a list of precautions to be taken "for security reasons" but, as mentioned earlier, the importance of these measures was not always fully appreciated. Moreover, in communications, time is also very significant, the communicator feels that his/her job is to get the message through, and realizes that COMSEC measures tend to delay the process. It is not surprising then that COMSEC was often regarded as a nuisance, and that precautions were sometimes accidentally or even deliberately overlooked. The omission of certain steps in the encryption process could lead to insecurity, and these occurrences had to be examined to assess the risk of compromise.

Evaluation of Violations

18.25 The responsibility for evaluating violations of transmission security and crypto security eventually fell to CBNRC. Although earlier the jurisdiction in these matters rested with the CPC and CSPC, it was CB that had to perform the task. The Comcentre or other office where the violation occurred would investigate and gather together all pertinent facts of the case, and after a preliminary study, often involving a board of inquiry, all the details were submitted to CBNRC. The latter would determine whether the incident constituted an actual breach of security, a possible breach, or merely a practice dangerous to security. Although CBNRC might comment on the seriousness of the violation and recommend remedial measures to preclude recurrence, the responsibility for disciplinary action, if any, would rest with the authorities in charge of the offender.

18.26 Loading limits had to be imposed on the use of keying elements such as rotors, and it was the responsibility of T&D to keep track of the total cipher groups used on all systems, as overloading could threaten the security provided. As cipher use increased, the crypto life of the rotors would be reduced.

Automatic Checks and Alarms

18.27 As crypto technology became more and more sophisticated, facilities were incorporated into cipher equipment to obviate the possibility of human error causing insecurity. While no device can probably ever be completely foolproof, many modern machines contain built-in checks and alarms, so that what amounts to a deliberate effort is necessary to cause the crypto equipment to compromise the clear text.

Consultation

18.28 S and T Group expertise was sought on any topic related to the security of communications. In June 1967, DND consulted CB concerning the value a potential enemy might derive from sonobuoy and LOFAR (low frequency analysis and recording) information transmitted by radio; and the possibility that countermeasures might be developed and applied in order to reduce or negate the value of the sonobuoy system.

Communications Systems

18.29 T Group was involved in the security evaluation of new communications systems, especially when there was a suggestion that they might provide an element of transmission security, e.g. difficulty in intercepting and D/F-ing, or resistance to jamming. DRB was conducting in 1961 a technical evaluation of meteor scatter systems, and later of some "noise and satellite systems". In 1967, CBNRC officers were deeply involved in discussions at the Defence Research Telecommunications Establishment (DRTE), Shirley Bay, regarding the "TOBACCO" and spread spectrum communications systems. S2 provided technical assistance, particularly with crypto protection, in the system-proving phase of TOBACCO. Discussions were also held with DRTE on wideband voice radio. S Group was asked in 1969 to evaluate a "secure system" of short range communications (K Band); their assessment was that it could serve only as a privacy system with good ELSEC features. There were many advocates of highly directional transmission systems (many considered microwave "secure"), and CBNRC had to demonstrate to "doubting Thomases" that such directional beams could be intercepted with a little effort.

18.30 With assistance from the National Research Council, CBNRC constructed an anechoic chamber in the Tilley Building in 1967-68. With all echoes and reverberations suppressed in this room, S Group was able to develop a secure telephone installation. The technicians also produced a secure TELEX installation for the RCMP Cipher Centre.

Appreciation

18.31 The unstinting efforts and unique abilities and dedication of many CB technicians were frequently recognized by recipients of such assistance: for example, in 1974, the Director General Communications Electronics Operations, DND, praised an S Group staff member (Bill Atwell) for his technical knowledge and ability, which solved certain problems in a timely fashion by working on a Sunday, "ten consecutive hours, under very unfavourable conditions" installing a new secure data link.

Bilingual Support

18.32 CBNRC published instructions in English and French for the use of one-time pads (later, bilingual operations codes were produced). CB also prepared regulations for the packaging and transporting of COMSEC material, for the routine disposal of superseded keying material, for the destruction of obsolete crypto equipment and for the emergency elimination of COMSEC material. Such regulations involved considerable detail; for example, instructions for the transmission of cryptomaterial and other crypto information specified detailed arrangements regarding authorized messengers, courier service, registered mail, registered air mail or security express packer.

Publications

18.33 T&D handled all the microfilm duties for CBNRC until 1958; and all the printing and duplicating work for the Branch until 1959, after which T Group was responsible for printing only COMSEC material and special jobs for which the Branch Printing Office was not equipped.

18.34 Technical writers were hired by S Group to prepare reports on all aspects of crypto equipment. During the Canadian production of ALVIS, CBNRC assisted the contractor (RCA Victor) in the writing of the manuals for this machine, known as the CID/610. Because of their unique expertise in the field, the CB technical staff had to write whole chapters providing COMSEC installation and operational configuration data and other criteria. The technical writing staff also wrote up TEMPEST reports from details provided by T3 personnel, enabling the latter to spend full time on radiation testing and site surveys. T Group also produced documents, e.g. "Specifications for the Preparation of Canadian Crypto Documents". And in May 1967 CBNRC began the publication of CTIBs ("COMSEC Technical Information Bulletins"), which summarized the latest details on new equipment, modifications, availability of new devices - in fact, any data that could be disseminated to the COMSEC Community. They were an immediate success. Each year they were bound in a spiral binder.

From MALLARD to SAMSON

18.35 Several senior officers of S Group, and to a lesser extent of T Group, were caught up in discussions associated with Project MALLARD[8], a scheme to develop a fully automatic, secure tactical communications system for voice, data, facsimile and telegraph circuits. The Canadian National Project Office for MALLARD was located in the Department of National Defence, and S Group provided COMSEC advice and assistance as required. Three or four officers from CBNRC, including S Group Head and one or more Section Heads, would meet with representatives of the American-British-Canadian-Australian (ABCA - Quadripartite) Armies and other COMSEC agencies in London, Washington, Fort Monmouth, N.J., or Ottawa for discussions. When the MALLARD project collapsed in 1971 it was quickly replaced by TRI-TAC (US) and SAMSON (Canadian)[9], and CBNRC participation continued.

[8] See para. 17.95 and following

[9] See para. 17.99 and following

Support to Service Communications

18.36 CBNRC's technical expertise was frequently consulted when problems with communications systems arose. The RCN approached T Group in February 1962 for assistance "in checking on and cleaning up technical characteristics of transmissions from HF radio equipment installed on ships". Through radio fingerprinting (RFP), a process in which the transmissions (as displayed on an oscilloscope) are photographed, individual distinguishing transmitter characteristics can be analysed and recorded. The analysis and classification of such "signatures" enables hostile DF stations to locate and identify the transmitter and hence the ship in which it is installed. The individual identifying characteristics can be completely or partly suppressed through careful regular maintenance of the transmitters. Varying the transmitter in use on successive occasions is another COMSEC expedient resorted to in an effort to avoid identification. CBNRC was also regularly involved in discussions concerning other communications matters, involving facilities or personnel. Staff members met with several representatives of the Canadian National - Canadian Pacific Military Communications Consultant Study Group in December 1966 to brief them on the application of COMSEC principles and equipment to wideband multi-channel communication circuits.

Just as important, but seemingly less pertinent, were discussions between 1967 and 1969 concerning security considerations involved in collective bargaining for COMSEC personnel.

18.37

s.15(1) - DEF

s.15(1) - IA

Crypto Equipment Testing

18.38 Frequent failure of the relay contacts in KW-26 and CID/610 equipments resulted in a request to S Group from R Group in November 1967 for an improved method of line-keying from crypto equipments using keying relays in their output. To meet this requirement, tests were undertaken to determine the contact life of various relays in diverse configurations. S Group explored several methods of keying the output line with solid state devices - e.g. a light-coupled system using a solid state light source, and a transformer isolated system using a silicone-controlled rectifier. These complicated systems were discarded in favour of a simpler method which limited the amount of current carried by the relay contacts, by having a transistor, rather than the relay contacts, act as the line-switching device. Ten of the transistorized keyers were fabricated by T Group for use by R Group with the KW-26, and two more for tests planned by DND. A redesigned electronic keyer was developed for use with the CID/610.

s.15(1) - DEF

s.15(1) - IA

18.39 CBNRC's checking of equipment installations to correct TEMPEST problems often turned up local innovations which introduced security hazards. During site surveys in 1963 it was discovered that some holders of KW-26 crypto equipment were using the device as a message reproduction system on occasion. Tests showed that when the transmitter-distributor and teleprinter were used for this purpose through the KW-26 with its switch in the "Stop Change Card" position, plain text signals leaked through to line despite the use of low level keying. The signal was also present during normal operation but was masked by the cipher signal. Although a modification to remedy the condition was made available, instructions were issued prohibiting the use of on-line equipment for preparing, checking or editing message tapes and for tape or page copy duplication.

External Advice

18.40

s.15(1) - DEF

s.15(1) - IA

Computer Security

18.41 The CSPC noted in September 1966 "the ever-increasing use of computers to process classified information" and considered the security implications. The members expressed the view that the problem was primarily one of physical security, namely, that of controlling access to the equipment and the associated input and output components, and of ensuring that persons having such access possessed the requisite security clearances. They acknowledged, however, that computers were subject to the hazards of electromagnetic radiation and, therefore, TEMPEST measures had to be invoked. CBNRC then entered the picture. As in the US, conflict developed between computer authorities, physical security authorities and COMSEC authorities over the boundaries of their respective jurisdictions. This involved the Department of Supply and Services (DSS), the RCMP and CBNRC. The Industrial Security Branch of DSS issued a manual purporting to set out interim policy on the security of data processing systems. Some statements in the Manual were in conflict with COMSEC policy and procedures. Meetings were held with DND, RCMP, DOC and DSS. Responsibility for Computer Security was not delegated to one particular agency, but each department, as with security in general, felt responsible for its own security in the matter. They floundered about without guidance, seeking advice from whomever they considered to be authoritative on the various aspects of the subject. The Treasury Board then stepped in and caused some fifteen working groups to be formed, each to study one aspect of Computer Security, and to write a chapter for a document that came to be known as the Treasury Board's Guide on EDP (Electronic Data Processing) Administration. S Group sent representatives to the COMSEC Panel, as did External, DND, RCMP, DSS, DOT, DOC and Department of Justice. Chapter X was devoted to the COMSEC aspects of EDP administration and was written principally by CBNRC, with input and comments from other members of the COMSEC Community.

18.42 In January 1974 the Security Advisory Committee (SAC) authorized the setting up of an Interdepartmental Computer Security Panel (ICSP), which was made responsible for reviewing and advising on the activities of the Security Evaluation and Inspection Team (SEIT). The SEIT, in turn, was responsible for the regular inspection of EDP facilities processing classified information. The ICSP members were to be of Director General level and were to provide advice to those concerned with implementing the security aspects of the Federal Government's EDP plans and operations. The SEIT was made up of technical experts and relied heavily on CBNRC's TEMPEST personnel. The ICSP was still in the process of organizing and the SEIT was busy with inspections as the period covered by this History drew to a close.

18.43 Discussions were held on 10 April 1974, involving representatives of CBNRC and the RCMP/EDP Branch, concerning protection requirements for the EDP communications of the the Department of Justice (DOJ). As a result of these discussions, CBNRC assumed the responsibility for carrying out a systems analysis of DOJ requirements. Further discussions, involving RCMP and CBNRC representatives and a member of the DOJ Jurimetrics Division, followed. After a TEMPEST Field Survey at the DOJ terminal location in the West Memorial Building on Wellington Street, an in-depth study was made of their IBM 3705 Computer Communications System.

18.44 A paper study of the communications security of the Statistics Canada Labour Force Survey Project was performed in April/May, 1974. A letter presenting CBNRC's analysis of the COMSEC facets of the project was sent to the Departmental Security Office of Statistics Canada, who issued a final report thereon. The CBNRC conclusion was that with the application of the security measures outlined in the report, a good level of protection against inadvertent disclosure and unsophisticated attack could be maintained, even though the system did not meet the requirements for full CONFIDENTIAL approval. In view of the low level of assumed threat it was considered that such measures would provide all the security judged necessary by Statistics Canada. In May 1974, at the request of the Department of Supply and Services, S Group provided specialist COMSEC advice on the protective measures necessary in positioning a new IBM computer being installed at the Government Printing Bureau to process classified data. After a thorough investigation, it was determined that the computer should be housed in a shielded room and all accesses treated for TEMPEST.

Other Outside COMSEC Support

18.45 The contributions by CB technicians to the smooth operation of other government agency crypto centres seem endless. They installed and maintained secure telephone links (KY-3) between DND and Washington and between NDHQ and External Affairs for NATO conferences and established a similar secure link (KY-3) between RCMP HQ and CBNRC. Also for the RCMP they evaluated and conducted tests of various relays, filters, line isolation units, shielded cables, distribution boxes and bulk magnetic tape erasers, and did a qualitative appreciation of the Datacoder key generator; they established the degree of susceptibility of an RCMP television camera to radio frequency signals across the spectrum; and they tested a Motorola two-way mobile radio system. They developed a secure closed circuit television system for operation between the National Defence Command Centre and the Directorate of Intelligence in the new NDHQ building; they produced a long range communications terminal - a mobile facility for the Canadian Forces; and by cannibalizing, they obtained 15 serviceable KG-3 equipments from 16 units "inherited" from NSA, gave ten to DND, and retained five against future needs of other departments. They made a thousand line-interface relay modules for DND ALVIS equipments. They manufactured and installed special units in telephone subsets for the Privy Council Office (PCO) secure telephone system; developed a secure facsimile system for use between the PCO Data Retrieval Centre in the Langevin Building and the East Block (using two DACOM 412 devices and two KG-30 equipments); and provided remote input facilities for a secure multiplexed teleprinter system to be used

s.15(1) - DEF

s.15(1) - IA

with the PCO computer. They investigated the feasibility of interfacing certain commercial modems with tactical ciphony equipment (KY-38) to provide secure voice communications over long haul military or commercial conditioned lines as well as over voice frequency circuits; and evaluated a terminal being developed by Computing Devices Limited for the SAMSON system. When asked in 1974 to investigate the feasibility of using available or future crypto equipment to secure information processed on the DND Interim Communications Network/Management Information System, S Group developed a means of using a multiplex system with KG-34 crypto. They ran trials of the Speakerphone to determine its susceptibility, when equipped with special cut-off relays, to airborne or structure-borne acoustic pick-up in the "on-hook" condition. They designed disconnect devices for various types of telephone, and universal filters for teleprinter equipment contact box assemblies, to interface with low level systems. They developed the Maritime Inshore COMSEC System - a speech privacy system for the Department of the Environment and the Ministry of Fisheries. They provided advice to the Canadian Standards Board on the TEMPEST implications of multiple translation systems involving electronic components. They launched an investigation into the deterioration of information stored on magnetic tape subjected to magnetic fields. Because fluctuation in the power drawn via the mains by a crypto device reveals intelligence, External Affairs needed an alternative power supply to be able to use NOREEN equipment in their missions behind the Iron Curtain. S Group developed a means of operating the device from a battery power supply composed of non-rechargeable cells, and determined the life-span of such a power supply under normal operating conditions.

Some Inside Assists

18.46 While providing such comprehensive support to other government agencies, CBNRC COMSEC staff also found time to help out within the Branch. They installed a two-station "intercom" system in the M Group production area, developed an inexpensive, miniature version door-opening device for physical security applications, designed an improved Commissionaire's reception desk with special communications facilities, and assisted R Group with the installation of a secure duplex teleprinter circuit to External Affairs.

s.15(1) - DEF

s.15(1) - IA

Chapter 19

Production of Keying Material

Chapter 19 - Production of Keying Material

The Task - Getting Started

19.1 The security of any well-designed crypto-system is totally dependent on scrupulously controlled production and conscientious and efficient use of the keying material. Production of key is a highly specialized area which approaches the state-of-the-art limits in random number generation, statistical analysis and quality control. All Canadian keying material is now produced and controlled by the National COMSEC Agency, CSE. This was not always the case: prior to 1947 the keying material requirements of the Canadian Government were furnished free of charge by the UK, in accordance with the British policy of supplying all Commonwealth countries with secure cipher systems, keys and settings[1]. Under pressure from UK authorities who wished to unburden themselves of the responsibility and cost, and at the urging of Canadian officials worried about the security of national information of a sensitive nature, the Communications Research Committee (CRC) commissioned CBNRC to establish a cipher materials production element, initially called the "Make Section". The name was changed to the "Test and Design (T&D) Section" in March 1948.

19.2 The task of setting up the crypto key production facility in CBNRC was begun in 1947 with an initial establishment of 39 positions. Later that year, 48 additional positions were authorized to cope with COMSEC tasks. The first order of business was the selection of technical and operating personnel, quickly followed by the planning of systems and the design and construction of keying material production equipment. At the 20th Meeting of the CRC on 7 August 1947 the Director CBNRC pointed out that office accommodation in the LaSalle Academy building was inadequate for CB staff, particularly with reference to the "Make Section", for which it was impossible to provide separate quarters as required

[1] See para. 15.7

by security regulations; further expansion of production facilities had, therefore, to be postponed until additional space could be made available. Nevertheless, One-Time-Pad (OTP) production was slowly getting under way during the fall of 1947. In preparation, modifications had to be made to IBM equipment. A card sorter was converted to a card scrambler and, in October, the Section commenced building a random card file. This file was destined to be the basic source of random material for several numerical codes for many years. A check was made on the random characteristics of the file, and the results were sent to the UK for study and comment. The Director CBNRC informed the London SIGINT Centre (LSIC) on 23 September 1947 that CB would soon be able to meet most of the requirements of Canadian users.

Printed Key Produced from Punched Cards

19.3 Printed or typed key is normally required in groups of four or five letters or digits conveniently spaced, usually within a small number of lines on each page. Random characters for producing manuscript material (for one-time pads, key lists, authentication systems, machine settings, etc.) were at first generated by hand methods because equipment was not available. Duplicators and stitching machines were on order. Some production devices were manufactured and others were ordered from the UK.

19.4 As equipment could be acquired and more space became available, manual operations gave way to automation. Using rotor-operated Scramblers, T&D would shuffle 120,000 alphabetic and numeric IBM cards (each of which contained random letters or digits punched in a certain number of columns). During the preparation of these cards, careful checks were required to ensure that the letters or digits punched occurred with random probability. Key was produced by extracting from the master file a small sample of cards and printing some (but not all) of its columns in a random order which was changed frequently. A complete line of key was printed with whatever spacing was required.

The first editions of Canadian-made one-time pads were delivered to the RCN in January 1948.

19.5 By the end of July 1948, the random numerical card file contained over 350,000 cards; another 100,000 were required to bring it up to "full strength", but space was limited and floor loading had to be considered in the premises, which had originally been designed for school purposes (LaSalle Academy). Accommodation in the IBM room allowed T&D to add only 3,000 more cards to the file. Two scrambles were performed per week. Preliminary work in connection with the preparation of a random alphabetical card file got under way in August 1949. The production quota of manually produced one-time pads and long subtractor tables for the year 1949 was roughly 600 editions. Because of space limitations, equipment for the automatic production of one-time pads could not be developed. Within a year of the move to Rideau Annex, however, the equipment had been designed and built and put into operation. A few months later, T&D were able to alleviate the overtaxed UK facilities by producing several series of two-way and three-way one-time pads for British Government use. Hundreds of thousands of one-time pads were produced in the 1950s and 1960s; in the mid-1980s OTPs/OTLPs were still being produced, but the total annual requirement had dropped to less than one hundred.

Key Tape

19.6 At the same time, plans were under way for the production of key tape as soon as sufficient space was available. At a special meeting on 23 September 1947, the CRC made provision for payment of $23,500 for equipment to be purchased that year for the generation of cipher key tapes. Equipment for four ROCKEX key tape generating stations was ordered from the UK and scheduled for delivery in February 1948, though the equipment itself was never in fact delivered. Consideration was given to having such equipment manufactured in Canada either by the National Research Council under the guidance of CB specialists, or by Bayly Engineering of Oshawa. (Col. B. de F. Bayly had participated in the development of the ROCKEX machine during WW II.) In the event, however, it was T&D itself that built the tape production equipment. While awaiting the delivery of drawings and materials from the UK in November 1947, the technical staff worked on design and preliminary construction of one-time tape generators. Commercial tape punches and tape readers were modified and automatic checking equipment was constructed. Workshop space was at a premium and only two generating stations could be built at a time. The first two were completed and producing tape by May 1948. A third station was built and in operation by July, despite a shortage of operating and technical staff. When the fourth station was completed in October, there was no space to set it up in the production area. Under pressure to get production under way and handicapped by lack of space, the technicians cast about for a vacant spot and found one: the Director was away on an official visit and in his absence the fourth generating station was set up in his office, enabling one-time tape production to reach 65,000 groups daily. By the time greater efficiencies were introduced into the equipment by redesign of some parts and resurrection of others from the scrap heap, production was pushed to 72,000 groups per day in February 1949.

19.7 The first bulk shipment of Canadian-made one-time key tape was delivered in September 1948 (88 editions of 2-way ROCKEX tape) to the Department of External Affairs. This occurred following extensive evaluation of the random qualities of the key tape at CBNRC, and an assessment of the results by GCHQ. Reports from the UK on samples sent there for testing assured CB of the perfect quality of Canadian production. Within months (by February 1949), shipments of ROCKEX tape were made to the US Army Security Agency (ASA) and to the GCHQ Senior Liaison Officer (SLO), Washington, as well as to the intercept stations at Coverdale and Whitehorse. In May 1949, key tape was shipped to Victoria Wireless Station. By the end of the year, six tape generation stations had been built; two of them had been set up in November at the Rideau Annex, and were producing tape even before the majority of CB staff had moved to the building. In January 1950, two more generators were operating and preparations were under way for eight additional generators. With ten positions producing in March, the shortage of technical and operating staff was acute and overtime was initiated. By the time all 16 generators were constructed and in operation in July (no more were planned), 2-way, 3-way and 6-way tape was being produced.

19.8 The beginning of the 1950s brought the PYTHON cipher systems - five-level tape-operated on-line crypto equipment, e.g. 5UCO, SIGTOT and ETCRRM machines. As the last two ROCKEX key tape generators were installed in June 1950, T Group began preparing for five-unit tape production. Fortunately this time, however, CB did not have to build its own production equipment. Key tape generators known as "DONALD DUCK equipment" - 45 of them - were acquired from the UK. As the production capability grew, key tape was supplied for the GCHQ-CBNRC 5UCO circuits and even for NSA's 5UCO circuits, as well as for use with SIGTOT by the RCN and RCAF, and with ETCRRM by the RCAF. Later, when CBNRC circuits to the intercept stations were converted to 5UCO, five-unit key tape shipments reached 6,500 reels per month. For security (tamper resistance) reasons, and for protection from the elements, the reels of tape were sealed in plastic. A high frequency welder was acquired for sealing the plastic envelopes.

TYPEX Keying Material

19.9 As with other forms of COMSEC material, TYPEX key settings and inserts were originally provided free of charge to Canada by the UK. This entailed a huge expense, especially in the provision of inserts. Production of settings was less complicated and less costly, and therefore Canada accepted this responsibility first. The Department of External Affairs Cipher Office were making their own TYPEX pin tire/insert settings in January 1948 for communication with missions in London, Paris and Berlin. When Bill Trowbridge examined their "hand" methods (29 January 1948), he discerned serious mechanical errors resulting in extremely dangerous limitations in the settings. He devised more secure methods which, although they too involved manual functions, were considered to provide the necessary protection, given the general weaknesses of TYPEX Mark II. Within two months, CBNRC was able to deliver a year's supply of settings to External Affairs. By July, TYPEX settings were ready for the RCAF.

19.10 The manual methods of preparing TYPEX settings at the start were time-consuming processes. The first stage was by drawing letters randomly "out of a hat"; discs, each bearing one of the variable letters of the alphabet, were "hatted" (scrambled in a container) and five withdrawn, one at a time, for one day's setting. These letters would be used to set up the inserts and drums in a TYPEX machine. With another similarly prepared random setting, "bits and pieces" from various sections of a text, other than from a newspaper, would be enciphered on the TYPEX machine. The groups resulting would then be chosen in random order for key settings which were printed on cards for distribution to TYPEX users. The quality of the settings so produced was good, but the process was slow and cumbersome and had certain

s.15(1) - DEF

other disadvantages. It was difficult to scramble counters (lettered or numbered cards) by hand, as there was a tendency for two or more counters to cling together and thus often appear together in the settings.

Thus there were reasons other than expedience for wanting to introduce automation into key production methods.

19.11 Some settings had been made by the Canadian Bank Note Company for the Canadian Army, with the aid of instructions received from the British War Office. A limited number of cards would be scrambled by IBM methods. This resulted in the fairly frequent repetition of groups. And so CBNRC assumed responsibility for producing all TYPEX key settings, using IBM methods and a large number of cards; with random plugging and the mechanical scrambler, a more nearly random shuffle was achieved. This, of course, also accelerated production, enabling a greater output to keep pace with the growing demand for keying material.

TYPEX Inserts

19.12 The production of TYPEX inserts, however, posed more serious problems. The Canadian Navy and Air Force used the same series of inserts as the Admiralty and Air Ministry respectively, while the Army was supplied with a separate series, common to both Australia and Canada, by the War Office. The Department of External Affairs held a separate series supplied by the Commonwealth Relations Office. The general policy during World War II had been to permit each series of inserts to remain in force for an extended period of time. This effected a considerable economy, and made it possible for the UK to meet the Canadian commitment without undue strain on their production facilities. Post-war research into the security aspects, both cryptographic and physical, of long term use of cryptomaterial prompted a policy change requiring replacement of inserts every two years. The resultant accelerated production schedules burdened UK facilities to the limit of their capabilities, and forced authorities to conclude that it would be necessary to charge Canadian users for each new series of inserts. For this reason, and also with the intention of effecting a substantial measure of dispersal which would provide a safeguard against production capacity being destroyed in wartime or disaster, UK authorities requested in December 1948 that Canada (and Australia) undertake to produce their own insert requirements.

19.13 Realizing too that the circumstances of peacetime use of cipher differ somewhat from wartime conditions, in that the majority of traffic would be for internal distribution only, the CRC, at its 42nd Meeting on 15 August 1949, requested Mr. Drake to prepare a projection of costs, including personnel required, to launch TYPEX insert production. It would be a complex and costly process to inaugurate. In CRC/109 dated 2 September 1949, Mr. Drake reported that the project would require an initial capital cost outlay of $44,350, with annual recurring costs of $44,375, including salaries for a staff of eleven persons, four skilled and seven unskilled. Mr. Drake made a case for installing a small specialized workshop within the confines of CBNRC - in preference to the security risks involved with commercial production, or to foisting the responsibility on NRC or the Defence Services, all of whom had expressed reluctance to take on the operation. He suggested that "if inserts were to be produced by CB, part of the cost might be covered by selling some of the product to the UK or even by requesting the Services and External Affairs to pay". Although this idea of cost recovery was mooted from time to time, it was never put into effect, partly because of security considerations, and partly to avoid complex administration.

19.14 At the 48th CRC Meeting on 22 December 1949 members expressed doubt about whether insert production would be a good long range project in view of impending changes in cipher methods. The 50th CRC Meeting on 2 March 1950 noted that "GCHQ stated TYPEX still had at least five years' life" and "any succeeding system would probably also use drum scramblers, which would make use of the same workshops" as had been used for producing inserts. (This proved to be prophetic, as the shops produced wired variable scramblers until 1980.) In CRC/109, dated 2 September 1949, Mr. Drake had recommended to the Chairman CRC that the CBNRC establishment be increased by 11 persons to enable the manufacture of TYPEX inserts. It was to be more than another year, however, before approval would be given to proceed with production. Many alternatives were considered. At the time, the RCN produced inserts for the CCM machine on a limited scale, but it was decided "that the RCN plant could not be expanded sufficiently to take care of all Canadian requirements"[2]. The CRC agreed that it was impossible "to request from the UK inserts to meet a large increase in Canadian requirements". Even the possibility of turning to the US was explored (to produce crypto variables for a British cipher machine!!). The CRC noted that the "US may have to begin producing inserts for NATO TYPEX communications, but members were agreed that for reasons both of security and assured supply, it was inadvisable to contract with an external source for supplies of this nature". Finally, at the CRC 63rd Meeting on 10 November 1950 the Chairman reported that the Senior Committee had given its approval for the production of TYPEX inserts.

19.15 Approval did not come a moment too soon, as the shortage of inserts in Canada was threatening to become acute. Personnel were hired, but were unable to proceed until the delivery of production equipment, which had to be imported from England. Such equipment is special-to-type and CB, of course, had not yet progressed to the point where it was

[2] See CRC/M/60, dated 7 Sep 1950

capable of constructing its own. Thus inserts for Canadian use continued to be manufactured in the UK by the Air Ministry under the control of the British Cypher Security Committee until well into 1952.

19.16 TYPEX insert wiring diagrams were prepared by T&D at the beginning of November 1951 and, six weeks later, Bill Trowbridge was able to inform the Director GCHQ, "We have completed and delivered to the Canadian Army our first series of TYPEX inserts". More were to be delivered in March 1952, and from that time CB began gradually to assume responsibility for the full national requirement of TYPEX keying materials. During the next twenty years, more than 50,000 inserts were produced, as well as tens of thousands of wiring patterns and machine settings. Production gradually tapered off as more sophisticated crypto equipment was introduced. Although the TSEC/KL-7 device was brought into use on 1 July 1956, the TYPEX continued to be employed, mainly as a back-up system, until 1969. The destruction of all TYPEX production equipment and material was eventually authorized at the end of May 1973[3].

Coming of Age

19.17 By October 1951, there were 54 persons engaged full-time in the production of COMSEC materials, and another 12 applicants were being processed for employment. The requirements of the three Services and the Department of External Affairs for one-time pads (letter and figure types), reciphering tables, rotor arrangements, daily machine settings, simplex TYPEX settings, authentication tables and all other material reproduced by "Ditto" and "Multilith" processes, were being met in full. In addition, all Canadian ROCKEX key tape (six-unit) requirements were being filled by T&D production. The manufacture of TYPEX inserts had begun, and CBNRC would meet the full Canadian requirement within a

[3] See T-437-3-1, dated 31 May 1973

year; all settings and rotor arrangements had been provided by T&D to Canadian users of TYPEX for over three years. Additionally, the Cipher Production Section had begun producing settings for CCM machines, and NATO TYPEX settings.

19.18 Compilation of random manuscripts for various series of basic books, message settings, indicator indices, single-subtractor frame tables and other material requiring reproduction by letter press and/or photolithographic processes was under way. Reproduction of such material could not yet be undertaken, however, until a classified printing unit could be established. The Director CBNRC, in a letter to the Military Services dated 30 November 1949 said: "Canadian Basic Code Books, Field Codes, S.S. Frame Tables and other cipher and security material ... cannot be produced in Canada at present due to the lack of secure printing and binding facilities." A request from GCHQ that same year for Canadian assistance in the production of "book ciphers for British use" sparked CRC discussion of the propriety of having classified material printed by the King's (later Queen's) Printer. At the time the latter's facilities could not provide the necessary security protection, and CBNRC had neither the space nor the large press type equipment required. The Canadian Bank Note Company was printing some departments' classified material, but it was felt that the time had come for a government-owned classified printing unit, especially for highly sensitive cryptomaterials. The struggle to set up a security printing plant is chronicled in Chapter 17. It was not until the fall of 1954 that the Queen's Printer's facilities were approved for the printing of COMSEC material. The main problem with having a classified printing unit operating as a special part of a large plant whose work, for the most part, is unclassified, is the difficulty of control - control from above by those not involved in the classified operations, and control within the classified area to prevent access by unauthorized persons. When there was insufficient printing to keep all the employees and equipment busy in the

s.13(1)(a)

s.15(1) - DEF

s.15(1) - IA

classified unit, efficiency and economy dictated that the resources be used for surplus unclassified tasks. Representatives of agencies, for whom these tasks were being performed, felt a need to inspect the work at various stages during the printing and, of course, this caused difficulties. The problem became even more acute when a new building was constructed in Hull for the Printing Bureau and the personnel of the classified and unclassified areas were regularly in direct contact. There was constant conflict and many "incidents". Both the COMSEC Community and the Printing Production staff found the rigorous requirements of maintaining a small highly classified printing section within a large unclassified printing establishment too difficult to cope with, and eventually T Group would have to take over the printing of all COMSEC materials. In the interim, T Group acquired small scale printing equipment and printed highly sensitive jobs such as keying material, and those requiring great precision and accuracy, while those that had to be done on large presses were done by the Queen's Printer.

19.19

19.20 CPC Paper No. 14 (CSB/41) dated 25 January 1955 noted: "The Test and Design Group of CBNRC at present employs 78 persons on cipher production and it is expected that this number will be increased to 85 during 1955. In addition, a special Security Printing Plant, the Nicholas Street Unit of the Queen's Printer, has been established for the purpose of printing classified material including those crypto publications which must be printed by "letter-press" or "photo-offset" process. This plant operates under the strict security control of the Cipher Policy Committee .... The total estimated cost for the production of crypto keying material to meet the estimated requirements of Canadian cipher users for the fiscal year 1955-56 is $492,000."

19.21 It was still necessary for the Canadian Government to continue to rely on the UK and the US for the supply of crypto devices. To be sure, there arose from time to time the suggestion, even the demand, that Canada produce her own cipher machines. The subject was discussed thoroughly on many occasions, and modest production programs undertaken as recounted in Chapter 22. Security can be obtained, however, without building one's own equipment. The integrity of the encryption is in the keying material; hence encipherment with a high-grade crypto device cannot be read, even by the designers/manufacturers of the device, if they do not have access to the keying material. By the end of 1951, all associated settings and keys used with cipher machines (developed in the UK or US) were Canadian-produced, with the exception of 5UCO key tapes (five unit). Apart from cipher machines, the objective was to meet in full by early 1953 all Canadian cipher requirements.

19.22 If conditions remain static, production should be a routine process. The demand for keying material, however, has never been constant for very long. Events on the national or international scene have usually caused requirements to fluctuate, often radically, because in times of crisis communications sky-rocketed unexpectedly. In addition, a compromise of keying material would result in a frantic request for replacement on short notice. Also, of course, the introduction of a new cryptosystem always required the initiation of a series of projects: developing the criteria, specifications and parameters appropriate to the keying material; designing and building the equipment to produce, check and verify the key; and often to acquire or develop equipment for tamper-resistant packaging of new material. All this took time and money. In some cases, details or even whole production equipments could be obtained from the US or UK, but most often CB production staff had to develop their own devices because of the difference in magnitude of the production effort involved. Since the crypto equipment for which the key was intended had been designed and built by the UK or US, they had also developed the key production devices first. There was an advantage in this for CBNRC, as T Group was usually able to introduce newer technology and improve on the original device, but it always had to be on a smaller scale and at lower cost.

19.23

s.15(1) - DEF

s.15(1) - IA

19.24 Canada has played a major role in the United Nations efforts to preserve peace and promote international security, participating in almost all UN peacekeeping operations. Involvement with the Korean War (1950-53) stepped up the demand for COMSEC materials for DND, and for External Affairs its participation in the International Commission for Control and Supervision in Vietnam and Laos, beginning in 1954, did the same. Other commitments, such as in the Gaza Strip (1956-67) and in the Congo (1960-64) had a similar impact on key production.

19.25 Meanwhile the kinds of keying material requested by T Group's "regular" customers continued to proliferate: HERMES key lists and LUCIFER settings for RCN use with CCM equipment; rotor arrangements for RCAF use with MERCURY equipment; and for several users multi-way tapes and one-time pads (e.g. 200 editions of 40-way OTPs for the Army, and six editions of 300-way OTPs for the Navy). T&D also produced basic books (compilations of oft-used words with corresponding code groups for use with one-time pads) for the Army (tactical terms) and External Affairs (diplomatic terms). New customers also appeared. The Department of Transport ordered S.S. frames and 2-way, 3-way, 8-way and 120-way OTPs (up to 900 editions) for meteorological communications; and One-Time Letter Pads were made

s.13(1)(a)

s.15(1) - DEF

s.15(1) - IA

19.26 Concern was expressed in January 1962 at the Communications-Electronic Security Policy Committee (CSPC) that some departments were using commercial codes in the belief that they were achieving a measure of security. The Committee directed CBNRC to prepare guidance on the selection and use of codes and ciphers, complete with a warning of the dangers of putting trust in unauthorized codes and explaining the difference between "privacy" and "security" systems. T&D developed a privacy system for northern detachments of the Department of Northern Affairs and National Resources. And in 1967 instructions in French were published for use with one-time pads.

19.27

s.13(1)(a)

s.15(1) - DEF

s.15(1) - IA

19.28

19.29 The BALLERINA system was developed to expedite the production of 6-unit (ROCKEX) tape to meet the mushrooming requirement. Existing generating equipment produced ROCKEX key tape at the rate of 300 characters per minute. BALLERINA operated at 3600 characters per minute, the electronics being slaved to the speed of a new punch. No time was lost in the generation of unacceptable characters, as occurred with the previous system. The BALLERINA produced an edition of key tape every half hour whereas the old equipment took four hours for the same output. Tape requirements increased to the point where six BALLERINAs had to be constructed and put in operation.

19.30 In December 1957, the Director GCHQ wrote to CBNRC to ask whether the Canadian capacity to produce 5UCO key tape could be accelerated. It was expected that large quantities would be required for at least the next ten years. T Group subsequently designed and manufactured a high-speed 5-unit key tape generator called BEAVER, to replace the aging UK-built DONALD DUCK generators which, over a period of eight years, had rendered yeoman service, but whose slow speed was inadequate to cope with the quantities of tape required. The BEAVER, like the BALLERINA, operated at a speed of 3600 characters per minute. Checking the increased output from the accelerated production schedule posed no problem for the key tape checking equipment which could read at the rate of 1500 characters per second. By 1966 CBNRC was providing key tape for sale to New Zealand by External Affairs. The funds received were paid into the Consolidated Revenue Fund.

19.31 The demand for keying materials rose steadily. New crypto gear, such as the TSEC/KW-37, to protect naval broadcasts, added to the growing requirement for key in all its forms. An explosion and fire in 1958 destroyed an area of the Jackson Building on Bank Street in Ottawa, where CB had stored large quantities of keying material. To replace this storage space, a large warehouse-type building was constructed adjacent to CB's COMSEC facility, located in the NRC Montreal Road complex.

19.32 Multi-way tape (one copy for the originator plus one copy for each addressee) was becoming more popular. Three-way and six-way ROCKEX tapes had been made since 1950. In November 1959 the Army asked for 18-way tape, and later External Affairs requested 10-way tape. These requirements were at first met by designing and constructing equipments known as "reproducers", which perforated and comparison-checked the additional tapes required. Punch blocks were modified in the Machine Shop to perforate three tapes simultaneously. Greatly increased requirements for multi-way ROCKEX key tapes in late 1962 created an urgent demand for additional tape-producing equipment. In order to meet these requirements with the least possible delay, one high-speed generator (BALLERINA) was modified to produce 3-way and 4-way key tape editions by adding a second high-speed reperforator to the system; the element-operating magnets of the two reperforators were wired in series and keyed from the existing output stages of the electronic unit. In addition, a large scale reproduction unit was developed, capable of producing up to an 18-way edition in one "run". The largest edition provided was for a 26-way net.

19.33 To ensure that in-house designed and built key generators were in fact producing random key, the designs were not only sent to the UK and US for corroboration, but the output of the generators was continuously monitored and checked. During 1960 and 1961, since the BEAVER (5-unit) and BALLERINA (6-unit) key tape generators were entirely CBNRC concepts, a project was inaugurated to investigate the random characteristics of both high-speed generators by recording the actual number of pulses fed into the binary unit during each consecutive gating period. Because of the high speed involved, the result was displayed for only one millisecond interval during each cycle of operation; hence the information had to be photographed with a multi-data camera operating at 60 frames a second. An electronic counter was used to total the pulses generated during each cycle and the result was displayed for one millisecond on special ("Nixie") counters. To ensure precise timing of the shutter opening of the camera, a control chassis was built to operate the clutch mechanism. Analysis of up to 30,000 sequential characters enabled distribution curves of consecutive excursions to be plotted, providing substantial information on the characteristics of the material being generated by the random signal generator. A read-out feature was later added.

Key Cards

19.34 The key-tape-operated cipher machines provided secure one-time protection and were automatic, but they used vast quantities of tape. ROCKEX, 5UCO, SIGTOT, ETCRRM, etc. were systems in which each plain text character was matched by at least one character on key tape. Shipments of key tape produced by T&D Group amounted to several tons each month. The users, to say nothing of the producers of keying material, wanted a tapeless device, one with a built-in electronic key generator. Both the US and UK were developing such equipment in the 1950s. CBNRC (C Group) and the Canadian Services turned to the ROMULUS cryptosystem (with TSEC/KW-26 equipment), and the RCN and RCAF adopted the JASON cryptosystem (with TSEC/KW-37 and RALEIGH equipment) to protect the fleet broadcast; T Group was tasked with producing the key cards required.

19.35

Pages 1271 to / à 1272

are withheld pursuant to sections

sont retenues 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

DAUPHIN

19.38 Since the spring of 1961, T&D had been considering ways and means of automating production of manuscript for printed keying material. They obtained a brief description and photographs of a GCHQ development called DAUPHIN, a specialized electronic key generator which also seemed to promise greater security and flexibility. A T&D technologist described it as "a programmable Table Look-up machine with full operational checking facilities which employs an 'expanded alphabet' method as its random source". There followed a two-year study during which T Group assessed the scope of a project to manufacture a Canadian copy of DAUPHIN. Reluctance to copy an obsolescent technology (vacuum tube) resulted in delay in starting the project. By August 1963, the decision had been made to proceed with the development but to convert the design from vacuum tube to solid state. As space had always been a problem at CB, the small size of a transistorized version would be a plus. A T&D Section Head visited GCHQ for several weeks of training and by April 1964 the Canadian version was in the design stages - a high-speed, random access, solid state device with magnetic core memory.

19.39 In addition to information needed for the actual building of the equipment, it was necessary to acquire peripheral equipment to work with DAUPHIN, and programming data for use in the finished equipment. Rented IBM 519 reproducers would have to be modified, and it was found that later models were advisable. Then, too, greater quantities of consumable materials would be required, since, for example, in producing one-time pads DAUPHIN could use up to 30,000 cards per day, because cards would be used once only and then destroyed, whereas the existing process used cards ten times. The added expense was considered justified, however, in view of the reputed greater dependability and improved security DAUPHIN offered. GCHQ assured CBNRC "our confidence in the reliability of DAUPHIN and the number of checks that have been incorporated as internal features of the individual programs is such that ... no statistical check is made on DAUPHIN produced cards".

19.40 Extensive changes were made to the DAUPHIN logic during the development of the Canadian version, especially to the logic of the address store, which was converted from magnetic core to transistor logic. A transducer was used to obtain the timing pulses from an IBM 519 reproducer, with a high intensity light beam driving a photo sensitive device. In order to simplify the output circuits of the DAUPHIN, the polarity of the power supply was reversed. By halving the cycle time in the transistorized version, T&D were able to double the data processing speed of DAUPHIN. S Group completed the construction and checking of the DAUPHIN system by the end of December 1965, and large shipments of programming material were received from the UK in the ensuing months. The various programs were tested through DAUPHIN, and then the system was transferred to T Group in October 1966.

19.41

Computer-Controlled Production

19.42 The shortage of floor space continued to plague T Group. In order to provide more room for production, imaginative means were used - such as building additional capabilities into existing equipment, e.g. a tape reader was interfaced with the DAUPHIN equipment, rendering it usable for checking tape, with an IBM 519 reproducer as the output device for recording the statistical data and making it possible to dispense with the High-Speed Tape Analyser.

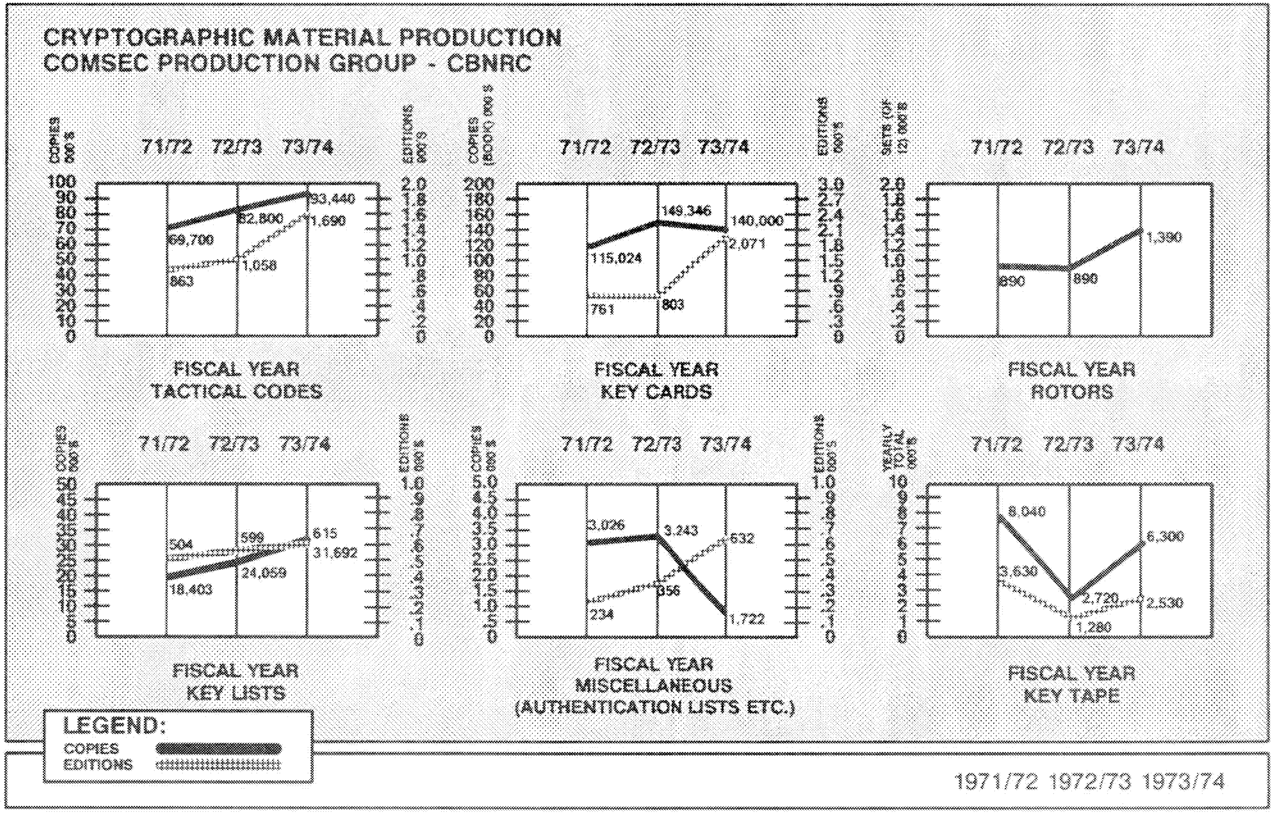
19.43

19.44 Planning began in 1970 to upgrade T Group's facilities for the production of manuscript for crypto keying materials and for the development of an electronic random generator for all key, in lieu of dedicated generators for each generating station. Initially, the IBM 407 Tabulator, used for manuscript preparation, was replaced by a high-speed magnetic-tape-driven phototypesetter. This was capable of mixing two fonts and six type sizes automatically from tape command, and provided high quality printing. Input data for the phototypesetter was prepared on M Group's 370/145 computer. This adaptive software intermixed the crypto variables generated on the DAUPHIN/IBM 519 equipment with appropriate typesetting command instructions. All cryptodata was recorded by T Group's IBM 1401 computer and supplied to M Group on 7-track magnetic tapes. This process was necessary until T Group could develop its own electronic random generator (the MP14CDN - see following paragraphs), which would produce random tapes from which crypto variables could be obtained directly; at that point the DAUPHIN/IBM 519 generating and formatting equipment could be phased out.

19.45

19.46 Requirements for new types of keying material created the need to develop and construct new production equipment, e.g. a high-speed multiple head perforator which was fabricated in the T Group Model Shop, as well as various mechanical parts. Numerous circuits were designed, and as many as 1,100 small circuit boards (Relay Modules) were made by T Group's Quick Reaction Facility (QRF) for the CID/610 crypto equipment. More than 3,000 modification kits were made for DND, who placed a Financial Encumbrance in the amount of $210,000 at T Group's disposal for the acquisition of component parts and specialized production equipment.

19.47 The advent of more sophisticated cryptosystems did not put an end to the requirement for one-time pads, low level tactical codes, authentication systems and call-sign encryption/disguise systems. It would appear that there will always be a need for these at the tactical level, or as a back-up when all else fails. An appreciation of the quantities of the main types of COMSEC material produced in the last few years of CBNRC may be gained from the chart shown at Annex A.


CRYPTOGRAPHIC MATERIAL PRODUCTION
COMSEC PRODUCTION GROUP - CBNRC

s.15(1) - DEF

s.15(1) - IA

Chapter 20

Use of Crypto Equipment in Canada

Chapter 20(cont'd)

Chapter 20 - Use of Crypto Equipment in Canada

General

20.1 Paper and pencil codes and ciphers were the only cryptosystems available to government offices prior to World War II and were used in the Departments of External Affairs and National Defence. There are still a few applications where these "book type" systems are necessary, but for the most part today classified government communications are protected by machine systems. During World War II, and until 1947, the UK supplied to the Canadian Government cryptomaterial and cipher machines free of charge[1].

20.2 All crypto equipments must provide the required degree of security for their intended use and be compatible with the associated transmission system(s). The type of crypto equipment designed to function with one particular transmission system, however, is not necessarily compatible with equipment used with other systems. Ideally, it would be preferable to have one crypto equipment that could be utilized with all types and forms of transmission systems. Any such universal equipment would likely be so complex that it might prove uneconomical to develop, produce and maintain. To provide speed, reliability and flexibility on national communication networks, a number of different transmission systems must be employed. It follows, therefore, that a variety of security equipments must be used if all crypto requirements associated with existing and projected types of transmission systems are to be met.

20.3 The complexity of crypto equipment design is attributable to the interrelation of operational security and technical considerations. There is a constant demand for minimum size and weight, and for capability of operation under extreme climatic and other adverse conditions, particularly in relation to the use of equipment in ships, vehicles, aircraft and

[1] See para. 15.7

other restricted or non-static locations. Security factors are, of course, paramount:

a) Modern cryptanalytic techniques are such that only very complex crypto equipments are capable of withstanding attack;

b) In addition to providing protection against cryptanalytic attack, it is necessary to safeguard the overall communications system from exploitation as a result of inadvertent radiation of plain text or other compromising information from the apparatus used to prepare, encipher and transmit messages;

c) There is also a need to reduce or eliminate the human element, and thus eradicate exploitable compromises caused by operating and/or procedural errors;

d) Finally, safeguards must be built into the machine itself to prevent undetected malfunctioning. Without a foolproof system of alarms to warn the operator and/or to stop transmission automatically when a fault occurs, it is possible for a cipher machine to appear to be working satisfactorily when in fact, to take an extreme example, plain text is being transmitted.

The number of cryptographic processes varies for different methods of transmission, but all necessitate equipment of varying degrees of complexity. Attempts to meet all requirements lead to an increase in the sophistication of techniques and the complexity of design, engineering and production factors.

20.5 The early machines, of course, did not have all the built-in precautions described above. The main objective of their designers was to incorporate enough complexity to make it impossible for unauthorized persons to exploit the encrypted communications. They learned through experience with their own inventions about the weaknesses of the systems, including the vulnerabilities caused by radiation or induction.

20.6 Cipher machines may be divided into two groups: off-line, in which encipherment is performed as one process, and the resultant protected version is then transmitted in a second operation; and on-line, where the cipher device is connected to the circuit and the processes of encryption, transmission, reception and decryption are carried out virtually simultaneously. The early cipher machines were all off-line, until the art of combining encryption and transmission was learned.

20.7 In the 1940s and 1950s a distinction was also made between Category A and Category B ciphers - the former being a system in which a compromise of one or more messages would not endanger other messages encrypted in the same system, and the latter being a system in which a "break" or "crib" into an encipherment could assist in the cryptanalysis of other messages. Special precautions had to be taken with "BECAT" or "CAT B" messages, e.g. the literal plain text had to be paraphrased before distribution. As the newer systems were stronger and all considered "CAT A", this distinction was no longer necessary. TYPEX Mark II and the early version of Mark 22 were CAT B; the security of Mark 22 was greatly enhanced by the addition of a cross-over plugboard and special operating procedures, which brought it up to Category A. Other crypto devices mentioned in the following pages were all Category A.

20.8 We speak of various generations of crypto machines. The lines of demarcation between generations are fuzzy, and depend upon the person doing the classifying and the reasons for doing so. For the sake of simplicity, in this History the crypto devices used in Canada will be discussed more or less in the order of their appearance chronologically, but grouped according to their method of operation, considering the simpler forms, e.g. rotor-operated electromechanical types, first, followed by electronic devices with vacuum tubes and tape transmitters, and then the solid-state types developed after semi-conductors and integrated circuits came into use. The latter, often called the third generation, were mainly devices with built-in key generators, obviating the need for bulky keying material.

TYPEX

20.9 The first cipher machines used in Canada were TYPEX (originally Type X) off-line electromechanical devices using a rotor-maze to scramble plain language. These were provided by the UK during the early years of World War II, and were used by the Departments of External Affairs and National Defence, and later by the RCMP. Their use declined in the 1950s and 1960s when other crypto equipment became available. TYPEX was also employed by other agencies such as the Department of Trade and Commerce and the Wartime Prices and Trade Board. CBNRC inherited TYPEX machines from the Army and British Security Coordination (BSC), and used them from 1946 to 1949. The last TYPEX message received at CBNRC was deciphered at the Guigues Street location in December 1949, and contained Christmas Greetings from the Director and Staff of GCHQ.

20.10 In 1946, the original wartime version, TYPEX Mark II, was still in use in Canada, but the security it provided was suspect. The TYPEX was a modified version of the German ENIGMA, a reciprocal system: complicated procedures and hollow drums with inserts had been introduced during the war years to counteract certain weaknesses; other minor changes were made to disguise the rotor turnover, etc., but it was feared that the Germans had solved the drum pattern, because the indicator system was simple and operators encrypted long messages with very little change in the settings between message parts. During the war, it was considered impracticable to increase the security of TYPEX by further modifications to the Mark II.

20.11 It is an accepted policy that the security estimate of cipher machines such as TYPEX should be based on the assumption that the wiring of the drums/inserts and every detail of the machine, except of course the variable keys, is known to a foreign power. TYPEX machines, without the drums, were captured by the Germans at Dunkirk. Bill Trowbridge, in a memorandum to the Director in July 1947, gave the assurance: "In spite of great efforts exerted against it (TYPEX), we must assume that it was never broken; however, they (the Germans) did work out theoretical principles of attack and were only a hair's breadth from their objective." He said the Germans failed only because of their tendency to place too much confidence in any machine system built on the lines of their own ENIGMA, which they believed to be unbreakable. He added, "As far as can be ascertained, drums and inserts were never compromised".

s.13(1)(a)

s.15(1) - DEF

s.15(1) - IA

20.12 Nevertheless, the faith of at least some Canadians in the security of TYPEX was shaken, especially when a UK assessment of the equipment in August 1946 said: "TYPEX Mark II, when the inserts are compromised, can be broken theoretically on a crib of 30-40 letters. Moreover, the machinery necessary for this form of attack is well within the compass of present-day electrical and mechanical achievement. One hundred machines of a suitable design could try all possible insert combinations and all possible drum readings in about three hours ... if one message on a key is broken every other message must be treated as compromised .... Every effort has been made to reduce the number of such cribs, but practical experience shows conclusively that they can never be eradicated." In order to minimize the danger as much as possible, operational precautions such as cyclic procedure and insertion of extra characters (figure-shift/letter-shift) were introduced. In effect, therefore, the security of TYPEX rested upon the conscientiousness of operators in implementing the procedural precautions in practice. The truth remains, however, that placing too much reliance on human efficiency is fundamentally unsound. The security should, as far as possible, be borne by the machine.

20.13

20.14 It would appear that Bill Trowbridge's conclusion was correct: viz. that TYPEX was never broken, despite its capture at Dunkirk. Military communicators were usually very conscientious in protecting cipher equipment and materials in view of the environment in which they worked. When Tobruk was captured by the Germans, there was no evidence of a TYPEX machine, and all TYPEX material was destroyed before the enemy arrived on the scene. Discipline as regards precautionary procedures in the employment of the ciphers was another matter. Use of the HAGELIN M209 was so careless that it was read 10 - 30% of the time; low-grade ciphers were broken almost completely; and SLIDEX was broken due to bad usage. Even book ciphers were well read; the German Navy read Allied high-grade ciphers until 1943, when they were stopped by the use of the SS frame system and the introduction of new and better basic books. These experiences were common to Allied Forces, including Canadian troops interworking with others.

20.15 The TYPEX Mark II was replaced in 1948 by the Mark 22, which was in fact a Mark II with a modified scrambler unit. Special settings, though costly to produce, were introduced to increase security: "Simplex" settings (not actually the equivalent of one-time pads, because, although truly random non-repeating keys were used, the insert wirings were fixed) to ensure that if the setting used for one message was broken, the solution of the whole day's traffic did not ensue; and "Publex" settings, based on a limited scramble, and used for enciphering TYPEX messages which had been or were to be published (and therefore might be used as a crib to the plain text in a less secure cipher).

20.16 The life expectancy of a cipher equipment, both cryptologically and logistically, is considered to be about fifteen to twenty years; consequently in the early 1950s the TYPEX was declared obsolescent. The UK discontinued manufacturing the device in 1953, although it was planned to use the equipment for several more years. This caused concern in Canada, and the Cipher Machine Production Group (CMPG) was directed to explore the possibility of manufacturing the equipment, or at least spare parts for it. In addition to being used by the Army, Navy, Air Force, RCMP and External Affairs, TYPEX had also been issued to the Shell Petroleum Company.

20.17 The CMPG reported several times to the Cipher Policy Committee (CPC), providing details of the anticipated requirement for parts and the estimated cost of producing them, and ventured the opinion that the project was feasible. The Committee members asked for information on the production of parts for other crypto devices as well, and soon the study developed into a much larger project in which cost became a prime factor. The Committee was told that the cost per unit spare part would vary inversely in proportion to the number of units required. It was suggested, therefore, that a ten-year supply should be ordered. Unfortunately, DND regulations limited quantities to the requirement for the first year of any hostilities. The CPC sought authority to produce in quantity. By the fall of 1954, with UK production of TYPEX machines having been terminated the previous year and production of spare parts about to cease, it was realized that Canadian production could not get under way in time. Thereupon, the Services obtained authority to place an order for a six years' supply of spare parts. The orders were coordinated by the Department of Defence Production (DDP). External Affairs reviewed its situation, and concluded it had no requirement to place an order. Production drawings of other equipments were purchased from the UK with the intention of exploring further the possibility of Canadian production. Thereafter, the London Communications Security Agency (LCSA) arranged with CBNRC in 1957 to have the latter store a complete set of production drawings for all future UK crypto equipments, in case the original drawings were destroyed or lost. This arrangement was modified in 1965 to include only equipments in which there was a definite Canadian interest.

20.18 The planning for a replacement for TYPEX began in 1953. As late as 1959, however, the Communications-Electronic Security Group (CSG) Chairman was urging other Canadian users to replace the device, insisting that such action had to be completed within five years. The KL-7 had been introduced in July 1956 as a replacement for TYPEX for NATO and Combined use, and the three Canadian Services had participated in the changeover. TYPEX continued to be used for national traffic for several years, however, while the COMSEC Community discussed the pros and cons of the various equipments proposed for adoption. By mid-1959 the RCN had replaced all TYPEX machines with KL-7. The Army was considering the SINGLET, a British rotor-operated device which could be compatible with the KL-7; however, they eventually bought the KL-7. The Air Force was planning on the eventual replacement of TYPEX with the KL-7; this was accomplished by the end of 1962. By this time the only use of TYPEX by the Canadian Services was in those instances where Army units were stationed in areas where the security hazards were such as to preclude the issue of "modern" crypto equipments, e.g. the Congo (1964) and Indo-China[2] (1964-73). The RCMP continued to use TYPEX, mainly as a back-up equipment to ROCKEX, but finally disposed of their equipments in December 1968. The External Affairs replacement program was slowed by the austerity program in effect at the time, but gradually disposed of their TYPEX holdings through replacement by more modern equipment at the rate of about one per month, until only the Saigon office was served by TYPEX in 1970; all equipments had been replaced by mid-1971.

PORTEX

20.19

s.13(1)(a)

s.15(1) - DEF

s.15(1) - IA

20.20 Sixty-five PORTEX machines were requisitioned by the Canadian Army in May 1956, and despite some teething problems the Army was satisfied with the device, and was planning to order an additional 50 to 90 when word came from England that production had been discontinued in July 1959. CBNRC produced keying material for the Army-held PORTEX equipments: High Tide key lists for high echelon and special purpose use, as a back-up to ADONIS; and Low Tide key lists for field use. (Both systems were Category "A".) CB also produced PORTEX inserts in 1961. By 1968 PORTEX was no longer required, and it was declared surplus. "Complete and utter destruction" of Canadian holdings of the device was authorized under Section 5(e) of the Surplus Crown Assets Act. This included the four equipments held by T Group for the production of key lists.

Combined Cipher Machines (CCM)

20.21 During World War II the US supplied the RCN with a number of Combined Cipher Machines (CCM, also called AJAX) for communication with USN ships and shore authorities. The CCM employed the same cryptosystem as TYPEX (the LUCIFER system, using 26-point rotors). In fact, there was a version of TYPEX, Mark 23, which was called a "CCM Adaptor" and was cryptographically compatible with the CCM. CBNRC used the CCM for secure communication with NSA until November 1947, when it was replaced by ROCKEX. However, the UK authorities were not satisfied with the security provided by the CCM. When the RCN in 1948 requested a change in procedure in communications between the RN and RCN, which would result in the RCN abandoning TYPEX in favour of CCM for all purposes, the reply was that the Admiralty felt, though it could not officially state, that "the security of the CCM ... is markedly less than TYPEX with all modifications". In 1952 GCHQ signalled CBNRC: "Nature of insecurity of CCM is newly discovered exhaustion attack based on catalogue from known wirings ... US authorities agree with us on insecurity ...."

20.22 As related elsewhere, the RCN at first obtained their CCM rotors from the US; later they wired their own, and still later the rotors and settings were produced by CBNRC. The latter held TYPEX Mark 23 until December 1949, at which time some CCM machines were obtained from the RCN; these were used by T Group for producing key lists. With different rotors and settings, the CCM employed the HERMES cryptosystem, and CBNRC produced these key lists for the RCN and the Army.

20.23 As the crypto life of the CCM drew to a close in the early 1960s, there was a campaign in NATO, spearheaded by France, to use CCM for meteorological traffic. HMC ships used CCM equipment for the decryption of synoptic reports in digital form which were required by ships and authorities with meteorological staffs. The equipment was, however, not quite appropriate for literal weather reports such as fleet forecasts, gale warnings and other

s.13(1)(a)

s.15(1) - DEF

s.15(1) - IA

plain language messages expressed in non-technical terms. Owing to the stereotyped nature and the large number of these transmissions, the security of CCM for this type of meteorological traffic would be much lower than for normal communications, and therefore certain restrictions would be necessary, e.g. special notched rings and key lists. NSA felt that the device was "eminently unsuitable" for this purpose because of its age, lack of spare parts and non-availability of adequately trained maintenance personnel. Destruction of the CCM was authorized in 1962; all Canadian-held equipments were collected by Canadian National Distributing Authority (CNDA) and reduced to slag by November 1963.

20.24

Pages 1296 to / à 1297

are withheld pursuant to sections

sont retenues 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

s.15(1) - DEF

s.15(1) - IA

20.28

20.29 The introduction of the KL-7 into Canadian Government communications provided a pattern to be used with other crypto devices. In November 1953 T&D asked NSA for the loan of a KL-7 with accessories, key lists, rotors, and technical and operating handbooks, to permit them to gain a thorough working knowledge of the machine. The receipt of two machines in February 1954 enabled them to become acquainted with the device and to demonstrate it to potential users. A short term loan of ten more machines made it possible for the Services to conduct trials in the field, and to complete their plans for acquisition. In the end, the KL-7 was also used in the POLLUX cryptosystem by the RCN, and jointly by the RCN and RCAF in Maritime operations. Special rotors and key lists were authorized, and abbreviated procedures were allowed because of the peculiar limitations when operating in aircraft.

s.15(1) - DEF

s.15(1) - IA

20.30

Other Rotor-Maze Devices

20.31 As late as 1959 the RCN and RCAF were using TSEC/KW-2 equipment on cross-border circuits with the USN. This device, with 26-point rotors and a 26-position plugboard, incorporated the GORGON cryptosystem. The equipment was phased out in December 1959, and all devices were returned to the USN.

7. See para. 19.19

20.32 The crypto devices discussed so far in this Chapter have all been electromechanical, rotor-maze machines. GCHQ developed two other "wired codewheel" devices, SINGLET and PENDRAGON. Both could operate in the ADONIS cryptosystem (among others), and so be compatible with the KL-7. These two devices were demonstrated to members of the Canadian COMSEC Community, but following user trials the preference was for the cheaper, simpler KL-7; installation instructions were drawn up to illustrate the changes that would be required for the UK devices to achieve telegraphic compatibility with North American standards, and the expense and effort were deemed impracticable. The next generation of crypto equipments involved the use of key tape; they were more automatic in operation.

TELEKRYPTON

20.33 The TELEKRYPTON was the earliest crypto device with one-time-cipher potential used in Canada[8]. Introduced into the Prime Minister's cipher office (External Affairs, East Block) on 27 April 1942, this electromechanical teleprinter signal mixer could have provided high-grade security. A commercial development, it mixed the plain language characters (perforated into teleprinter tape in Murray code) with characters on a second tape, a key tape, to produce an enciphered signal which was transmitted to line. Having never been instructed in COMSEC, and therefore unaware of the significance of the expression "one-time-cipher", the cipher clerks, including the writer, made up tape loops, using text from a magazine or newspaper for key, and fed this cyclical key tape through the mixer until it wore out and had to be replaced. The main cipher link used was between External and the Canadian Embassy in Washington. It would have provided one-time security if random one-time key tape had been used. Later on, when such key tape was available, TELEKRYPTON was used by External (up to 1948) in a more secure mode. This was the first of the PYTHON systems - operated

[8] See para. 15.6

by 5-unit key tape. It was a step forward because it was also the first on-line system, in which the encryption and transmission were combined in one process. TELEKRYPTON was also used between the Examination Unit (XU) on Laurier Avenue, Ottawa (later the Joint Discrimination Unit (JDU) on Guigues Street) and the British Security Coordination office (called the "British Intelligence window in North America") in New York. The External Affairs equipment was later turned over to CBNRC for experimentation.

ROCKEX

20.34 ROCKEX equipment was a welcome addition to crypto centres which had previously used rotor-operated equipments and book ciphers. Although it, too, was an off-line equipment, it became the work horse for all Canadian Government crypto centres and their networks. Because a prepared plain text tape could be fed into a ROCKEX machine and automatically enciphered at about 35 groups per minute, it was a major advance over the TYPEX with which encipherment took place at an average rate of five groups per minute. (Although a good operator would regularly exceed this rate, some did not, and this was the argument used to justify purchasing the speedier ROCKEX.) Moreover, crytographic security was greatly enhanced because ROCKEX employed one-time random key tape.

20.35 At the 17th Communications Research Committee (CRC) Meeting on 8 May 1947 agreement was reached on the purchase of 15 ROCKEX equipments for SIGINT use - five for CBNRC and ten for the intercept stations. DSigs (Army) processed the order using "Defence Research SIGINT funds", and also provided the ancillary teletype equipment. Delivery was slow, however, and by 9 February 1949 only four equipments had reached CBNRC; as traffic volume was steadily increasing, Bill Trowbridge found it necessary to request DSigs to help speed up delivery of the remaining one. The Defence Services had begun using ROCKEX equipment as early as 1947, and External Affairs by 1948, with CB technicians setting up the

s.15(1) - DEF

s.15(1) - IA

equipment and training their personnel. CB also supervised the installation of ROCKEX with suppression kits and a screened cage in the Canadian Consulate General in New York in August 1949, and conducted TEMPEST tests in the vicinity of the installation, as explained below.

20.36

20.37 The first ROCKEX equipments used in Canada were Mark II models. The UK confirmed in 1948 that future models would be engineered to suppress radiation, but that the induction risk could remain if the equipment or its ancillaries were carelessly installed or modified. CBNRC Communications Centre at first used ROCKEX II equipments (as many as 18 units), acquiring one to four at a time up until April 1950, and then gradually disposed of them as they could be replaced by ROCKEX IIIs and Vs in the late 50s and early 60s. External Affairs sought to purchase a large number of ROCKEX Mark IVs, but after TEMPEST tests run by CBNRC[9] bought Mark IIIs in 1956 instead; later some of these were converted through modification to ROCKEX Vs, the TEMPEST version of ROCKEX III, and others were replaced by purchasing ROCKEX V equipment. At about the same time the Services and the RCMP were also graduating from ROCKEX IIs to IIIs and Vs. Although somewhat different in circuitry and operation, ROCKEX II, III and IV were cryptographically identical. Bill Trowbridge, in a memorandum in February 1958, notified Ken Hughes (C2) that all three versions were radiation offenders, but that the danger could be minimized if the equipment was installed and maintained in accordance with technical specifications. CBNRC returned ROCKEX equipments to the Services as they were superseded by other devices between 1959 and 1968. The Services declared all

[9] See para. 24.12

ROCKEX equipment surplus in 1969, and disposal was authorized. External and CBNRC retained a few ROCKEX machines in use for another fifteen years.

NOREEN

20.38

20.39 Although the use of crypto equipment was spreading, most government communications continued to be in plain language even in the late 1950s. The CSG prepared a paper, which was eventually issued as CSB/79 dated 31 December 1958, and which outlined the long-term policy of the Canadian Government with respect to the cryptographic protection of its communication networks. In essence, CSB/79 recommended reduction in the transmission of plain language, recognized adoption of a total encryption concept as the ultimate goal, and urged conversion to automatic on-line transmission wherever possible with the minimum delay.

5UCO

20.40

s.15(1) - DEF
s.15(1) - IA

20.41 External Affairs and the Services installed 5UCO on certain point-to-point circuits in 1954-57; the RCN, for example, used it between Ottawa, Halifax and Whitehall. It took CB almost ten years, however, to convince the Services to convert the other SIGINT circuits - those between CBNRC and the intercept stations - to 5UCO operation. The RCAF favoured conversion of the station circuits to on-line with 5UCO, but the Army and Navy felt that traffic loads did not warrant the expense. Although anxious to upgrade all their communications/crypto capabilities, they were daunted by the anticipated costs. The cipher facilities possessed by the three Services - primarily off-line, manual systems which were slow and expensive in manpower - could not cope with the huge task of encrypting all unclassified information sent by high frequency radio, which had proven to be a major source of COMSEC weakness. Viewed individually, unclassified messages appeared to have no intelligence value; on the other hand, a collective analysis of unclassified messages sent in the clear in 1957 on main line point-to-point radio-

10. See para. 14.31 and Annex 14.D

teletype links, and on shore-to-ship radio-teletype and Morse broadcasts using high frequencies, yielded considerable intelligence. Part of the problem of the cost of converting CB-to-station circuits to on-line was resolved when NSA gave Canada 23 5UCO machines in 1959 (having replaced them with KW-26 on US circuits). All the Canadian intercept station links were converted to 5UCO in 1960. There remained the expense of supplying these circuits with key tape, but CBNRC was happy to shoulder the extra effort and cost in order to achieve greater security.

20.42 The 5UCO was a very reliable, automatic, synchronous, electromechanical/electronic duplex equipment. It encrypted at 66 words per minute - twice the speed of ROCKEX - and, being on-line, transmitted automatically, thus eliminating the delay factor normally attributed to the use of COMSEC measures. Transmission of 5UCO-encrypted traffic was affected less by line hits than was plain language. Security alarms were adequate to prevent unsafe operation. Unfortunately, the 5UCO did have some TEMPEST problems. In addition to the extravagant use of key tape, 5UCO also required considerably more technical support because it was the technician, not the communications operator, who controlled the crypto machine. The 5UCO enabled Canadian users to cope more readily with the burgeoning traffic volumes in the 1950s, and allowed them time to seek a "tapeless" device. The KW-26 and ALVIS were being considered as replacements. The RCN ceased using 5UCO in 1962, and CBNRC in 1963. The Army continued using the device for three more years. Five serviceable machines were returned to the UK, where a need existed for them. The remaining machines were destroyed (at Merrickville) as they became surplus to requirement. Final destruction certificates were rendered in 1971.

Other PYTHON Systems

20.43 As indicated previously, the PYTHON cryptosystems were those that employed one-time 5-unit key tape. By the mid-1950s several of the NATO countries had developed on-line PYTHON systems. The US version was the SIGTOT, a start/stop, simplex system which was used by the Canadian Services on certain operational circuits as a stop-gap measure until a tapeless device could be acquired. The SIGTOT came in various configurations, involving several different constituent devices. Norway also produced an acceptable start/stop, simplex device, called ETCRRM (pronounced ET-SET-RUM). It was adopted by NATO, and was used by the RCN and RCAF in NATO formations. In CBNRC, C Group experimented briefly with ETCRRM in 1958, but after installing security modifications, turned it over to Ottawa Wireless Station. The ETCRRM was also manufactured in the UK under the name DERBY. SIGTOT and ETCRRM/DERBY were compatible, and could interoperate with a common key tape.

20.44 Neither the SIGTOT nor the ETCRRM was suitable for use on HF radio circuits. Also, both devices were serious TEMPEST offenders, and warnings about this danger were frequent. Radiation could be reduced by buffers, but as these ciphers were only regarded as interim systems, users hoped to acquire later generation systems before too much modification was necessary. Newer, more secure equipment had been produced, but financial constraints prevented most authorities from making the purchases they desired. The adoption of improved crypto facilities did not keep pace with the modernization of message handling methods and transmitting techniques. Moreover, although traffic loads were greatly in excess of the intended usage for which the PYTHON (and other) systems were designed, and warranted the adoption of more automatic equipment, many users were still dependent on PYTHON or even off-line and book cipher systems. The lack or inadequate supply of better crypto equipment made it difficult to upgrade the tape-using devices. Many Canadian users were still scrambling to obtain SIGTOT equipment cast off by US communications facilities when the latter converted to KW-26. This was true even as late as 1963, at which time word came that the KW-26 production line would halt in 1964. As the KW-26 was one of the main contenders to replace PYTHON equipment, this latest news spurred members of the Canadian COMSEC Community to renew their efforts. Using the sort of arguments indicated above, they were able to pry loose funds for the purchase of equipment with self-generating keying facilities built-in. In the spring of 1971 the Deputy Minister of National Defence reported that $30 million had been expended by his Department during the previous five years on the procurement of on-line systems, and that the total DND expenditure for the full COMSEC program could shortly exceed $74 million. The disposal of ETCRRM and SIGTOT equipment "by authorized secure means" was ordered in February 1971.

KW-26

20.45 The equipment suggested by the US to replace PYTHON cipher devices was the TSEC/KW-26, a fully electronic on-line crypto machine with a key generator (61-stage shift register) incorporated. It was a duplex, synchronous on-line equipment for use on HF radio and long line circuits. The stages of the key generator were pre-set automatically by insertion of a daily-changing punched card, obviating the need for expensive, bulky key such as key tape (by comparison, a duplex circuit would require 4 to 8 key cards daily at a total cost of only one or two dollars, as against the $54 needed for 24 reels of PYTHON tape)[11]. An elaborate system of alarms automatically interrupted transmission in the event of equipment malfunction or operator errors, in order to minimize the possibility of security problems. Two terminals could remain in crypto synchronism for up to two hours, even if the signal were interrupted. In addition the KW-26 provided traffic flow security and could operate in several modes,

[11] See end of para. 20.40 above

although only one mode was used in Canada. The circuitry was engineered to render the device "acceptably radiation-free".

20.46

20.47 In the meantime, DND did obtain authorization to purchase 216 KW-26 machines (RCAF 112, RCN 73 and Army 31), for delivery in quantities of 10 to 20 each month from the fall of 1961 to the end of 1962. In the 1970s, CBNRC opened up a KW-26 link to pass

12. See para. 14.64

s.15(1) - DEF
s.15(1) - IA

intelligence to External Affairs and the Privy Council Office (PCO).

And finally, a few KW-26s were still being used by DND in December 1985. (D/COMSEC proclaimed the KW-26 the most useful piece of crypto gear DND had ever used, primarily because of its durability.)

ALVIS

20.48 The UK, too, developed a replacement for their tape-operated on-line equipment. The initial design, called INCUBATOR, was intended to serve as the basic equipment for a wide variety of applications using one of four types of control box. Only one version caught hold, in Canada at least, viz. the ALVIS or BID/610. The BID/610 had two modes of operation: Mode A, cipher text auto key, and Mode B, a "long cycle" additive key cryptosystem. Although development was under way in the mid-1950s, production problems introduced delays, so that even in 1961 only informal information was available for procurement planning. It was inevitable that comparisons would be made with the KW-26, delivery of which was to commence in September 1961. The CSG noted price increases indicating that ALVIS would cost $2,000 to $3,000 more per duplex terminal than the KW-26. In March 1962 the CSG was informed that further cost increases and delay in delivery would result from the need to modify the equipment, in order to incorporate certain operational facilities which the Canadian Services considered essential.

20.49 In 1960, the Canadian Army's interest in acquiring ALVIS had increased greatly as international tensions worsened, and procurement plans were changed in order to purchase larger quantities of ALVIS than originally anticipated. By

1964 elements of the Canadian Army were being deployed with United Nations forces in Cyprus, and expressed an urgent need for a number of machines for use there. (As noted elsewhere, the use of COMSEC material and equipment by Canadian forces operating under foreign commanders, other than US or UK, was not authorized, except for machines such as TYPEX which were obsolescent.) External Affairs was also evincing intense interest in ALVIS, and requested firm quotations on six equipments; they later bought 97 in all. RCMP, DND and CBNRC each acquired a small number of BID/610 machines.

20.50 Enthusiasm for building a Canadian crypto machine climaxed at this time. The Intelligence Policy Committee (IPC) had given approval in principle in 1961 to the production of ALVIS equipment in Canada, but many factors intruded to introduce delays: e.g. it took a year-and-a-half to negotiate an overall agreement with the UK Government. The project to produce the Canadian version of ALVIS, the CID/610 (CID - Canadian Inter Departmental, as distinguished from BID - British Inter Departmental) is detailed in Chapter 22. The CID/610 developed only Mode A, and also incorporated design modifications to meet Canadian needs. DND bought 872 copies of the CID/610. External bought only the UK version. A Standing Group instruction dated 17 April 1962 approved BID/610 for the encryption of NATO information of all classifications, subject to the condition, among others, that it be operated within a 50-foot secure zone; Corrigendum 1 to this instruction, dated 31 March 1964, changed the secure zone from 50 feet to 200 feet. TEMPEST tests which were conducted on the Canadian-produced ALVIS equipment, as related in Chapter 22, showed that all the devices tested met the prescribed standards.

20.51 The SAMSON Program was initiated in the late 1960s to develop a national strategic communications net to provide secure data and telegraph circuits for operational and administrative communications between DND bases. At the time there was a large inventory of CID/610 equipment, and it was decided to use this device with SAMSON. In some ways, the KW-26 would have been preferred for this purpose, partly because it was synchronous, whereas the ALVIS in Mode A was a synchronous, although it could be used as a self-synchronizing start-stop equipment. The KW-26 had a top speed of 100 words per minute (w.p.m.), while the speed of the ALVIS was able to be increased to 220 w.p.m. Eventually, SAMSON with ALVIS was put into operation after the end of the period covered by this History, and the CID/610 continued in use in the SAMSON system for many more years.

KW-37 & RALEIGH

20.52 Reference has been made to the incorporation of alarm systems into crypto devices to detect any malfunction that might lead to insecurity. Perhaps the ultimate in US alarm philosophy is the KW-37 equipment used in the naval broadcast system since the late 1950s. It uses the JASON cryptosystem. The KW-37 is a synchronous, on-line teletype security system providing traffic flow security. It contains 53-stage electronic key generators, for which punched cards are used to provide the daily set up of variable elements. The transmitter has three identical key generators which are set up, keyed, and started simultaneously; and all three generator "outputs" are continually matched against each other. Unless at least two of these output streams match exactly, the system shuts down. If only one stream does not correspond exactly with the other two, its generator can be removed, fixed, and replaced without interrupting communications. The KW-37 receiver has only one key generator which is set up daily with an exact copy of the punched cards used in the transmitter generators. A broadcast net consists of a single transmitter and any number of slave receiving terminals. If a ship leaves one broadcast zone and enters another, it can simply insert the appropriate key card and tune in to the nearest JASON broadcast any time during the 24-hour cryptoperiod, at which point its KW-37 receiver will accelerate and search until it catches up to the transmitter, and then will automatically synchronize with the signal. The KW-37 was designed to minimize TEMPEST problems.

20.53 Because the US JASON cryptosystem development was so far advanced, the UK proposed in October 1956 that the cryptographic equipment for on-line ship Radio Teletype (RATT) broadcasts of the CANUKUS navies should be the KW-37 or equipment compatible therewith.

In order to enable the RCN to monitor the US naval broadcast (for use in CAN-US HF/DF stations) the USN made five KW-37 receivers (KW-37R) available to the RCN in 1958.

20.54 The Canadian naval primary broadcast transmitters at Halifax and Esquimalt were also eventually (1962) protected by KW-37T. The importance attached to securing the shore-to-ship broadcasts may be gauged from the fact that the RCN was able to obtain in October 1957 authorization to spend more than a million dollars for delivery of seven transmitters in 1959-60, and 99 receivers in 1960 and 1961. The use of the KW-37 by the RCN for shore-to-ship broadcasts was approved by the CPC in February 1959. As the world political situation worsened, the RCN within a year increased its order by an additional transmitter and 15 more receivers. The following year the order was further increased to ten transmitters and 129 receivers. Total RCN holdings of the KW-37 eventually reached 30 transmitters and 145 receivers. When the RCN order for KW-37s was placed with the Department of Defence Production (DDP) for processing through NSA, DDP queried NSA about the possibility of the equipment being produced in Canada. This resulted in protracted discussions of the pros and cons of Canadian production, with NSA not voicing opposition, but merely noting that such action would certainly delay the acquisition of the equipment by the RCN. Bill Trowbridge pointed out that the small quantities required by Canada would hardly justify the tooling costs ($700,000). DDP finally agreed, due to the adverse timing factor, to place a purchase order on NSA to meet the RCN requirements for KW-37 equipments.

20.55

20.56

s.15(1) - DEF

s.15(1) - IA

20.57 The RCAF Maritime Command worked in close cooperation with the RCN in anti-submarine operations. When the Navy were fitting KW-37 receivers in ships, the Air Force felt it would be an advantage for their Maritime reconnaissance aircraft to be able to read the naval broadcast during joint and combined operations. They conducted studies and evaluations of the KW-37R in Argus Maritime Aircraft. Some US activities expressed an interest in the results of the RCAF trials. The KW-37R, however, had not been designed for airborne use. The RCAF also conducted trials with the UK RALEIGH equipment. The latter was preferred because of its smaller size, its weight (about half that of the KW-37R) and power characteristics (28 watts as compared with 320 watts for the KW-37R), but the price was 85% higher per unit. Nevertheless, the RCAF invested in 44 RALEIGH machines.

20.58

s.15(1) - DEF

s.15(1) - IA

20.59 As the period covered by this History drew to a close, the KW-37 and RALEIGH were still very much in use. Large scale integration (LSI) techniques were being introduced into crypto equipment production, and a replacement (KW-46, VALLOR) was being planned for the JASON devices. It would be another ten years, however, before this would come to pass.

KW-7 and PUGILIST (BID/660)

20.60 In response to an RCAF request in 1961 for information on secure air/ground/air communications equipment, NSA offered the TSEC/KW-7 for Canadian trials, though this offer took some time to be implemented. The RCN also indicated an interest in trials of the equipment on ship/ship and ship/air circuits. The KW-7, developed under the name TRADER, is a transistorized, on-line, start/stop or synchronous, half-duplex teletypewriter security equipment designed for netted use over marginal tactical radio circuits as well as wire circuits. The cryptographic element is a 39-stage electronic key generator, with keying variables inserted by means of a plugboard or a punched key card. It incorporates the ORESTES cryptosystem and is cryptographically compatible with the UK BID/660 (PUGILIST). The KW-7 does not provide traffic flow security. It has been designed to minimize TEMPEST problems, and its modular construction, using printed circuit boards (500 transistors and 1,000 diodes), enables easy maintenance.

s.15(1) - DEF

s.15(1) - IA

20.61

20.62

20.63 Meanwhile CBNRC technicians were sent on training courses, and requests were made for KW-7 devices for Canadian trials. Competition for the few copies of the equipment available for trials was keen, as the USN and USAF extended their testing periods in efforts to determine the redesigning necessary to accommodate their needs. Procurement details were sought by CBNRC as NSA warned of approaching contract deadlines. The Canadian Services were anxious to place their orders for the equipment, but hesitated to do so until sufficient trials could be completed to enable them to have confidence that the KW-7 was what they needed. Four devices were finally obtained for Canadian trials. Engineering evaluation and laboratory testing were done at CBNRC, and familiarization courses were run for technicians of other departments. Tactical trials at sea and on landlines were conducted by the Services with no major problems encountered. (A CBNRC technician supervised the initial trials in Halifax because RCN personnel were unfamiliar with the equipment.) The CSPC approved the KW-7 for traffic of all security classifications on 11 September 1961, and NATO followed suit on 14 August 1963 (SGM 360-63).

20.64 On the strength of their experience in limited ship/shore and ship/ship trials, and with other testing still in progress, the RCN order for KW-7 equipment went forward in December 1962, with plans to begin use in early 1965. Deliveries were earlier than anticipated, however, and three RCN ships were fitted out in December 1963, and others in succeeding months. (KW-7 equipment was aboard the USS Pueblo when it was captured by North Korea on 23 January 1968, but Canadian traffic was not affected because different keying material was used.) In all, the Department of National Defence acquired 724 KW-7s, the RCMP 165, the Privy Council 14, and External Affairs borrowed two from DND. These quantities were still in use in the mid-1980s.

20.65

Page 1319

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

20.67 The RCMP soon learned that the British Security Service were planning to use TOPIC, and their interest also was aroused. As the period covered by this History drew to a close, External Affairs were negotiating the procurement of 144 TOPICs (down from an earlier intention to buy 300) at $20,000 each, over a three-year period, 1976-79. The RCMP bought two.

20.68 Following an informal enquiry from GCHQ, CBNRC Communications Centre considered the possibility of using TOPIC for special (e.g. "EYES ONLY") traffic to External, CANSLO/L, CANSLO/W and GCHQ as a replacement for ROCKEX. Because the amount of traffic involved with all these offices was small, CBNRC obtained only one TOPIC machine. Unfortunately, because of design changes, the version CB bought was not compatible with those at GCHQ. External had both versions, however, and were able to intercommunicate with GCHQ and CBNRC. As a consequence, the TOPIC at CB was not used with the CANSLOs, but only for messages for External that had to be double-encrypted - and ROCKEX had to be retained well into the 1980s until it was replaced by a NATO device (RACE).

Key Generators (KGs)

20.69 Every modern key generator cipher machine fielded since the late 1950s can be viewed as not much more than a special-purpose, hardwired computer with some programmability or variability to permit crypto set up and change of keys. An examination of the newer machines shows them to be progressively smaller, faster and more efficient. As the years passed, the role of the electronic key generator expanded in communications security. There are many factors responsible for this progress; among them are:

a) An increase in the number of communications systems requiring security;

b) The growing recognition of the value of COMSEC; and

c) The remarkable technological advances which have dramatically reduced the size and power requirements of crypto equipment.

20.70 The TSEC/KG-3 is a modularly constructed, transistorized key generator for the encryption/decryption of digital signals. With various conversion equipments the KG-3 will provide high-grade security for any digitalized type of communication at speeds up to 100,000 pulses per second; this includes facsimile, data, voice and multi-channel teletypewriter signals. The KG-3, with two key generators, is a half-duplex transceiver. The "receive only" equipment, with one key generator, is called the KG-12, while the full duplex equipment, a combination of KG-3 and KG-12, is designated as KG-13. They use the PONTUS cryptosystem. Variables are set by means of a punched key card.

20.71 The RCAF in 1961 were investigating ways of securing the logistics data circuits associated with their Air Materiel Command operations. As a trailblazer, they were watching closely USAF plans to use the KG-3 to provide an airborne, on-line cryptographic teletypewriter capability, and ultimately to provide crypto security for data and HF voice communications. Although the KG-3 was not originally designed for airborne use, modifications were introduced to enable it to operate in large aircraft. The KG-3 family of equipment would permit

s.13(1)(a)

s.15(1) - DEF

s.15(1) - IA

two-way communications at a much faster rate than any equipment available at the time, and could offer greater versatility in that facsimile, voice and data could also be passed.

20.72

20.73 A small number (15) of KG-3 devices had been specially modified for the USN to permit use of a clock start. These were designated KG-15. When the TOBACCO communications system was under development in the mid-1960s, CBNRC learned that the USN still held the KG-15s but were not using them. Five of the KG-15s were transferred to CBNRC on a long-term loan basis, and were used during the system-proving phase of TOBACCO. (The five devices were still held by S Group in 1985.)

20.74 In 1970 CFHQ asked CBNRC to enquire whether the KG-13 production line could be reactivated in order to provide approximately 500 high-speed on-line crypto devices for the SAMSON main line routes. However, on CBNRC's recommendation, the decision was made to use KG-34s rather than KG-13s for this purpose when SAMSON was finally implemented. Two years later CFHQ sought a loan of six KG-13 equipments and ancillaries from the US, to be used in a secure computer data system linking the Canadian east coast with two locations in Ottawa. The computer facility was to provide secure, on-line, data exchange between the NDHQ Data Centre and Maritime Command HQ, Halifax, and between the Data Centre and Defence Research Board (DRB), Shirley Bay. Because equipment in the KG-30 family would not be available by the planned implementation date, July 1972, DND wanted to borrow rather than buy KG-13 equipment, which would be replaced as soon as KG-34 equipment became available. NSA was unable to assist, because slippage in the KG-30 production program resulted in extra pressure on the KG-13 equipment supply situation, and there were no surplus equipments. By December of that year, however, sixteen KG-3 machines were obtained on loan from NSA; ten of these were serviced at CBNRC and transferred to DND; the remaining six were retained by S Group, CBNRC (and were still on inventory in December 1985, as were the 10 at NDHQ).

The KG-30 Family

20.75 The TSEC/KG-30 family of nine equipments (KG-30 to KG-38) are all miniaturized, serial-synchronous, binary, digital key generators for tactical use. With suitable ancillary equipment and external timing, the devices can provide security for all types of digital communications including speech, facsimile, data and multi-channel teleprinter. All KG-30 series equipments are cryptographically compatible with each other. Keying variables are inserted by setting a linear sliding permuting device in accordance with a key list. The cryptoprinciple uses an 81-stage stepping register, and the system was judged capable of providing security for all classifications until at least 2,000 A.D.

20.76

s.13(1)(a)
s.15(1) - DEF
s.15(1) - IA

20.77 DND had two very large programs looming in the late 1960s and early 1970s. In October 1968 enquiries were made as to the cost and availability of the KG-31 equipment, which was being considered for the TOBACCO communications system; this project involved the transmission of short bursts of on-line encrypted traffic in the HF range. By January 1970 the selection had changed to the KG-34, the fixed plant member of the KG-30 family, and five of these generators were ordered to serve as an integral part of the service test model phase of Project TOBACCO, with a further seven KG-34s to be ordered in 1972. S Group technicians were deeply involved with the testing of KG-34s in conjunction with TOBACCO between 1972 and 1975.

20.78 The second project was a much larger one - the Strategic Automatic Message Switching Operational Network (SAMSON), a program to secure DND operational and administrative circuits for data and telegraph communications. The plan was to use CID/610 on the "tails" and KG-34 on the "long-haul" circuits. DND initially estimated it would need 500 high-speed on-line crypto devices to satisfy the latter requirement. In January 1970 they ordered five KG-34s, and CBNRC/S Group ordered two KG-30s to handle CB's technical support role with SAMSON. In 1971 DND asked for cost and availability details for an anticipated order for some 300 KG-34s. In the following months they conducted a feasibility study on the use of the full duplex KG-34 and half duplex KG-36, and the ancillary equipment necessary to use these devices in Project SAMSON. The project was slow in developing. As a result they missed the production contract deadline; the price per unit increased, and in April 1972 DND trimmed their planned total requirement to 250. They ordered 75 more KG-34s in the next 15 months, enough for the first phase of SAMSON. In toto DND acquired 205 KG-30 family equipments for SAMSON and the DND Management Information System. They relied heavily on CBNRC technicians for the testing and installation of data links, especially in the new NDHQ building with its shielded enclosure (in 1974).

20.79 While DND were getting their act together, the RCMP ordered eight KG-30s. In 1974 they acquired another 60 units of the same device for use on high-speed voice and data circuits of their Security Service. In December 1972, CBNRC/R Group had also ordered two KG-34s for use on their SAMSON link. Then the Privy Council Office suddenly found a need for KG-30 equipment ("for the Prime Minister's Office") in 1974 and, like so many others, expected immediate delivery. Crypto equipment, however, cannot be bought off-the-shelf. The six KG-30s they requisitioned had to be made to order. Fortunately, CBNRC was able to borrow five of the devices from NSA to tide the PCO over until their own equipments were delivered. The PCO put them to work with DACOM 412 equipment to secure facsimile transmissions, with the help of CBNRC/S Group, who participated in the evaluation and testing of the DACOM 412 in Germany, developed secure interfaces, and assisted with the setting up of two nets - one for the secure facsimile and the other for the internal data link between the East Block and the Langevin Building and Postal Station B complex. Finally, the Department of External Affairs also invested considerable funds in this family of key generators (77 KG-30s and 30 KG-34s) for use with their missions abroad.

Speech Secrecy Devices

20.80 The demand for ciphony (secure speech) equipment has always been strong, but development problems plagued the designers and seemed insurmountable at times. In the spring of 1948 the Security Panel considered the feasibility of installing telephone scramblers for interdepartmental use. CBNRC was asked for an assessment of the degree of security which might be expected and an indication of what was entailed.

20.81 CBNRC's first COMSEC engineer, Ed de Grey, had said in a 1947 report that secure speech was still in the "bright idea" stage. To be sure, there were some voice scrambling systems in existence, but they offered no security whatsoever, and only served to prevent eavesdropping by the general public. Many proposed systems did not "encipher" speech in the true sense, but merely involved speech inversion or continuous variation of the carrier frequency on which the speech was transmitted, so that unravelling the signal was more of an engineering problem than a cryptanalytic one. CBNRC asked GCHQ to confirm Mr. de Grey's assessment and they replied: "the type of scrambler now in use operates on simple frequency inversion using 2600 cycles .... It is not regarded as providing any security except against casual overhearing and eavesdropping. Equipment is now available to the public in UK on hire from the GPO .... Practice has shown that switchboard operators who hear a good deal of scrambled conversation in the performance of their duties are, after a time, often able to reconstruct a high percentage of the scrambled conversations they overhear, without the aid of any unscrambling equipment." The scrambler was used to a large extent by the UK Foreign Office for internal and interdepartmental use in London "but full regard was paid to the limited security rating given the system". In the US as well, scrambler telephones were only authorized for information no higher than CONFIDENTIAL. The UK acknowledged that the provision of a secure scrambler telephone was an urgent requirement of ever-growing importance, but emphasized that no properly secure speech secrecy system had yet been devised (October 1948), nor could one be envisaged. The search for a secure apparatus for landline telephones presented enormous technical difficulties. By 1951 the requirements were being defined, but progress was inhibited by practical and fundamental technical limitations.

20.82 In the early 1950s, the RCAF undertook the development of a speech secrecy device to which they gave the name SEASHORE. It was examined cryptanalytically by GCHQ and assessed as impractical; as a consequence, radical changes were incorporated. The device used a type of "keying plate" which was scanned and which acted as the scrambling and descrambling element in the system. CBNRC completed an evaluation report on SEASHORE in January 1953, based on theoretical study only, because the Branch had no machine aids for practical testing. The report found basic security flaws in the system. CB told the CPC in April "to obtain a more specific and detailed evaluation, it would be necessary to refer to an organization with more extensive facilities and analytical machinery". Subsequently, NSA began an evaluation of SEASHORE in May 1953. A preliminary investigation discovered weaknesses in all three types of proposed key generators, which would indicate that security protection even for a matter of hours was unlikely. Further study confirmed that

SEASHORE was susceptible to cryptanalytic attack. The project was therefore abandoned.

20.83 Discussion of the CBNRC evaluation report on SEASHORE inspired suggestions that there was a need for a highly specialized evaluation capability, and for a Canadian organization which could develop and produce cipher equipment, especially since the supply of such equipment could be suspended in an emergency. Other government agencies began to be involved. The CPC at its 20th Meeting on 5 February 1954 expressed criticism of a Defence Research sponsored project as "a speech privacy system only, the security of which did not approach the lowest limits set for true speech secrecy". The Chairman noted "that it was quite apparent that considerable waste of public funds resulted from grants being made for projects which had not been considered by competent authorities". The Committee agreed "that CPC approval should in all cases be obtained before the expenditure of funds for the purpose of any form of crypto development was authorized".

20.84

20.85 Meanwhile the US and UK were pushing ahead with experiments in an effort to develop speech secrecy equipments to meet the various needs being defined. A US/Canadian Communications Security Conference was held in Washington on 17-19 November 1952, during which developments in all fields of crypto were discussed. Ciphony devices included systems based on many different principles, e.g. some with cipher text auto-key and some with vocoders. Those intended for tactical use - for VHF and UHF - were reasonably priced, but those designed for long range high echelon use were either extremely costly (estimated at about $300,000 per unit) with good quality speech, or "moderately expensive" (about $60,000 to $80,000 per terminal) where the quality of speech was sacrificed to the extent that "adverse psychological factors came into play". By 1959 the average cost per terminal was estimated at about $123,000.

20.86 In August 1954 NSA informed CBNRC that the US had no secure speech equipment available for purchase. Several equipments were under development but none had reached the production stage. No commercial developments were satisfactory from a security viewpoint. "Protected" telephone systems in use which did not employ cryptoprinciples attempted to provide security through physical separation from other communications systems, and through physical protection afforded to their lines. An internal system being installed at NSA involved complete shielding to prevent cross-feed between "red" (internal to the building) and "black" (commercial telephone company) phones.

20.87 NATO, too, was expressing concern at the general lack of telephone security. A meeting of the European (later called Allied) Communications Security Agency (ECSA, now ACSA) in July 1955 called for measures to protect classified communications, by avoiding references to sensitive information, or by adopting countermeasures to prevent attacks on telephone lines, either by physical sabotage against installations or by the exploitation of transmissions. Among the remedies advocated were the use of privacy equipment where the requirement was simply to guard against casual eavesdropping, and secrecy equipment where a vulnerability to interception by hostile agencies was known to exist.

20.88 With the introduction of the transistor in the late 1950s, electronic security rapidly took hold in COMSEC. In the succeeding years NATO countries other than the US and UK - especially France, Italy, the Netherlands, Norway and West Germany - were underwriting crypto equipment developments in an effort to corner a part of the NATO market for COMSEC devices. Normally, this would not affect Canada, because Canadian policy dictated that crypto equipment used to protect classified information would be restricted to devices developed by the UK or US Governments, unless otherwise specifically authorized. Exceptions, though rare, were made, as in the case of the Norwegian ETCRRM[13], but it would not be until 1972 that a speech secrecy device developed by a country other than the US or UK would be installed and used in a Canadian Government office.

20.89 To meet an urgent requirement by the RCMP for security for voice transmissions on mobile radio nets, CBNRC decided to try its hand at developing ciphony equipment. With no engineering facilities, efforts had to be limited to theoretical development. A system of processing speech by a complex random conversion technique was proposed in 1958-59 to provide a high degree of privacy until quality speech security equipment would become available - expected around 1962. It was evaluated by GCHQ/LCSA as inadequate. The idea itself was good, involving as it did the latest semi-conductor techniques, but without practical facilities CBNRC had no way of developing the concept. The RCMP, however, themselves proceeded to experiment with privacy equipment. A device called HOMER/BRAUN (probably after Corporal Braun, a cipher specialist with the RCMP) was used for a short time. It was apparently a modification of a commercial equipment developed by Motorola. CBNRC examination of HOMER/BRAUN found that it was very transparent, and probably more dangerous than plain language because it gave a false sense of security and was relied on too heavily. However, an improved version of HOMER/BRAUN was evaluated by S Group in May 1974, and found to provide some short-term protection.

PICKWICK

20.90 In 1957 the COMSEC Community undertook to develop a long-term Canadian crypto equipment policy, culminating in CSB/79 of 31 December 1958, which provided guidance for the next fifteen years. The paper noted "To date neither the Services nor the civil departments have had any experience in the employment of speech secrecy equipments". Although

[13] See para. 20.43

s.15(1) - DEF

s.15(1) - IA

crypto for all forms of communication was in demand, progress was being made in the protection of teleprinter messages, whereas the main deficiencies were in the speech, facsimile and data transmission fields, where development was lagging seriously. GCHQ had been active in these fields, and had provided information to CBNRC as early as 1954 on secure telephony devices such as PICKWICK, and facsimile crypto such as MOUNTEBANK. By the early 1960s Canada had shown considerable interest in PICKWICK, a start-stop, cipher text auto key system (designed for wideband circuits) that provided good quality speech on lines of less than twenty miles. The Privy Council (the Prime Minister and Cabinet) were considering the possible establishment of a local area PICKWICK net to include 13 or 14 subscribers. The cost was the major stumbling block; although the initial capital cost of PICKWICK had dropped to an estimated $10,000 (and was expected to go lower), the high recurring costs involved in the rental of special wideband (10 Kc), or four normal (3 Kc) Bell Telephone wire circuits put the damper on the project, especially in view of the government austerity program in effect at the time. Another consideration, too, was the need for compatibility, in case in the future local secure telephone nets and secure long distance telephone circuits involved US-developed speech security equipment. In the event, no PICKWICK devices were purchased by Canada.

20.91

KY-3

20.92 The KY-3 is a wideband, full duplex, single-channel, transistorized, digital speech security equipment. Like PICKWICK, its range is limited to 20 miles. For operation over long-distance circuits, it requires a wideband carrier, or conversion to a narrow band signal by means of the compatible HY-2 ancillary device. The KY-3 uses the TROILUS cryptosystem, and keying variables are inserted by means of a punched key card. The KY-3 was designed to provide secure facilities for short-haul, urban-type networks because of the cost of the wideband circuits required. It was approved for passing Canadian national traffic at the 61st CSPC Meeting on 6 December 1963.

20.93 CBNRC ordered two KY-3 equipments in 1965 to set up an experimental circuit, and to provide S2 staff with experience in the use of ciphony equipment. This was a fortunate move, because urgent requirements were being raised for such equipment. In January 1965 a call came for a special channel between CBNRC and the Joint Intelligence Room at NDHQ; by March of that year planning was underway for circuits interconnecting "special purpose terminal equipment" located in three separate offices: External Affairs in the East Block, NDHQ at Cartier Square, and CBNRC; and before the equipment arrived, CB decided to give top priority to a secure speech link between CBNRC and RCMP Headquarters. The two KY-3 devices cost CBNRC just over $5,000 each, and were installed in November 1968 on the CB-RCMP link. NDHQ and External vacillated in placing their orders for KY-3 equipment; when they finally were ready to purchase, the production line had run out, and no new contract was to be let. In the next ten years, despite pleas from Canadian and American agencies for hundreds of KY-3s, no more were in fact produced. The agencies had waited too long, and it would have been much too costly for the manufacturer to tool up again and revert to producing the equipment.

20.94 The previously stated requirement for a circuit for the Prime Minister in Ottawa to talk to the President in Washington could not, therefore, be filled by Canadian-owned KY-3s, and once again we had to borrow equipment from the US. Fortunately the USAF were able to provide equipment for this purpose. In all, NDHQ were able to borrow eight KY-3s from the USAF. They were still on inventory, as borrowed equipment, in 1985.

DELPHI (BID/150)

20.95 Meanwhile the US and UK were also devoting their attention to the protection of tactical voice circuits. Because speed and simplicity are paramount in combat situations, and the information being transmitted needs only short-term protection, security is often secondary to expediency. Paper codes, which give a few hours protection, were usually used to disguise all or part of a transmission. In some cases simple devices, such as circular or linear slide-rule-type codes, were employed. There was continual and insistent demand, however, for speech secrecy equipment. GCHQ began tests of its DELPHI (BID/150) equipment in 1959, and CBNRC conducted trials the following year. It was a fully-transistorized, single channel, push-to-talk high-grade system. Its key generator was of the cipher-text auto key variety, employing three shift registers. It provided excellent quality speech and high-grade security. Keying variables were inserted by means of a punched key card. Beginning in 1965, DELPHI was used by the Fourth Canadian Infantry Brigade operating with the British Army of the Rhine (BAOR) in Germany, using compatible radio sets. Keying material was provided by GCHQ. The BID/150 equipment formed part of the BRUIN program, which was the BAOR tactical communications system for low echelon use (division and below).

20.96

s.15(1) - DEF
s.15(1) - IA

DAKOTA (BID/200)

20.97 The Canadian Brigade in Europe also had experience with another UK-developed equipment, a six-channel, duplex, speech secrecy device called DAKOTA (BID/200). It was designed for use over wideband UHF radio links. The equipment was on loan from the UK. Consideration was given in February 1969 to purchasing one unit, but it never came into use in Canada.

NESTOR (KY-8/28/38)

20.98 The US developed the NESTOR cryptosystem for use in low and medium echelons with VHF/UHF radio sets. It was incorporated in three cryptographically compatible devices: KY-8, KY-28 and KY-38. All three versions are wideband, half-duplex, transistorized, tactical speech security equipments; keying variables are set from a key list. They are operationally equivalent to, but not cryptographically compatible with DELPHI. (Although the UK favoured a common system, the US said they were not interested in a combined system at this level.) CBNRC bought two KY-8s for laboratory testing and for demonstration to potential users. This model is somewhat larger than the other two versions.

20.99 The war in Vietnam gave new emphasis to the need for protecting tactical communications, and added impetus to the effort to meet the need. What was required was a device that would be small and light, but rugged enough to survive the rough handling in battle conditions. DELPHI, used by the British and Canadian forces in Germany, weighed 23 Kg (50 lb.). The US developed a microminiaturized version of NESTOR, the KY-28, for airborne/shipboard communications, with integrated circuits and multilayer printed circuit boards designed for use with a large number of AM/FM radio systems, including the radio used with DELPHI. The KY-28 weighed 8 Kg (17 lb.). The US also produced an even smaller version, the KY-38, a manpack (portable) model, which could also be mounted in vehicles. It weighed only 7 Kg (15.5 lb.).

20.100 Thousands of these NESTOR equipments were manufactured exclusively for US combat forces in Vietnam (the USAF alone held almost 14,000 copies), and the Canadian Forces at first were unable to place orders for them. However, as the US Forces began their withdrawal from Vietnam in 1970, a large inventory of equipment became available, some new, some used and reconditioned. This was mainly due to the redeployment of US Forces, but also partly because of the potential availability of the next generation of speech secrecy equipment (SAVILLE family) in the 1971-74 time frame. Accordingly, the Canadian Forces ordered 56 KY-28s in April 1970, and by December were planning for 500 to 800 more. NESTOR had proven very reliable, and was tremendously popular, so that instead of carrying through with earlier plans to "unload" part of the inventory, the US Services decided to deploy the equipment to their units throughout the world. As a result, demand grew, and production of the KY-38 was resumed in 1971-72, and of the KY-28 shortly thereafter. This was helped along by slippage in funding for the development of the next generation of ciphony equipment.

20.101 In view of these new circumstances, DND requested price and availability information on 872 KY-28s and 681 KY-38s. When procurement details were received, a Program Change Proposal was approved by DND and the Treasury Board, and an order placed for 283 KY-28s (ship/airborne fitment) and 776 KY-38s ("tracked and wheel" fitment) in November 1971. The timing of the order enabled DND to save about a million dollars (down from 5-1/2 million to 4-1/3 million dollars), because the increased Canadian procurement coincided with larger US Service orders and a better price was negotiated. The RCMP also acquired a dozen KY-38s. It is interesting to note that ten years after the end of the period covered by this History the Canadian Government still held 1,129 NESTOR equipments on inventory. Even though NSA referred to NESTOR as "obsolescent" equipment because production had ceased in 1975, it still saw many more years of service even in the US. The USAF regarded SAVILLE (referred to above as the next generation of speech secrecy equipment) as "only marginally better than NESTOR". They pointed out that NESTOR had proven very reliable, and that SAVILLE offered no improvement in speech quality and only slight improvement in synchronization time, and offered no solution to bandwidth problems. The USN supported this stand.

ELCROVOX

20.102

s.15(1) - DEF

s.15(1) - IA

Privacy Equipment

20.103 Many government agencies expressed a need for a low cost "black box" which would provide a modicum of privacy. There were many topics whose sensitivity did not warrant the expenditure of large sums of money, but needed some protection from the casual listener.

Identification Friend or Foe (IFF) Equipment

20.104 On behalf of the RCAF, CBNRC asked NSA in April 1958 for information on the KI-1 equipment. This was a device designed to encrypt IFF information, a system used to identify friendly aircraft, and to provide security against hostile aircraft masquerading as friends. A modularly constructed, transistorized cryptosystem, the KI-1 would encode and decode interrogation and response signals of the MARK XII IFF system. It was succeeded in 1966 by the KI-1A, a microminiaturized device using monolithic integrated circuits as logic elements. Keying variables are inserted by setting a special multicontact switch with a code changer key. The KI-1A was approved for Canadian use at the 65th CSPC Meeting on 12 March 1968. (As of 24 March 1975, it had not been released to the UK.) DND acquired the KI-1A for use in ships and aircraft. In 1975 the Canadian Forces held 12 of the KIT-1A (Transponder Computer) - 6 owned and 6 on loan from the USAF; and 64 of the KIR-1A (the Interrogator Computer) - 22 owned and 42 on loan. Later they bought hundreds more of each.

20.105

s.15(1) - DEF

s.15(1) - IA

20.106 CBNRC and the RCN ran tests using the KL-4, and were favourably impressed. The USN had mixed views, and a controversy raged pro and con between 1959 and 1961 over its proposed adoption; in the end the decision went in favour of the device, and the RCN ordered 308 KL-4s in March 1961. The device replaced the CSP 1750 in the RCN in January 1966. However, considerable opposition to the use of the KL-4 continued in the USN, and a proposal was made in May 1970 that it should be withdrawn from combined use and the CSP 1750 reinstated. CBNRC trials showed that in normal PENELOPE usage the KL-4 was faster and easier to use where there were many call-signs to be encrypted/decrypted, but when only a few call-signs were involved it was much faster and easier to use the CSP 1750 than to have to set up the KL-4 with keying material, and then process the call-signs. The KL-4 was used by the RCN until it was withdrawn from service in 1975.

Authentication Devices

20.107 Because imitative deception played a role in communications, both military and civil authorities had a requirement to establish the authenticity of transmissions. Usually this could be done by some simple process involving elements at the beginning of each message. There was, however, also a need for challenge and reply authentication, e.g. when an aircraft wished to land at an airfield during wartime. Authorities wanted a common authentication system for all purposes, and efforts were made to provide a simple standard device. Circular slide-rule-type contrivances were most commonly proposed, but these were found to offer little security. Small battery-operated (or dynamo-operated) devices, such as the KL-98 and KL-15, were offered by NSA, but were rejected on the grounds that they required too much manipulation for a pilot in the dim light of a single-seater aircraft flying at tree-top level at high speed. The most successful and most widely-used authentication system was TRITON, which used a grille with tiny windows exposing letters printed on a key list. The key list usually changed every six hours and provided 1,296 potential challenges, each with twelve possible replies. With the widespread use of on-line crypto, the need for message authentication declined. Similarly the use of IFF equipment in aircraft lessened the need for challenge-and-reply authentication.

Evolution of Equipments

20.108 Thus the use of equipment to provide security for communications progressed from the very simplest to the extremely complex. Paper codes were replaced in some instances with sliding devices and grids. Mechanical contrivances gave way to electromechanical devices, usually employing rotors, with plugboards and switches. Thermionic tubes ushered in a series of electronic equipments in the 1940s reducing transmission delays by means of on-line operation. The introduction of transistors in the late 1950s made possible rapid strides in the crypto security field. With the coming of integrated circuits in the 1960s, the security of communications improved dramatically in performance and cost. By 1973, US and UK COMSEC specialists were making use of metal oxide semi-conductor chips and large scale integration techniques, which enabled them to produce a crypto package no larger than a pocket novel; in

1975 NSA was demonstrating BANCROFT (a member of the SAVILLE family), whose crypto component occupied a space measuring one by four by six inches, and contained an analog-to-digital converter, a key generator, and storage and controls for three days' key. By the end of the period covered by this History, these devices, which could be keyed by daily fill material in electrical form, and even electronically from a remote location, were being tested for use in the following years.

20.109 Information on the SAVILLE family of equipment[14] - LAMBERTON, VINSON, BANCROFT and PARKHILL - was provided to CBNRC as early as 1967, allowing the Canadian Forces to begin planning for their use. DND were negotiating to purchase 200 to 400 PARKHILLs (a narrow band, analog speech security equipment for HF radio circuits) and 2,500 to 3,500 VINSONs (a wideband, digital speech system for VHF and UHF nets) in 1974 and 1975, but were experiencing great difficulty in obtaining funding.

20.110 The search continued for a device to protect telephone conversations at a reasonable cost. The major US development was BELLFIELD, which passed through various stages, as NSA sought the most efficient combination of components: speech processors, modems, key generators, key distribution systems and terminal subscriber units. It was a program to develop a narrow band, digital, full-duplex secure voice equipment for use with switched systems. The first usable version was the KY-70, produced in limited quantity and reserved for US Government use. The KY-71, of which CBNRC/S Group bought two copies, and subsequent versions, were considered the answer to the Canadian Government's secure telephone requirement, but progress along this line did not occur during the period of this History.

[14] See para. 20.100

Chapter 21

Evaluation of Crypto Equipment

Chapter 21 - Evaluation of Crypto Equipment

Requirements and Procedures

21.1 The need for a Canadian capability to evaluate, or at least to produce independent, comprehensive security assessments of, various types of crypto machine systems, particularly 'commercial' systems, was appreciated in the initial stages of the development of COMSEC in Canada. Cryptosystem evaluation is a highly specialized area requiring extensive special purpose laboratory resources, which are normally available only in national COMSEC agencies. This is a prime responsibility of such an agency, and could not be done effectively or conveniently by individual departments. The question of producing crypto equipment was also raised from time to time. Both undertakings, however, would be considered in-depth, papers would be written summarizing the results of studies, conclusions would be reached and recommendations made, but regularly the cost of such projects caused the authorities to defer the proposals "for the time being". All agreed that production in Canada was desirable, but the extent of the requirement would determine whether or not it was feasible. The production of Crypto Equipment in Canada will be covered in Chapter 22.

21.2 Every year CBNRC, as the Canadian COMSEC Agency, was called upon to evaluate several inventions submitted by members of the public in Canada and elsewhere. Most of these were ridiculously simple, while a few were so complex as to be completely unwieldy. They would vary from unsophisticated codes and disguise procedures, through transposition and movable strip systems, to on-line non-synchronous rotor-maze machines and speech scrambler devices. Many were interesting, but all so far submitted possessed weaknesses - none have offered sufficient security protection for government communications. Several authors have made astonishing claims for their inventions, and a few have become markedly antagonistic when their offerings were politely declined. This is a very delicate area, since, although it is highly unlikely that someone "out there" will discover a concept that has not been considered by Canadian, US, UK or other Allied government crypto specialists, certainly no one would completely discount such a possibility, or take a chance on passing up an idea that might be offered to a rival or potential enemy. All proposals must be given fair consideration, because most of them come from honest individuals, although some "cranks", "crackpots" and mischievous persons also make submissions. By proposing "inventions" with known weaknesses, for instance, it would be possible to test (for intelligence purposes) the expertise and capabilities of government specialists and, at the very least, to tie up otherwise needed facilities. The submissions were usually made to DND, RCMP, External Affairs or Members of Parliament, and were then passed along to CBNRC for evaluation. Procedures for dealing with crypto inventions were developed by the Cipher Policy Committee (CPC), and revised as capabilities developed and responsibilities shifted. Originally, all crypto inventions were to be passed to the Office of the Deputy Minister of National Defence and referred to the Joint Telecommunications Committee (JTC) (of DND). In 1953 the CPC published a paper (CSG Paper No. 9/53, CPC Paper No. 6), later superseded by CPC/P/15/55, which prescribed that civilian departments should forward invention submissions to the Security Panel, who would initiate a standard interim reply and refer the submission to the Secretary of the CPC; similarly DND would pass the submission to the Inter-service Committee on Inventions, who would also initiate a standard interim reply and refer the submission to the Secretary of the CPC; the latter would arrange for a security evaluation, and report back to the Security Panel or the Inter-service Committee on Inventions, as appropriate, who would then inform the inventor of the extent of the Government's interest in the device or idea. Invariably the reply would thank the individual, but add that the Government had no requirement for such an item at the present time.

21.3 At its 15th Meeting on 10 August 1954 the Communications Security Board (CSB) considered CPC Paper No. 8, which proposed, among other things, the establishment of a cipher evaluation group. The Board left the paper with the CPC for further consideration but agreed "without our own evaluation facilities, however, we must accept UK or US evaluation without question". Overall Canadian Cryptographic Policy, as first enunciated in this CPC Paper No. 8, went through various revisions, eventually emerging as CSC/P/2/72 in September 1972; all versions required that classified information be encrypted in an "approved" cryptosystem. The 1972 paper further stipulated: "All systems used for the encryption of national traffic must be approved by the National COMSEC Agency. Such systems shall be of Canadian, US or UK Government origin except as otherwise authorized (e.g. for NATO purposes)." These provisions had, in fact, been applied since 1948, and as cryptography became ever more sophisticated, CBNRC sought to enhance its evaluation capability.

21.4 CPC Paper No. 8 had also recommended hiring from the UK one mathematical cryptanalyst and one cipher development engineer. By late 1954 it was apparent that GCHQ could not release such experts, due to pressure of work. At the 26th CPC Meeting on 5 November 1954 it was noted that it would take 5 to 10 years for CBNRC to train staff and to get started on cipher evaluation and/or development. Training of specialists could begin by integration with NSA and/or GCHQ. Discussion indicated that "the present requirement is to do re-evaluation of allied machines (UK and/or US) only, and not development". GCHQ and LCSA were asked to recommend a high-speed analytic machine, "a general purpose electronic computer" for CBNRC's proposed evaluation unit. GCHQ had "two Robinsons and two Collossi", old wartime rapid analysis machines, but was in the process of assembling a large general purpose computer for solving mathematical problems arising in connection with cipher machine development. In reply to CBNRC, LCSA "made it clear that it was useless their setting up an evaluation unit until their SIGINT organization advanced a long way beyond low and medium grade cryptanalysis". The Director GCHQ pointed out that any such venture must be a long-term plan, as a large computer would require, "apart from engineers to service it, operators to run it and cryptologists to set it problems ... five trained programmers to write enough programs to keep it busy one shift a day" ... and was likely to cost a million dollars. The cost of building such a device, or of purchasing an IBM computer similar to one used at NSA, was too great for CBNRC to consider, and no further action was to be taken until two or three specialists could be trained and had acquired several years experience.

21.5 Undaunted, the CPC prepared a new paper, CPC Paper No. 14/55 (CSB 41), dated 25 January 1955. It concluded that the establishment of a crypto evaluation unit in CBNRC was a "feasible and worthwhile undertaking". It recommended that personnel such as "Ph.D. mathematicians" should be sent to GCHQ for training. (An electronics engineer, G.R. McCully, had been hired in June 1954 to establish an evaluation and development facility. He was sent to GCHQ in January 1955 for training, but unfortunately he resigned from the Branch in October of that year.) The CSB, at its 16th Meeting on 16 February 1955 considered CSB 41 and agreed "to authorize the Director CBNRC, to build up a crypto evaluation unit", but "to defer a decision on the purchase of high-speed computing and rapid analysis machinery". However, little progress was made in the next few years toward establishing a Canadian Crypto Evaluation Unit because of the inability to recruit staff with the appropriate qualifications.

21.6 In 1957, Mr. Drake visited GCHQ and reported: "that Agency had recommended that the proposed (Canadian) cipher machine evaluation efforts should be diverted to COMSEC evaluation generally." One reason given for this proposal was that the existing UK/US combined effort on cipher machine evaluation provided for the necessary recheck on security assessments. Although this did little for the cause of establishing an evaluation capability at CBNRC, the CPC "agreed that the GCHQ proposal appeared to have merit".

Page 1349

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

s.15(1) - DEF

s.15(1) - IA

Efforts to Establish Evaluation Capability

21.9 As the workload involved in the production of CID/610 wound down, attention could be diverted back to the need to evaluate crypto equipment. The establishment of a crypto evaluation unit in CBNRC had been judged a feasible and worthwhile undertaking, although it had been agreed to defer indefinitely a decision on the establishment of a cipher machine development unit. The cost of building up a staff which could design and develop crypto equipment was considered too great even to contemplate, but it was thought that two or three mathematicians and engineers could be acquired and given the task of evaluating crypto devices placed on the market by commercial firms. Various government departments, enticed by advertising brochures which promised absolute security for a few hundred dollars, questioned the need for COMSEC approved equipments costing thousands of dollars. Such commercially-developed cipher machines must be examined and evaluated by competent authorities to determine whether they provide adequate security protection and, if not, potential users must be warned against them. The false sense of security engendered by the use of a cheap but insecure device encourages communicators to place too much reliance on the system and this, in the long run, is worse than no security measure, because then at least the user is aware of the vulnerability and will take less risk. For this reason Canadian Government policy requires that classified information to be transmitted by electrical means must be encrypted in a cipher approved by the National COMSEC Agency[1].

21.10 In CB, Gord Thomson had been striving to expand the technical engineering and evaluation capabilities of the Test and Design (T&D) Group, assisted by Vic Williams (1951-1969), Ferdy Laporte (1948-1977) and Al Joyce (1948-1979). Mr. Williams, however, had been engaged nearly full time in the design of equipment to produce and check keying material. And Ferdy Laporte and Al Joyce, together with Baxter Smith and Lyn Mulligan, were fully occupied with providing support and assistance to the Services, RCMP and External Affairs in the secure use, maintenance and modification of the various cryptosystems. Later, when T and D Group was divided in February 1964 into T Group, responsible for the production of keying material, and S Group, charged with COMSEC engineering, it was hoped that the new S Group Head, Don Fairley, would be able to embark at last on an evaluation effort. However, the burgeoning

[1] See para. 21.3

responsibilities associated with TEMPEST and with the production of CID/610 made it impossible to devote any of the 27 persons on S Group staff to evaluation. During the next few years, S Group was also involved in conducting operational trials of crypto equipment, including tactical voice equipment planned for use by the Canadian Forces and the RCMP (e.g. TSEC/KY-8-28-38), and in developing keying material production equipment (e.g. a Canadian solid-state version of the UK designed vacuum-tube-operated DAUPHIN system).

21.11 During a reorganization of S and T Groups in September 1971, when Ken Hughes transferred from T5 to S1, he brought with him the responsibility for COMSEC Doctrine, and immediately launched a campaign to establish an evaluation capability. The primary responsibility for the evaluation of cryptosystems was assigned to S Group. Specific reference was made to commercial and non-Allied government systems: "If equipment is of non-US or UK government origin ... S Group is to ... conduct an evaluation of the cryptoprinciples employed in the equipment and form an assessment of the security depth afforded ... and conduct a TEMPEST evaluation of the equipment." However, lacking a proper evaluation capability, when asked about the protection provided by a commercial cipher device, CBNRC would have to seek assistance from NSA or GCHQ, who might or might not have already assessed that particular product. Thus the advice that CB was able to give was more or less "second-hand". Even the assurance that Canadian Government classified communications could not be exploited, because we made our own keying material, was based upon assurances received from the US and UK.

Assessments of Specific Devices

21.12 Several commercial crypto devices, in which certain governmental departments expressed an interest, were, in fact, given COMSEC assessments. In each case all technical security features of the equipment were considered, but a rigorous mathematical analysis of the security of the key generation could not be done because facilities for such a procedure were not available. Such factors as security alarms, integral physical security and TEMPEST integrity, including cipher signal modulation, were assessed. A comparison would be made, for example, of the COMSEC features of an approved secure speech equipment with those of the device submitted for examination. Before the evaluation was returned, it was sent to NSA for a critique and in every instance the CBNRC conclusions were confirmed.

21.13 Evaluations of submissions by private individuals or by commercial firms had been made in the late 1940s by T&D with considerable assistance from the "SIGINT side of the house", and occasionally by reference to GCHQ or NSA if the inventor was not in Canada. As T Group staff developed more expertise they took on full responsibility for the assessments during the 1950s and, of course, when S Group was formed the task fell to its staff if a device was involved, although paper systems continued to be dealt with by T5 until COMSEC Doctrine was transferred to S1 in 1971. In many cases, SIGINT assistance continued to be obtained from O Group. During the 1960s S and T Groups ran tests of various crypto devices offered by NSA (e.g. KW-37, KW-7, KL-4, KG-14, KY-8-28-38) and by GCHQ (e.g. SINGLET, PENDRAGON, RALEIGH, ALVIS), coordinated the Canadian trials of each, and approved them for use for the protection of Canadian Government classified communications. This activity continued in the 1970s, and, in addition, operational evaluations and qualitative appreciations continued to be performed on many commercial equipments (such as Datacoder and Speakerphone). When S1 established an Evaluation Unit in 1974, and later when S5 was set up as a full-fledged Evaluation Section, S Group was able to complete its own evaluations. Submissions continued to be received, perhaps five or six each year, from individuals and small commercial firms, mostly via DND, and occasionally through External Affairs. Now that the organization is known as the Communications Security Establishment, some submissions are made directly to CSE.

s.15(1) - DEF

s.15(1) - IA

Evaluation Re-examined

21.14 In June 1972, Art Browness, Assistant Director COMSEC (AD/C), in a memorandum to the Director, proposed the "establishment in Canada of an evaluation capability, not necessarily as a prerequisite to development, but primarily as a means of properly performing cryptographic and/or cryptanalytic assessments, including independent security analyses of cryptographic keying material". He advocated recruiting three people: one senior mathematician, one cryptanalyst and one 'electronics-mathematics' engineer, to be integrated within GCHQ for a two-year training period. Regarding the acquisition of appropriate computer facilities, he referred to an earlier suggestion that a computer installed in the University of Toronto be used on a part-time basis, as an alternative to the procurement by CB itself of rapid analysis equipment or a general-purpose computer. Efforts to recruit satisfactory personnel and to obtain access to such analytical equipment had in the past proved unsuccessful. Mr. Browness sought to have the question of establishing an evaluation facility re-examined. A decision on the proposal was deferred because of the "uncertainty of the situation about the whole SIGINT/COMSEC program in Canada". Thus after 25 years CSE was still attempting to develop an evaluation capability, but was still being frustrated by the cost of such an undertaking. As early as 1948 the terms of reference of the COMSEC Agency had included responsibility for examining and reporting on the security of codes and ciphers and carrying out "research into the design, development and production of cipher machines, cipher systems and other security devices"[2]. Again in 1955 the CSB, while deferring a decision on the development of cipher machines, had authorized the Director CBNRC to build up a crypto evaluation unit.

21.15

[2] See Annex 17.A

Tentative Beginnings and NADIR

21.16 A cryptanalyst/mathematician, Marla Cooper, was seconded from O Group to S1 in July 1973. George Dawson, who had been intimately involved in the Canadian production of ALVIS, had been acquired from DND in October 1972. These two organized the first stages of an evaluation unit in July and August of 1973. In preparation for the project, Marla Cooper visited NSA for three weeks from 25 February to 15 March 1974, "To absorb all available information on the theoretical and practical approaches to the evaluation of speech privacy devices and key generators with a view to the establishment of an evaluation unit at CBNRC". Events were militating against the project, however: Mr. Hughes, who had adopted it as his main objective, and had sought out and prevailed upon Marla Cooper to lend her extensive resources to the undertaking, was appointed to the D/CANSLO/C position and left for NSA in July 1974. In addition, other tasks were assigned a higher priority.

21.17 Almost coincidentally with Mrs. Cooper's secondment, the RCMP in August 1973 requested CBNRC to participate in what they termed a "feasibility study", but which broadened into a development project that tied up CB's evaluation staff for the next ten years. This was Project NADIR. In a last-ditch effort to prevent the NADIR project from aborting once again the infant evaluation unit, S Group formed a Cryptographic Evaluation Panel with representation from the "other side of the house", viz. one each from the cryptanalytic, SIGINT engineering and computer areas as well as from S Group itself. The panel endured for only a few months, however, as NADIR gathered steam, because only two people were available for either evaluation or development, and the latter was given priority.

The Final Stages

21.18 At this point another paper was produced, CSC/P/4/74, entitled "Cryptographic Evaluation - Canadian Capability". It was considered at the Meeting of the Security Advisory Committee (SAC) on 21 May 1974. The Committee agreed that the Treasury Board should be made aware of the high priority which the SAC attached to the establishment of an in-depth crypto evaluation capability. Mr. Dawson and Mrs. Cooper were soon deeply involved in the NADIR feasibility study. Unfortunately, Mr. Dawson transferred to the Department of Communications in September 1974. Nevertheless, S Group was very fortunate in acquiring a young engineer, Milan Kuchta, in June 1974; he had begun research into the use of fibre optics in COMSEC, but was then diverted to the NADIR project (which occupied most of his time for the next ten years). Mr. Kuchta, with the assistance of bright, forward-looking mathematicians, engineers and technologists, developed an Evaluation Unit that won the admiration of both NSA and GCHQ. First, however, they had to devote their efforts to NADIR and related projects.

21.19 Thus the evaluation effort never really reached fruition during the period covered by this History. Each time a start would be made, the personnel were appropriated for other purposes. Nevertheless, the requirement for a capability to evaluate crypto devices grew in importance until it would not be denied. As Canadian industrial firms entered the crypto equipment production field, and as foreign firms sought to export crypto equipment via Canada to countries prohibited by their own authorities, CBNRC/CSE was forced to provide expertise in the area. S Group had to provide advice, and to assist the CSC in the development of a policy on Canadian Production and Export of Crypto Equipment. The problem at issue was the extent to which CBNRC should become involved with commercial firms engaged in the production of crypto equipment. A paper was drafted proposing several options for the various degrees of cooperation and assistance that CB might render to manufacturers. CSC/P/5/74, dated 2 December 1974 and entitled "Involvement of the National COMSEC Agency (CBNRC) in the Security Evaluation of Commercial Cryptographic Equipment Offered by Canadian Industry for Non-Federal Government Use", was considered by the SAC at its Meeting on 14 January 1975. The Committee approved the option which proposed that the National COMSEC Agency provide a crypto-evaluation advisory service on a "need-to-know" basis to Federal departments considering the sponsorship of a commercial crypto equipment development, but with no direct association between CBNRC and the commercial establishment involved. The paper was updated in 1976 and again in 1985, retaining the provision that the National COMSEC Agency should have no direct association with a commercial establishment. These developments, however, contributed to the advancement of the evaluation capability.

Chapter 22

Production of Crypto Equipment in Canada

s.15(1) - DEF

s.15(1) - IA

Chapter 22 - Production of Crypto Equipment in Canada

Confused Beginnings

22.1 The first cipher machines used in Canada were provided by the UK. This was normal, since up to and including the time of World War II Canada depended very heavily on the Dominions Office/Commonwealth Relations Office for assistance in communications as well as in many other areas. This support to Commonwealth governments was a heavy burden, and after the war UK authorities requested Canada and other Commonwealth countries to provide their own keying materials. The UK, however, continued to design, develop and manufacture crypto equipment, but did not encourage Canada to do so. The US quickly entered the field. Originally, both the UK and US turned their own equipment over to Canada on a long term loan basis, so that they could communicate securely with us.

22.2

22.3 Although from the beginning of Canada's entry into the COMSEC field - in 1946 and 1947 - some imaginative souls felt that Canada could and should produce her own cipher devices to ensure national security, other more realistic officials realized that this was not practical at least not at that time. The idea would not go away, however, and continued to surface from time to time, particularly when new departmental representatives appeared on the COMSEC scene. The subject was discussed thoroughly on many occasions, and modest production programs planned and even a few undertaken. The major obstacle was the tremendous cost of development and production of equipment to meet a small, non-recurring requirement.

22.4 The Director of Telecommunications Operations, RCAF, in March 1953 found an urgent requirement for 30 SIGTOT cipher machines for use within the NATO organization (for the First Canadian Air Division to meet operational commitments under SHAPE). The RCN also had a NATO requirement for SIGTOT equipment. CB enquired whether NSA or the US Services could meet these requirements. When NSA was unable to comply, the Cipher Policy Committee (CPC) was asked to consider the possibility of having the equipment manufactured in Canada. The RCAF later reduced its urgent requirement to six machines, and the USAF was able to supply them. Supreme Allied Commander Atlantic (SACLANT) provided for the RCN needs. The CPC agreed there was no further necessity for production.

22.5 A Cipher Machine Production Group (CMPG), a working level sub-committee of the CPC, had been formed in September 1952, "on an interim basis to investigate and submit recommendations to the Cipher Policy Committee as to whether or not it is advisable for Canada to undertake the production of approved cipher machines and associated spare parts". GCHQ was asked for advice and information regarding the problems involved and the cost of producing crypto equipment. The CMPG Chairman, the Secretary, and a representative of the Department of Defence Production (DDP) toured a Montreal plant (Northern

Electric) specializing in the manufacture of complex parts and assemblies considered similar to those used in cipher equipment generally. Officials and technical costing experts of the firm then visited Ottawa Wireless Station, where they examined a ROCKEX cipher machine and later submitted a production cost estimate. A paper with specific proposals was prepared and submitted to the CSB. The paper, CSB 35 dated 16 February 1954, pointed out that although the Departments of External Affairs and National Defence used Canadian-produced cryptomaterial, "Canada is entirely dependent upon the UK or the US for the supply of the cipher machines with which this material is used". It recommended the establishment of cipher machine production facilities, a cipher evaluation group and a cipher machine development group.

22.6 Discussion at the 26th CPC Meeting on 5 November 1954 indicated that the requirement at that time was to do re-evaluation of crypto machines in use or considered for use, but that development of equipment should be postponed because "the setting up of a large unit for this purpose would appear to be uneconomical as the number of new cipher machines introduced is limited". The Minutes continued: "Since independent operation of Canadian Forces is very unlikely, the Services are bound to employ the cipher systems used by the major cooperating forces. The requirement for a unique machine for strictly Canadian use appeared therefore to be so limited that it would be uneconomical to undertake development for this purpose." The CPC rejected a suggestion by the Director LCSA (London Communications Security Agency) that Canada produce PORTEX, because the device would have only limited application; it was not favoured by the Services or by the Department of External Affairs.

22.7 Thus the decision was always made on grounds of economy. The enormous cost of development was considered not warranted in light of the ready availability of equipment from the UK and US. The CPC agreed to prepare a new paper on the subject but to defer any other action on the grounds that "establishment of cipher evaluation and development units ... is not likely to be practical or feasible in the immediate future on financial and economic grounds". They suggested that "CBNRC proceed to build up a nucleus of trained personnel within the next 4 or 5 years through integration of selected persons with NSA and/or GCHQ staffs" and proposed that "as an interim measure ... Canada will state requirements ... for ... machines ... and, if necessary, contribute financially to the development effort put forth by the UK".

22.8 The CSB at its 16th Meeting on 16 February 1955 agreed to "defer indefinitely a decision on the establishment of a cipher machine development unit" but the Board had no objection to an "External Affairs requirement for a 'miniaturized' mechanical ROCKEX machine which might be submitted to the UK authorities for development ... (as it) ... would not ... involve Canada in any financial outlay". Accordingly, CB authorized an expenditure of $200 for Gord Thomson to develop a miniaturized ROCKEX, called SAPPHIRE, for use in areas where TEMPEST considerations were paramount (e.g. missions behind the Iron Curtain). Since SAPPHIRE made use of standard Teletype parts it was considered that Canadian production would present no serious problems. A working model was sent for study to GCHQ, who found that it had no radiation problem and no compromising acoustics. A short time later GCHQ produced a fully motor-driven version called NOREEN, which was purchased by the Canadian Department of External Affairs.

22.9 At its 10th Meeting on 15 June 1955 the Cipher Machine Production Group reviewed the recommendations of CPC Paper No. 14, which in effect laid down the conditions under which Canadian production of cipher machines could be undertaken:

i) The total number of machines and spare parts required justified tooling-up, and

ii) The Canadian unit cost was not out of line with the United Kingdom or the United States unit cost, and

iii) The estimated delivery date would be adequate, and
iv) Security requirements would be met throughout production;

or without these conditions if there was no alternative source of supply. If the Cipher Policy Committee considered that the above conditions were met in a particular case, it would submit its recommendations to the Chairman of the Security Panel (later to the Chairman of the Communications Security Board) for approval. From that point forward, any large scale requirement for crypto equipment would be studied in the light of possible Canadian production before a contract would be let. The CMPG had held ten meetings between 1952 and 1955, but the lack of a continuing interest in Canadian production of crypto equipment resulted in an absence of direction, and the Group never called an 11th Meeting.

Estimates of Requirements

22.10 During a visit of Major General W.R.C. Penney, Director of the London Communications Security Agency, to the US in 1957 it was agreed "that the task of reviewing Combined crypto requirements should be undertaken without delay" and that "Canada should be in on any such discussions from the start and that such requirements should be considered on a Combined (CAN/UK/US) basis only at this time, without the restricting influence of whether or not the systems concerned are to be released to NATO". Thus Canada became a member of a tripartite (CANUKUS) panel considering existing crypto systems and the need for new systems to meet current and future requirements.

22.11 The vulnerability of government communications, particularly those of DND, reached a high in the 1950s. Concern over this fact also peaked, and every attempt was made to enhance COMSEC. With the introduction of the transistor in the late 50s, electronic security protection rapidly took hold and the security record dramatically improved. Even before this radical innovation could have full effect, however, investigation of communications security needs was under way. A Canadian Crypto Equipment Policy paper (CSB/79, dated 31 December 1958) was prepared by the CSG, reviewing both on-line and off-line equipment needs and the devices available to meet these requirements. It was estimated that the total cost would reach $33 million to $43 million for Canadian Government Departments over a five-year period. The paper included complete and specific proposals for the purchase of various equipments. Coinciding with UK, US, CANUKUS and NATO policies, it recommended adoption of "on-line automatic security equipment for use wherever feasible ... abolition of plain language on the air ... quick, reliable and secure communications systems", and noted that Canadian Services must be equipped with the same COMSEC devices as the UK and US Services with whom they worked. The policy was approved by the CSB at its 24th Meeting on 27 February 1959.

Canadian Production Under Consideration

22.12 This gave rise to renewed speculation about the possible production of crypto equipment in Canada. The same arguments were dug up again and rehashed. Discussions were held with the Department of Defence Production (DDP), who then began sending a representative to the Communications-Electronic Security Policy Committee (CSPC) meetings. The Radio Corporation of America (RCA) wrote to DND and DDP, soliciting participation in any Canadian production of crypto equipment. The DDP member informed the Communications-Electronic Security Group (CSG) that a general agreement existed which provided for the production of UK and 5US Military equipment in Canada. Initially it was necessary to approach the appropriate design authority (Security Agency) for concurrence and the release of production drawings. An important requirement, too, was the preparation of special industrial security regulations for safeguarding crypto information and, of course, assurance that firms concerned could implement such regulations. Fortunately, retired Defence Services senior officials had obtained employment with RCA,

s.13(1)(a)
s.15(1) - DEF
s.15(1) - IA

providing easy access to the firm which had a number of employees cleared to SECRET and TOP SECRET, and also had areas specifically organized for the production of classified items.

22.13 When considering the possibility of Canadian production of cipher machines, the CSB at its 16th Meeting on 16 February 1955 had decided that each requirement should be reviewed by the CSPC as to feasibility before CSB approval was sought. When the Intelligence Policy Committee (IPC) assumed the COMSEC responsibilities of the CSB in 1960, the CSPC, CSG and CBNRC were already launched upon a review which would result in recommendations being presented to the IPC.

22.14

s.13(1)(a)
s.15(1) - DEF
s.15(1) - IA

22.15 Despite the problems and obstacles, it was becoming apparent that the day was approaching when the manufacture of crypto equipment would be undertaken in Canada to satisfy tri-Service requirements for an on-line cryptographic machine, in compliance with the national policy to encrypt all teletype traffic on the military communications networks. The main reasons for wanting the devices designed and built here were to be able to ensure the maximum in security, and to establish a North American source of supply for British crypto equipment and associated spares. In addition there were always those who felt that Canada should be able to profit financially from such an enterprise. It was generally accepted that Canadian firms had the necessary expertise and capability, but that the total national requirement would likely be so small as to render it impractical economically to establish a permanent arrangement for the manufacture of crypto devices. The CSB had decided (at its 16th Meeting) that no commercial benefit could be derived from the undertaking, and so the principal objective was to provide Canadian industry with experience in such manufacture, in order to set a precedent for meeting emergency situations. If, of course, production for others such as NATO countries could be arranged, so much the better, but indications were that there was very little likelihood of that happening.

Problems Involved

22.16 The problems of providing cryptomaterial and devices which will guarantee the security protection of transmitted information have never been generally understood and appreciated. Even today members of committees glibly propose that Canada should develop and produce crypto equipment not only for domestic use but also for sale to our allies. There is a recognition of some complexity in the make-up of such devices, but there is also a complete lack of understanding of the problems of having them manufactured by commercial firms. People are so used to buying off-the-shelf items - e.g. typewriters and computers - that they are unable to conceive of a product that must be built "special-to-order". At the 16th Meeting of the CSB on 16 February 1955, in addition to the decisions recorded in the previous paragraph, it was agreed, after considerable discussion, to defer indefinitely a decision on the establishment of a cipher machine development unit, and that "production drawings and specifications for approved cipher machines should be obtained and contacts established with suitable commercial firms to permit production on short notice in an emergency".

22.17 "Production on short notice" is a naive proposal. Canada undertook to produce the CID/610, a Canadian version of the British ALVIS equipment, the BID/610, to be completely interoperable and compatible with its British counterpart. The Department of Defence Production, after consultation with United Kingdom authorities, concluded that UK quotations on costs and delivery dates could be met by Canadian production of ALVIS equipment - that any time lag would not be greater than six months. Although approval for Canadian production was given by the IPC in July 1961, it would be more than six years before the project was completed. Mr. Drake (at the 54th CSPC Meeting on 9 January 1962) remarked: "the original estimate of the CSPC had envisaged commencement of Canadian production (of ALVIS) in 1963 and completion of the order by 1965." In fact, production did get underway in 1963, but was not completed until the fall of 1967. Implementation problems continued for another two years. The project took longer than planned because, although the IPC had originally authorized production of "exact copies" of the British version, certain changes were proposed after Canadian trials of UK equipment. Each of these modifications had to be designed and developed in Canada, approved by the British Design Authority (GCHQ), and then incorporated into the design of the equipment. This, of course, resulted in slippage of production deadlines. It should be pointed out, too, that since this was the first undertaking to produce crypto equipment in Canada, there was no precedent and there

s.13(1)(a)

s.15(1) - DEF

s.15(1) - IA

were no established procedures, and therefore considerable delay was introduced in making the arrangements.

22.18

22.19 Meanwhile, arrangements were progressing for the production of ALVIS equipment in Canada. It became apparent that one such project was all that could be undertaken at a time, and nothing further developed towards Canadian production of a US-designed crypto equipment. The IPC invited DDP to make suitable arrangements for the manufacture of ALVIS in Canada, and invited NRC to assume the responsibilities of Canadian Design Authority, and to provide the personnel and facilities required for this task (IPC Meeting on 11 July 1961). One of the main production problems to be faced was security control. It was expected that CBNRC would act as the Design Authority in Canada, ensure that security arrangements were adequate, and coordinate any design changes (CSG 67th Meeting on 5 April 1961). While CBNRC did assume these responsibilities, the requirement to maintain a low profile interfered, and the RCAF became the official Canadian Design Authority. An ALVIS Production Working Party was formed, on which all three Services, CBNRC and DDP were represented, and all proposed design changes had to be approved by this Working Party.

22.20 The search for a manufacturer began in the spring of 1961, with the preference stated for an all-Canadian firm. It was thought that a small firm would simplify security arrangements and ensure lower production costs. By the fall, the CSPC was informed there were no developments in regard to the selection of a Canadian Manufacturer. By this time, an offer of production rights for ALVIS had been received from Britain. The offer was not entirely satisfactory as to price, materials or timing. Payment for manufacturing rights and production drawings was estimated at £200,000 plus 7 1/2% of the UK unit cost. Component sourcing information was expected from the UK in the fall of 1961, and drawings in early 1962. Engineering assistance was expected to be a problem, as CB would require two engineers to monitor production on a continuing basis in order to meet the required crypto and radiation security standards.

Delays Set In

22.21 At this stage, some disturbing news came from England. The cost of ALVIS was rising, and production was behind schedule. That meant increased licensing costs, and a delay in Canadian production. CSG Members, especially the RCN, were having second thoughts, since the UK ALVIS equipment was apparently going to cost $2,000 to $3,000 more per duplex terminal than the US TSEC/KW-26 equipment (both ALVIS and KW-26 were electronic, transistorized, on-line start/stop or synchronous crypto equipments, for use with standard 5-unit telegraph code). The ALVIS, of course, was a simple machine, very useful for netting arrangements as planned in Canadian Military communications, whereas the KW-26 was a very complex equipment. (Incidentally, in the end DND bought 414 KW-26s and External bought 97 BID/610s, while 872 CID/610s were ultimately produced in Canada for DND.)

22.22 While awaiting Treasury Board (TB) authority to arrange a suitable production cross-over arrangement with the British Ministry of Aviation, and subsequently awaiting word from the UK on a draft licence agreement, CBNRC and DDP were busy drafting physical and personnel security requirements. In the spring of 1962, Northern Electric was mentioned at the CSPC's 55th Meeting as the likely firm to receive the Canadian contract, as it was confirmed that "this company could meet the necessary security requirements". By September 1962, a satisfactory draft licence agreement had been received from the UK. It was "intended as an overall agreement between the British and Canadian governments, to be supplemented by a commercial agreement between the companies involved". Negotiations by this time had been switched from Northern Electric to RCA Victor. DDP and RCA representatives visited the UK in December 1962 to "negotiate an overall agreement on the Canadian production of ALVIS. During the visit, a company-to-company contract was successfully concluded between the British Automatic Telephone and Electric (AT&E) Company, a wholly-owned subsidiary of Plessey Limited (the British manufacturer) and RCA (the designated Canadian manufacturer)". This enabled Canada "to receive from Britain production engineering information on all aspects of the ALVIS project". The visitors noted that at the UK plant "current production methods were practically limited to hand operations. There appeared to be no automation".

22.23 Many decisions and arrangements were yet to be made. The IPC approved secretarially a proposal recommending certain procedures for incorporating design changes in Canadian-produced ALVIS equipment. There was concern that a Treasury Board desire to "consider" the design changes could delay production and "hinder the Design Authority in the performance of its task". Although each of the Services had different plans for using the equipment, they had agreed to accept all proposed modifications; otherwise several versions of CID/610 would have to be produced, and this would increase the unit cost and the production time. ALVIS had just been released to NATO. The Department of Trade and Commerce were aware of plans to manufacture ALVIS in Canada, and were anxious to promote sales of the Canadian version, CID/610, to NATO. The draft agreement with the UK, however, prohibited such sale; provision was made for Canadian Government use only. The Department of Trade and Commerce "agreed to restrain their interest for security reasons". LCSA requested that no mention of Canadian production of

ALVIS be made during NATO discussions (e.g. during consideration of MC 74/1, a NATO Military Committee paper on COMSEC policy).

22.24 This ambivalence was constantly present among Canadian authorities. There was the desire to obtain crypto equipment for the lowest possible price, but also to take advantage of any profit that might accrue to Canada if it arranged to undertake the production itself. The authority to establish the necessary developmental background for such a venture was, however, never forthcoming. The Director CB had suggested to the CSPC that CBNRC would be better equipped to deal with the ALVIS production program if some development capability had been initiated previously. The authorities defended their position by saying: "Since there is no firm or extensive requirement for a unique Canadian cipher machine, the establishment of a cipher machine development capability in Canada would be very difficult to justify." They added "the current British/US development programs appear to be adequate to meet all known requirements for such equipment for many years to come". It was agreed that "ALVIS" would be retained as the code-name for the equipment, and "CID/610" as the crypto short title, but that "Canadian Telegraph Convertor No. 1" would be the unclassified contract title for use in correspondence with the manufacturer and other contractual dealings.

Activity Commences

22.25 The engineering study contract with RCA Victor, the first phase of Canadian production, at a cost of $44,830, was approved by the Treasury Board in February 1963. Certification of the invoice for £50,000 submitted by Plessey was being completed by the three Services, and payment was expected shortly. RCA Victor was already engaged in the initial phases of the study contract, a production engineering and design appreciation. The transfer of information from AT&E to RCA Victor was proceeding well: two shipments of production drawings and specifications had been received. DDP were developing cost estimates for in-plant training, manuals, and spares provisioning requirements. RCA representatives were invited to a meeting of the ALVIS Production Working Party. DDP and CBNRC had approved the production space allocated for the project at RCA's Montreal plant, and the RCMP had endorsed the security arrangements.

22.26 Although all concerned continually enquired about the status of the project, it was difficult to predict when actual production would commence. Early in 1963 the sourcing of components was underway. If Canadian-designed transistors could be obtained, Canadian content could reach the hoped-for level of 85% to 90% without too great an increase in cost. It was expected that Canadian production delivery dates would run approximately six months behind UK forecast delivery dates; but then problems developed. There was delay in receiving information from the UK, and there were questions about using Canadian produced transistors instead of those produced in the UK. After much debate, Canadian transistors were used, and this led to problems later.

More Delays and Increased Costs

22.27 It was hoped to complete the study phase by mid-June 1963, and then to be prepared to start on two prototype or pre-production models, with completion slated for mid-November. At that point, RCA could be authorized to proceed with the production of 150 to 200 units to enable a determination of unit cost. In fact, the study phase was completed by 15 July 1963, only a month late. There was one major technical problem which arose because of a proposal to have a switching matrix instead of a replaceable plugboard as a key setting device, but this would not be resolved for another year. In the meantime, Phase I completion was approved by mid-September, and Phase II - the manufacture of two pre-production models ("pre-pros") - was given ministerial approval in DND, and awaited Treasury Board concurrence so that it could be negotiated with RCA Victor. One month delay was occasioned in awaiting TB approval of funding for modifications, and the arrival of needed information from the UK. Another month's slippage resulted from the late delivery of components (there was difficulty in obtaining a certain type of rectifier), but two prototype models were completed and available for examination and test by the last week of January 1964.

22.28 Negotiations were now underway for Phase III, which would include training by the contractor of 30 Service personnel during a six-weeks course. It was expected that production models would commence delivery in September 1964 at a rate of 20 per month, then 30, then 50. Earlier estimates of a cost of $5,800 were revised to $6,400-$6,600 per unit. At this point, incorporation of low level keying to suppress compromising radiation was proposed. The Army wanted high level keying, but this would have constituted a design change, resulting in further delay and increased cost. The Production Working Party agreed to use relays in the output circuit, which permitted the production of a single version, with a choice of high or low level operation. Incorporation of this modification and others postponed the projected delivery date of the first production unit from September 1964 to January 1965. The latest cost estimate, including modifications, was $7,350 per unit. This compared favourably with the original estimated price of the BID/610, which however had by now been considerably reduced. The requirement for CID/610 dropped from 1,002 to 986 with no increase in unit cost.

22.29 Although officially the RCAF was the Design Authority, two CBNRC technicians visited the RCA plant to observe and assist during engineering and systems testing of the two pre-production models. Both devices passed the tests by mid-April 1962. The keying problem was satisfactorily resolved, with the decision in favour of a matrix selector which would undergo tests at RCA, and then the two "pre-pros" would be shipped to CBNRC for crypto and radiation tests. Later they would go to LCSA for testing and approval. Modifications accounted for 10% of the cost of the CID/610, which was however a great improvement over the BID/610. The CSPC noted that not only CBNRC but also LCSA and the British Ministry of Aviation considered the Canadian model better than the BID/610 insofar as radiation was concerned. Efforts were under way to make the necessary financial arrangements for the project, with the RCAF CSG Member interceding with the Assistant Deputy Minister (Requirements) in DND, pointing out that if funds for some advance procurement could be allocated it would expedite the start of production. During S Group testing of the CID/610 prototypes, more modifications were required, including structural changes which were performed in the T Group workshops. During this time, too, T Group was producing ALVIS keying material for use by External Affairs with BID/610. Drafting of the CID/610 Operating Manual by S Group was well ahead of requirement.

Initial Production of CID/610

22.30 In May 1964, authority was given for the release of $4,160 for the start of Phase III, and in July the Treasury Board approved production of 986 units. The first production models (ten) were expected in February 1965, to be followed by thirty in March and fifty in each of the succeeding months. CBNRC was responsible for evaluating the first ten and approximately one in every thirty units thereafter, to ensure that the rigid production standards were being met and maintained, as far as the cryptosystem and radiation characteristics were concerned. The RCN was anxious to obtain ten equipments for training purposes. However, during engineering and radiation tests of the prototypes, CBNRC discovered problems and deficiencies which necessitated design changes. It was planned to incorporate most electrical design changes in one of the prototype models, which would then be tested for radiation problems by CBNRC. The other would be sent to England for three months of tests by LCSA. The design changes would, of course, introduce further delay. Delivery could be 40 weeks from when DND authorized full production, but such authorization was not expected before mid-November 1964, when RCA Victor would provide estimates of the costs involved in incorporating the design changes.

22.31 Production got underway in December 1964. CID/610 met the required radiation limits (US Fed. Std. No. 222) and the Production Working Party had accepted the Matrix Selector and the Key Setting Tool. F/L G. Dawson, as courier, accompanied one prototype to Britain, representing the Canadian Design Authority. Don Fairley and Lyn Mulligan of CBNRC visited LCSA at the same time "to handle policy matters and provide technical assistance respectively". A Documentation Working Party was set up for the preparation of CID/610 manuals. Since DND would be the main user of CID/610 equipment, and in order to conform to Service procedures, LCdr. W.D. Moyes wanted the manuals to have CIS (Canadian Inter Service) designators in the short titles. CSG policy, however, dictated that where more than one department used a publication it must have a CID (Canadian Inter Departmental) designator. The alternative of producing both CID and CIS versions of one publication would involve an unacceptable expense. It was agreed that CID/610 manuals used only by DND (such as installation instructions or parts listings) would bear CIS short titles, whereas those used also by civil departments must bear CID short titles, but would take into consideration any special DND requirements. CESD (formerly LCSA) queried the CONFIDENTIAL classification of CID/610 documents, when BID/610 documents were all classified SECRET. Discussions on the subject during the CSG Chairman's visit to the UK resulted in agreement that CID/610 documents would bear the same security classification as their BID/610 counterparts. Technical manuals for the CID/610 were to be written by the RCA Victor Company under contractual arrangements with DDP. The Company, however, was not familiar with the operational configurations and the COMSEC aspects of the CID/610 installation. As a consequence, the responsibility for drafting the chapters and other portions of the manual in which these criteria were detailed was assigned to CBNRC S Group.

22.32 By January 1965, all was going well despite five months slippage. Release had been given to RCA Victor for all major components. To date, the military had released $5,000,000. The cost per unit was expected to remain at $6,000 with "first off production" about 1 August 1965. The prototype, modified by CBNRC after radiation tests, was undergoing trials in England. A mock-up of the technical manuals was in circulation to CSG Members. The following month brought a requirement for more modifications which, though minor, would add to the cost and delay delivery of the first models. Testing continued at CBNRC and in the UK. CBNRC, as the ultimate Canadian authority in crypto matters, was asked to be the agency responsible for repair and subsequent testing of CID/610 Noise Generator Boards found faulty by users. The CSG Chairman drew attention to the shortage of staff at CB, but reluctantly agreed to having the COMSEC Agency assume the responsibility on a trial basis. The security classification of the basic CID/610 and BID/610 equipments was lowered from SECRET to CONFIDENTIAL. The Key Setting Tool when not set would be classified CONFIDENTIAL CRYPTO, but when set to key it would bear the same classification as the key to which it was set. The overall security classification of the CID/610 contract would remain SECRET.

Prototypes Approved

22.33 LCSA trials found that the one prototype CID/610 which they had been sent met the required standards, and the second prototype tested for radiation at CBNRC was also found to be satisfactory. One of these would be returned to the contractor. Meanwhile, there was further slippage at the plant, with the prediction of "first off" being put back month by month.

22.34 With the integration of the three Military Services came a reduction in the quantity of CID/610 required. In December 1965 the order was decreased from 986 units to 872; there would be no increase in unit cost, but there was a contract termination charge of $325,000. The first two production units of the CID/610 were delivered to CBNRC from RCA Victor on 30 December 1965. An additional 24 equipments were delivered the following week. In order to expedite testing, S Group had fabricated cable sets, prepared for system installation, and drafted test procedures and data sheets. The ninth and tenth equipments produced, when tested OK by CBNRC, were regarded as "sealed samples", and the design was frozen, i.e. no more changes would be permitted.

22.35 It was necessary to obtain the approval of SECAN (the NATO Security and Evaluation Agency) before CID/610 could be used to pass NATO traffic. The British Ministry of Aviation gave permission for SECAN testing with no formal change to the licence agreement. The request for approval had to be accompanied by two complete terminal installations, including ancillaries, all of which would be retained by SECAN. Each proposed configuration would be tested for approval, and this would require six months. The delay involved concerned DND, who wished to begin using CID/610 in the fall of 1966. In any event, when the equipment was installed it would not be possible to provide separate crypto-communications facilities for NATO and national traffic. So for the moment the question of NATO use was held in abeyance. As for national traffic, since the CSPC had already approved BID/610 for this purpose, a separate authorization for the compatible CID/610 was not considered necessary. External Affairs already had 18 BID/610s in operation, and were contemplating the possibility of acquiring more. A new format for operational key lists for use with CID/610 had been agreed. The cost of having the new format produced by the Queen's Printer would have been prohibitive, so they were produced by T Group CBNRC.

Hitches - Spare Parts and Manuals

22.36 Some problems with the delivery of spare parts were encountered after 65 equipments had been completed by April 1966. However, it was hoped, after resolution of the difficulties, to re-establish equipment production by mid-June. DND was anxious to begin operations. Training courses had been held in March, April and May, using the first ten production units immediately after they had been tested by CBNRC. The manuals likewise were urgently required by DND, and in order to expedite them it was agreed that T Group CBNRC would produce them. Production resumed and, by the beginning of July, 200 units had been delivered. Output was averaging 25 every two weeks. The total cost so far was $8.2 million, expected to reach $8.5 million. The new target date for completion of production was 1 September 1967. The military representative told the CSPC that the Services planned on operational installation early in 1967. As production continued (474 units were produced by the end of 1966), a Contract Demand was raised for spare parts. Treasury Board approved this contract in February 1967.

22.37 Meanwhile, problems developed in the operation of installed CID/610 equipment. Intermittent failures of matrix selectors were reported. In addition, failure of some of the Canadian transistors occurred, three at CBNRC, others at the Carp Communications Centre. No transistor failures were experienced with the two prototypes tested by CBNRC and LCSA, nor with the ten first production equipments, thoroughly checked by CBNRC, two of which were also tested by NSA. All units tested performed entirely satisfactorily before full production release was given. There was no evidence during these extensive trials of any transistor weaknesses. A basic objective of the production procurement had been to embody the maximum Canadian content into the equipment. This resulted in the use of Canadian components wherever possible, and in particular the use of 2N217 transistors produced by RCA. Canadian component selections were supported jointly by the Department of Defence Production and the Canadian Military Electronics Standards Agency component divisions. The decision to use the 2N217, of which a total of 740,899 were embodied in the equipment, was deliberate and was taken only after demonstration in the prototype equipments that this type of transistor was satisfactory. RCA performed several separate tests to assure themselves and DND that the choice was sound. The full services of DND Quality Assurance (QA) facilities were used throughout production, with two resident inspectors assigned full time at the plant. Supporting DND/QA were CBNRC, as the Canadian Communications Security Authority, and a Working Party of the CSG.

22.38 SECAN completed the failure analysis study. Approval was temporarily withheld, as several areas were detected where component failures would give rise to insecure conditions. CBNRC had devised modifications to overcome the two most serious failures. The main problem was one of configuration, and was common to both CID/610 and BID/610; CESD (LCSA's new title) was not concerned about immediate modification action. However, DND was anxious to launch CID/610 operation in February 1967, and pressed for corrective action. Answers to all problems were found; the CSG approved the modifications, and directed the engineering staffs of CBNRC and CFHQ to coordinate their implementation. A NATO memorandum, drafted by SECAN, approved CID/610, conditional on the incorporation of modifications, and imposing two standard NATO restrictions: a) a 200-foot secure perimeter, and b) installation of power line filters in accordance with NATO Standing Group requirements. New submissions would be required if CID/610 were used with other ancillaries. By this time (April/May 1967) 710 equipments had been shipped, and no major production problems were reported.

22.39 Deeply involved in preparations for Expo 67, the RCMP suddenly had a requirement for crypto. They had had off-line ciphers (ROCKEX, TYPEX), but without protection for their on-line communications RCMP officers were unable to hold teleconferences on classified subjects, and would have to drive from Ottawa, Montreal and Toronto to a "meet" (their term) in Kingston (or elsewhere) for urgent discussions. They borrowed CID/610 equipment from CFHQ (Air), and attempted to order ten equipments from RCA Victor, but were too late to get an "add-on" to the contract - and, of course, there would not be another production contract.

22.40 The UK design authority introduced a secondary variable capability into the BID/610. A modification was incorporated into the matrix selector of the CID/610 to provide an equivalent facility. The Canadian Secondary Variable (SV), which was actually a new crypto variable component, would use the same random pattern as that in the BID/610, and would therefore be fully compatible. Since the primary variable provided the required level of security, the SV was not intended to provide increased crypto protection, but rather to act as an additional barrier in the event of compromise of the key setting. The SVs would be used on CAN/UK circuits, but held in abeyance on domestic nets.

22.41 The TEMPEST (radiation) testing of CID/610 equipment placed an enormous load on CBNRC's modest facilities. Several priority projects had to be postponed in an attempt to cope with the flow of equipment off the production line. Moreover, the many design changes necessitated extended tests. In view of the consistently satisfactory results obtained throughout the first part of the TEMPEST testing program it was considered that there would be little risk if the sampling rate were reduced; accordingly, the CSG authorized a reduction in the radiation sampling rate from one in thirty to one in sixty. The TEMPEST testing was completed in October 1967, and all devices tested met the prescribed standards.

ALVIS Production Completed

22.42 The last equipment of the 872 ordered was shipped on 8 September 1967. Spare parts production continued until May 1968. The final tooling was to be retained and stored by RCA Victor against the possibility of a further requirement arising. CBNRC, DDP, DND and RCA representatives would meet within a year, and if no additional production was required the special tooling would be returned. One complete set of updated production drawings and engineering data (3 or 4 file cabinets) would be stored in CBNRC. Incidentally, CB had also agreed to provide emergency storage for drawings of various UK crypto equipments. By mid-May 1968, the production of spare parts was complete. Since DND was concerned, however, about the high percentage of matrix selector malfunctions, both electrical and mechanical (over 50% of the devices were affected), the tooling and drawings for these were retained at the plant. RCA would rectify the faulty matrix selectors at no cost to the Crown. The manufacturer's responsibility extended a year from the date of delivery of the product. A year later, DND had DDP arrange a contract for the overhaul and repair of the matrix selectors. Because of the high failure rate a shortage of spares developed. However, in November 1969 the CSG was informed that the number of failures was decreasing as a result of better handling.

22.43 Meanwhile, the failures of 2N217 transistors continued. DDP reported that information from the US indicated that the transistors had a very short life. This caused considerable concern, because DND had purchased a ten-year supply. Very extensive investigations were conducted, including comparison tests with US-produced 2N217 transistors and UK-produced OC71 or NKT280 transistors. The problems were attributed to various causes: e.g. RCA had changed the potting compound, etc. In any case, it was found that the problem disappeared if all the 2N217 transistors mounted on the type A boards were replaced by UK transistors; other type boards were, by comparison, minor contributors to the problem. The number of transistors involved was 12 per board on 18 boards in each of 862 equipments, plus 770 spare boards, for a total of 195,432 transistors. The cost was $111,500 ($73,500 for material and $38,000 for labour) as compared with $200,000 (including labour and material) to replace all transistors on all boards. As for the overall CID/610 contract, the funds committed for production amounted to $7,200,000. In addition, the cost of the licensing agreement was £300,000. The total cost of the project, therefore, including spares, was $8,593,356. The unit cost of the CID/610 emerged as $10,000, well above the original estimate of $7,000.

The production line was now shut down; the CSPC was informed that it could be reopened, but that that would be very costly.

Review of Undertaking

22.44 In retrospect, was ALVIS production in Canada a worthwhile venture? Opinions have been divided on the question. The RCAF CSPC representative was guarded. He admitted that the undertaking had provided work for Canadian industry, but involved no new challenge in the electronics field; in fact, he felt that the work mainly consisted of repackaging and transistorizing the British equipment. In view of the additional cost to DND, he considered that the Committee should look very carefully at any possible repetition of a project which involved the making of "Chinese copies" of a British or US equipment. The DDP (now Department of Supply and Services (DSS)) representative disagreed, pointing out that the Canadian equipment had incorporated several significant design improvements. The RCN representative compared the experience with that of purchasing a US crypto device, noting that as quantity production of the TSEC/KW-7 equipment had increased in the US, the cost of the equipment to Canada had fallen steadily from $4,000 to $2,500 per unit. The Director CBNRC observed that one of the factors that influenced the decision to produce ALVIS in Canada was the need to establish a North American source of supply for British equipment and associated spares. Bill Trowbridge, CSPC Secretary, conscious of CB's limited resources, observed that when crypto equipment was procured from the country of origin, the necessary documentation - operating and technical manuals - were provided, but with the Canadian ALVIS it had been necessary for CBNRC to produce Canadian manuals - a complex and costly undertaking. Two years later Mr. Trowbridge, as the CBNRC representative on the CSPC, had the same point in mind when he said that if Canada ever again undertook the production of another British or US equipment, every effort should be made to manufacture an exact replica of the original equipment, because each modification issued by the original design authority involved an independent

R&D project at CBNRC to adapt it to the Canadian equipment, in order to maintain compatibility; this created a heavy strain on CBNRC's limited laboratory facilities, and at times even delayed other important projects. Thus the experience with the CID/610 project made CBNRC cautious about supporting future proposals for Canadian production of crypto equipment, but did not stifle the enthusiasm of others to embark on such an undertaking.

NADIR

22.45 In August 1973 the RCMP requested CBNRC to participate in a "feasibility study leading to a large scale production of a quasi-secure speech privacy device applicable to all levels and tasking" within the RCMP FM networks. It subsequently developed that the RCMP had a requirement for some 10,000 units of a crypto device to protect tactical voice communications nets, some of which carried classified information and therefore required secure, not quasi-secure, protection. The development was called the NADIR Project.

22.46 In the following twelve months, CBNRC, the RCMP and the Communications Research Centre (CRC) of the Department of Communications collaborated in the preliminary development of NADIR. CBNRC developed the cryptologic, the alarm criteria and keying material information; the RCMP provided operational procedures; and the CRC developed the portable radio, subcontracting with Bell-Northern Research (BNR) for implementation of the design in hardware. BNR submitted a preliminary test report for a programmable shift register using custom-designed integrated circuits and random access memory, and designed and produced custom Large Scale Integration (LSI) chips for a field programmer. As CBNRC did not have the facilities to do either a system simulation or a failure analysis, arrangements were being made toward the end of 1975 to submit a NADIR package to NSA for evaluation. This was the first original cryptologic that CSE ever designed and, in fact, was the first time CSE ever built any custom integrated circuits for any project. The cryptologic was basic, but the implementation of functions, microprocessors and software control was innovative. The continued development of this and related projects occurred after the period covered by this History.

Conclusion

22.47 CBNRC's sally into the field of crypto equipment production was stimulating, and paved the way for future efforts. It was encouraging in that it proved that the desire and the capability exist in Canada, but it also demonstrated that undertaking such projects without adequate resources gives rise to frustration. Venture capital is not readily available in Canada, either in the governmental area or in the world of business.

Chapter 23

COMSEC Monitoring and Analysis

Chapter 23 - COMSEC Monitoring and Analysis

Introduction

23.1 It will be obvious from the preceding Chapters that Canadian Government communicators "in the early days" not only took few security precautions, but did not really know whether any precautions taken were effective. The best way to find out if unauthorized persons can derive intelligence from our communications is to do exactly what those persons would do themselves to get such information. Our own SIGINT successes against foreign communications generated concern about the level of COMSEC maintained on Canadian networks. The introduction of COMSEC measures in some areas also caused the authorities to wonder about what information was being inadvertently revealed elsewhere, but it was not until the late 1950s that any concrete action was taken to learn more about this, and to take corrective action.

23.2 Transmissions by radio (even microwave) are easy to intercept, because the signals are on the air, available to be picked up by anyone with a suitable receiver - if the signal is strong enough to be heard. In particular, high frequency (HF) transmissions can be heard at great distances, and therefore the use of minimum power is advised. Even landlines can be "tapped" if they are accessible. The first step is to collect the communications traffic in its transmitted form - plain language, code or cipher - and then to examine it to determine whether any sensitive or intelligence type information is disclosed. Unlike the SIGINT analyst, the COMSEC analyst is not concerned directly with the total content of the information, but rather with whether any intelligence was indeed revealed, how it was made available, and how this can be prevented. The important objectives, therefore, are the isolation and identification of those COMSEC weaknesses which can allow sensitive information to be derived from communications, and the development of measures to preclude or at least make more difficult the exploitation of the transmissions.

These objectives embrace the complete range of communications security (in order that no unintended information be revealed) - crypto security, transmission security, electronic emission security and, of course, physical security.

The Threat Examined

23.3 The let-down in security consciousness following World War II rendered defence communications very vulnerable, and this vulnerability reached a high in the 1950s. Most transmissions were in plain language, and even though individual messages were unclassified, a study of their contents in relation to others over a period of time could reveal a surprising amount of intelligence. A determined campaign to make users more conscious of COMSEC, and more particularly of the need for high standards in it, was launched in the US and the UK, and its influence was also felt in Canada. Commonwealth Quarterly Liaison Notes sent to Canada from the UK placed great emphasis on transmission security; Mr. Drake drew attention to this at the Cipher Policy Committee (CPC) Meeting on 20 January 1956, and suggested that the time had come to analyse Canadian Government communications. He observed that, initially at any rate, such an undertaking would be hindered by staff limitations in CBNRC. The Chairman lamented the lack of monitoring facilities, but expressed reluctance to endorse any serious diversion of the SIGINT effort for this purpose. However, the RCN had limited monitoring facilities in Halifax and Victoria, which the Director of Naval Communications thought might possibly be diverted to national use for two or three days at a time. The alternative to monitoring transmissions was collecting "drop copies" - the printed copies of messages sent. This had the disadvantage of missing out on the "operator chatter" between the actual message texts, which often revealed intelligence about cipher procedures, or even referred to the subject matter of individual classified messages. Nevertheless, since the easiest and most readily available means was the drop copy method, this expedient was resorted to for the initial study.

23.4 CBNRC was asked to conduct an examination of the plain language (UNCLASSIFIED) communications of the Canadian Armed Services during the month of March 1956. Drop copies of 6,000 RCN messages, 6,000 Army messages and 50,000 RCAF messages (two weeks traffic) were studied, and sensitive information identified. The CBNRC analysis shocked the various committees. The CPC Chairman characterized the situation as dangerous, with serious implications; and the Joint Intelligence Committee (JIC) said it was obvious that intelligence of great value was being made readily available to a potential enemy through plain language transmissions.

23.5

Preliminary Responses

23.6 A CPC working party was formed to outline interim measures to improve the situation, to provide an estimate of the costs of such measures, and to make long term recommendations dealing with the problems and costs of implementing an on-line crypto equipment policy. A paper was produced in June 1957, CSB/66, entitled "Improvement of Security of Canadian Armed Services Communications", which was approved by the CSB at its 21st Meeting. It recommended provisional measures to be implemented by the Defence Services. Long term proposals were later set forth in CSB/79, the Canadian Crypto Equipment Policy[1]. The ultimate objective was to restrict the flow of plain language traffic, especially on H/F radio circuits.

23.7 A second analysis operation was conducted by CBNRC, this time against the RCN exercise "BEAVERDAM" in December 1957 in the North Atlantic. It was observed that although operating procedures and discipline during the exercise were on the whole of a reasonably high standard, COMSEC regulations were applied rather loosely on certain occasions. At the same time, the Supreme Allied Command Europe (SACEUR) continued to press for cooperation in the monitoring of NATO-funded circuits; assurances were given that national circuits would not be monitored unless requested, and SHAPE offered its facilities to train personnel in communications security monitoring. The CPC directed the Communications-Electronic Security Group (CSG) to "examine the problem of Canadian monitoring facilities", including the scope and organization of existing facilities, and to submit proposals to improve them as necessary. The members of the CSG were each to prepare a submission on the status of their individual facilities.

Monitoring Facilities

23.8 The RCN was the only Canadian Service employing a full-time monitoring organization: it consisted of two small (7 man) civilian units, one stationed on each coast. These units carried out spot checks on all naval fixed and mobile radio circuits, monitoring for procedural errors, breaches of circuit discipline and cipher malpractices. The teams possessed no traffic analysis capabilities. The Army had had a Security Troop to monitor tactical communication circuits within the Division, but upon reorganization the new Brigade set-up did not provide for such a unit. The only monitoring facilities available were provided on an "ad hoc" basis to summer concentrations and exercises, by borrowing personnel from other units and establishments not participating in the exercises. Such staff was often

[1] See para. 17.65

not available because of personnel shortages and, in any case, any who were provided were almost completely untrained for the purpose. The Air Force acknowledged that it had very limited monitoring facilities for the purpose of policing air/ground/air radio circuits and teletype circuits. Analysis of sample transmissions was performed solely to check operating procedures. All three Services agreed that there was an urgent need to improve facilities. The RCN called for the establishment of both COMSEC and ELINT analysis organizations, and recommended that this work could best be done by CBNRC.

23.9

Further Measures to Improve

23.10 Meanwhile, the Services took steps to eliminate the weaknesses discovered in the CBNRC

COMSEC analyses. As of 1 March 1958, the RCAF transferred to landline much of its plain language traffic formerly carried over "trunk radio circuits". The Air Force also initiated action to procure additional ROCKEX (off-line) and ETCRRM (on-line) cipher equipment. These measures would reduce the total amount of plain language traffic on RCAF HF radio circuits by approximately 70 per cent. The Army removed plain language from the majority of its HF radio circuits through the extended use of 5UCO equipment and landline facilities. Most of the RCN shore circuits were landline, and 5UCO equipment had been installed on certain main channels. The problem of plain language shore-to-ship communications would remain, however, until suitable on-line equipment became available.

23.11 CB analysed drop copies of unclassified plain language messages transmitted by the Military Services over HF radio circuits during the month of May 1958. The Cipher Policy Committee noted that the report reflected a definite improvement over the two previous years. A year later some important circuits still carried plain text, e.g. the RCAF Goose Bay HF radio circuit, and occasionally the Army Ottawa-Boddington Radioteletypewriter (RTT) circuit (when on-line crypto was inoperative), but on the whole the situation had improved. An analysis of plain language messages transmitted by the Department of External Affairs during January and February 1959 was carried out by CBNRC, and the results indicated that transmission security was being adequately maintained by the Department.

Requirements for Additional Resources

23.12 A paper, CSG/P/23, entitled "Canadian Monitoring Facilities" was drafted in early 1959; it reviewed existing facilities, and contained recommendations from the CSG Members as to what the capabilities should be. The RCN was happy with its stationary units on each coast, but it was felt that there was a need for at least one mobile unit, which could tour the various Commands and assess the regular standard of communications security, in addition to being available for the monitoring of exercises. It was stated that the minimum requirement was for four persons, to form a team which would become part of CBNRC. As the Minutes of the Meeting which considered the paper put it: "Close study of the draft paper gave rise to a lengthy and spirited discussion on various aspects of the monitoring problem." In fact, several years and several redrafts later there was still spirited discussion - which always occurred whenever there was a proposal involving additional personnel. In 1960 and 1962 the Communications-Electronics Security Policy Committee (CSPC) deferred approval of the paper pending the outcome of the Services' crypto equipment procurement program, on the grounds that more widespread use of ciphers, especially on-line equipment, would reduce the amount of information available for exploitation by unauthorized persons. They looked toward a total encryption concept in the distant future.

23.13 The paper was rewritten several times and finally emerged as CSG/P/31 (CSPC/P/44). During discussion by the CSPC in May 1962, it was agreed that the establishment of a central COMSEC analysis unit at CBNRC, to which drop copies of material could be sent for study, would be desirable, beneficial and relatively inexpensive; whereas any extension of the current monitoring facilities by the Services was thought to involve considerable extra expenditure. Nor would the Committee endorse any increase in staff for CBNRC to perform monitoring duties. CB's Assistant Director (A/D) questioned the advisability of establishing a COMSEC analysis unit within CBNRC unless it could be confirmed that the flow of monitored material would be sufficient to keep the unit actively employed. He also stressed that drop copies provided a look at only part of the picture, and that their analysis did not give a true indication of the overall security of communications. In the end, the Committee approved the paper subject to the condition that further consideration be given at a later date to the extent to which each Service and Department could implement its recommendations. One year later, the CSPC again considered the paper, and it was suggested by the RCN that CBNRC set up a mobile monitoring facility. The Director CB explained that this was not practicable, but he offered to expand the existing COMSEC analysis facility to provide a continuing capability for the study of drop copy traffic to be provided by the "customer". The members endorsed the suggestion to increase the flow of drop copy to CBNRC for analysis.

23.14 Soviet Bloc SIGINT and hydrographic ships with extensive antenna arrays had been frequenting the waters off the east and west coasts for several years. By 1963 these visits were becoming more prevalent and more daring. Their continued presence indicated that there was information to intercept of sufficient intelligence value to warrant the operation.

First Practical Steps

23.15 Two T Group staff members were given intensive training as COMSEC analysts, and were established in 1964 as the nucleus of a COMSEC Analysis Section. They began accumulating information to build up a library of pertinent details and background data to be used in the study of Canadian Government communications. Some twenty COMSEC analyses had already been completed by the combined efforts of COMSEC and SIGINT staffs of CBNRC, some of whom were pressed into service on an ad hoc basis.

23.16 The first COMSEC monitoring/analysis effort of the fledgling new section, T5, was mounted against a war game exercise involving Canadian and USN Tactical Trainers at Halifax and Newport News, Virginia, and also involving some of their associated bases and headquarters such as Argentia and Maritime HQ. The exercise was not only to assess the COMSEC standards on the exercise nets, but also to assist with establishing the requirement for speech secrecy equipment. The provision of ciphony-equipped circuits interconnecting Naval HQ, Command HQ, and operational bases, together with cross connections to

s.15(1) - DEF

appropriate RCAF and Army authorities, was under study in 1963-64. Speech secrecy equipment was (and still is) extremely expensive, and the need had to be fully justified. For this exercise (CANUSTREX 63), three secure teletype (T/T) circuits and three unsecured voice circuits were installed - the T/T lines for actual exercise communications, and the voice circuits for the training supervisors' use. A measure of the security consciousness of at least some of the individuals involved can be gained from a statement one person made on a voice circuit that was being monitored: "I can't tell you here. This line is bugged. I'll call you back on the Bell Telephone line." Apparently they were more concerned about interception by COMSEC personnel than by a possibly hostile foreign power. Other organizers had said that they would simply talk around classified subjects using "veiled references".

23.17 In the fall of 1964, the two T5 staff members supervised the RCN monitoring team at Esquimalt in the monitoring of Exercise HARD SHOT. From analysis of pre-exercise communications the team was able to present a preliminary report to the Admiral eight hours before commencement of exercise activity, providing details of the Blue Forces' order of battle and strategy which, in his words, "would shoot down the whole exercise" if furnished to the Orange Forces[2]. The operation could not, of course, be cancelled because of the tremendous expense involved, so the Admiral asked the monitors to withhold the information for the time being. The incident did,

[2] Orange Forces - In Pacific exercises, the "enemy" forces were called Orange; in Atlantic exercises they were Red Forces.

however, serve as an object lesson. It was cited frequently in subsequent years to illustrate the need for COMSEC, and the dangers of careless communications.

23.18 The monitoring and analysis operation itself worked very well, possibly too well. Some authorities were so sensitive about the faults and shortcomings that showed up in their communications that they actually refused to have the reports disseminated. One Commander called in all copies, and asked his staff to "prepare a rebuttal". The verdict was "no rebuttal possible". On another occasion, air transport operations revealed so much information before an exercise got under way that the initial report caused the authorities involved to refuse to proceed unless a code was provided within a few hours to enable them to operate securely. This, of course, was impossible, and they eventually agreed to continue with the exercise, on condition that Air Transport Command (ATC) was not held responsible for security breaches. Thereafter an Air Transport Code was developed for them by T Group. Previously, they had maintained that their job was simply to move people and cargo like a commercial airline, and that they should not have to bother with security. When it became evident that their operations reflected much of the military action, they realized that they had to take precautions. There were many more instances of participants trying to talk around sensitive subjects - no one is capable of doing that successfully. "Veiled references" are no more than transparent subterfuges. An uninvited (or enemy) listener will no doubt be well trained in the art of interpreting vague terms and circumlocution, whereas the intended listener may be confused and ask questions seeking clarification, thus causing further unnecessary disclosure.

Various Deficiencies

23.19 The main problem experienced by the analysts was in obtaining sufficient material to analyse. Unable to secure authority to acquire personnel and facilities to do the monitoring, they were dependent upon "customers" to perform that function. The flow of traffic to CBNRC was spasmodic and irregular. Frequently the Committee Chairmen would appeal to the members to send material for analysis. The members would deplore the paucity of material forwarded; there would then follow promises and an exercise or two, but no sustained flow. Occasionally there would be traffic from several operations in the same time period, making it necessary to expand the section temporarily to four or five persons to cope with the analysis, but more often the staff had insufficient material for operation at full capacity.

23.20 At first, all traffic received was in the form of written drop copy. Later, magnetic tape recordings were submitted by the dozens, sometimes hundreds. As the section had no transcribing facilities, the tapes had to be sent to the RCN monitoring teams on the east or west coast for transcription. This introduced unacceptable delays; eventually the section acquired playback equipment, and some of the analysts put in idle time transcribing tapes. This did not sit well with the classification people in the personnel office, who insisted that since the analysts spent part of their time as transcribers, they should not be paid the full salary of analysts. Rather than accept a pay cut, the analysts discontinued transcribing, whereupon clerical and secretarial staff were pressed into service; these personnel, though very willing and cooperative, were totally unfamiliar with the "sounds" of voice radio and the jargon of communicators, and could not read manual Morse Code; accordingly the transcribing suffered. When large quantities of tape were received, they were sent once again to the RCN monitoring teams on the coasts. On one occasion the transcription was done at NDHQ and at the Forces' school in Kingston. Not surprisingly, some of these staffs resented having to do "other people's work", and this resulted in delays and unsatisfactory transcribing. The transcriptions were often incomplete because the monitor/interceptors did not realize what was important to the analysts, or were too busy doing other jobs to be able to pay full attention. Occasionally it appeared as though the tapes had been edited - the analysts suspected that "incriminating" evidence had been removed. Eventually a transcribing position was authorized, and a typist was hired and trained for the work. This enabled the staff to complete an analysis report on an exercise in a much shorter time. Eventually, too, some monitoring equipment - receivers and recorders - were acquired, and the staff grew to five members.

Concrete Applications

23.21 In the late 1950s, CBNRC had been called upon to do perhaps one analysis for each Defence Service per year, and occasionally one for External Affairs. As dedicated facilities became available, demands became more frequent. At first the Navy was the most frequent bidder for CBNRC analysts' services, while the Army and Air Force appeared reluctant to "wash their laundry in public". Later the Army caught up with and even passed the Navy, as interest in the monitoring service was generated during COMSEC courses held at CB for communicators. In the fall of 1965, a quantity of messages was collected at CFHQ from the National Survival Attack Warning System, and sent to CBNRC for analysis. In addition, a COMSEC monitoring and analysis report was made on the first Integrated Services exercise ("SOCKEYE") - a joint amphibious landing operation in the Queen Charlotte Islands off British Columbia.

23.22 Although many exercises were similar to others monitored and analysed before, there was also an interesting variety of operations, often providing something different to look at. Some involved only Canadian participants, some were Combined (Canada - US) exercises, and on some NATO exercises CB worked with NATO COMSEC units. By way of illustration, exercise FAIRPLAY was one of several occasions when CB staff went to North Bay to mount a COMSEC attack against NORAD communications; Exercise NIGHT SEARCH saw CB analysts participating in a NATO surveillance, counter-harassment and anti-submarine exercise in the "Iberian Atlantic" and Western Mediterranean; Exercise ROUGH RIDE was one of the NATO anti-submarine and convoy exercises worked on in the Western Atlantic; and there were exercises in the Pacific ranging as far west as Hawaii, and involving US naval forces. In addition, there were land forces exercises in the Maritimes ("WEBFOOT"); near Penhold, Alberta ("PRUNING SAW" - an ALCANUS operation); and on Vieques Island in the West Indies ("PRAETORIUM PACIS II"), as well as many others.

23.23 Some analytical undertakings involved no movements of troops, as for instance the study of Material Command facsimile traffic consisting of critical supply data. Another type of project would have the analysts examining the use of an operations code during an exercise, for instance by the 4th Canadian Mechanized Brigade Group (4 CMBG) in Europe, to evaluate the adequacy of the code. Still others had the COMSEC Analysis Section monitoring RCMP surveillance operations during the Commonwealth Prime Ministers' Conference and the Royal Visit.

23.24 These are only a few examples of the hundreds of monitoring/analysis exercises conducted by CBNRC, but will serve to provide an insight into the variety of tasks undertaken. As the commitments became more complex, the analysts learned new techniques and acquired better equipment. For example, when the period covered by this History was drawing to a close, S Group designed and constructed for them a Recorder Interface Unit - a voice-actuated facility which would allow up to twelve tape recorders to monitor telephone lines without any noticeable interruption to the lines. It was first tested during Exercise WINTEX in January 1975.

Summary

23.25 The COMSEC Analysis Section had great success in its prime role, but it had to overcome obstacles on the way. As with other COMSEC functions, the activities had to be justified, and there was the usual struggle for personnel and equipment. Perhaps the most difficult impediment encountered was the opposition of personnel evaluators. For years, the latter withheld recognition of the COMSEC staff as analysts on the ground that their work was not the same as that of SIGINT analysts. It was finally realized that COMSEC analysis can be even more exacting than SIGINT, partly because the people for whom the report is written know whether the observations and conclusions are correct or not (since they were involved in the action being reported), whereas the SIGINT customer must accept conclusions drawn by the analyst without being able to confirm their accuracy.

Chapter 24

TEMPEST

Annex:

Chapter 24 - TEMPEST

The Background

24.1 However secure a cipher system may be cryptographically, there is a risk that its security may be partly or completely nullified if an unauthorized person can intercept by acoustic or electronic means certain intelligence-bearing signals emitted during the normal operation of the equipment. COMSEC authorities became aware accidentally during World War II of the dangers of interception of clear text from cipher equipment by means of radiation and induction. Bell Telephone Company technicians in New York, commissioned to develop a cipher equipment for the US Services, stumbled upon the phenomenon in 1941. They thought they had produced a secure device, but discovered that each pulse triggered a reaction on another piece of equipment across the room. Testing showed that the same effect was produced on equipment across the street. Because of the exigencies of wartime, little attention was paid to the problem; a veil of secrecy was thrown over the subject, and an instruction was put out to ensure a 100-foot secure perimeter around such machines when they were operated.

24.2 After the war, COMSEC authorities found time to take another look at the problem. Years later the NSA Director for COMSEC (Paul Neff) told the Communications-Electronic Security Policy Committee (CSPC) that even during the war the US Service Authorities had considered radiation "one of the major and most pressing problems in COMSEC", but for various reasons, under the pressures of war conditions, progress and education in the field had been slow. In the ensuing years, technical knowledge was acquired, and testing techniques and specialized equipment were developed to deal with the problem. The problem of radiation of intelligence from cipher machines was recognized as highly dangerous, particularly in sensitive locations (i.e. where undetected interception could be undertaken within a radius of 200 feet). Much research into the problem was necessary because of the indefinite nature of the

s.15(1) - DEF

radiation, the number of factors involved, and the varying conditions existing at each location. The most effective defence was considered to be the design of crypto equipments which have inherently low radiation characteristics, and designers of new crypto devices sought to reduce the danger area from a 200-foot radius to a 20-foot radius. New crypto equipments were designed to meet specified standards, but communications and other electronic and electromagnetic equipment posed major difficulties. It was determined that all information-processing equipment radiated "unwanted" or "spurious" signals which were susceptible to unauthorized, surreptitious detection and exploitation.

24.3

Early CB Involvement

24.4 In the first three years of its existence, CBNRC was struggling to establish a COMSEC entity, a presence. In 1947 and 1948 a start was made in the crypto security aspects of COMSEC. Then in June 1948 GCHQ passed to CBNRC a British War Office warning that ROCKEX cipher machines were insecure in certain operating conditions because of radio frequency radiation. It was not until late 1948 that CBNRC technicians turned their attention to learning about the dangers of radiation and induction: they then began modifying CBNRC's crypto and communications equipments to prevent them from emanating spurious signals which might be radiated or conducted to distances where they could be detected and exploited by unauthorized persons.

24.5 The topic of radiation and induction security was at first referred to simply as "Radiation". Later, as policy on the subject became better defined, the unclassified word "TEMPEST" was applied to the investigation and study of compromising emanations - unintentional intelligence-bearing signals, which, if intercepted and analysed, disclose classified information being transmitted, received, handled, or otherwise processed by any information-processing equipment. The term TEMPEST was intended to refer to the problem as well as to measures to correct it, but has come to be used loosely in reference to any aspect of radiation or induction insecurity. There are two methods of dealing with the TEMPEST problem:

a) The design of new equipment to be secure against compromising emanations; and

b) Palliative measures to be taken with existing equipment to correct TEMPEST weaknesses.

24.6 Method a) above, the incorporation of TEMPEST security features into the design of crypto equipment, is a function of the design authority, and since crypto equipment used by Canadian Government agencies was almost exclusively produced in the UK or US, this area was not normally a major concern for CBNRC. However, Chapter 22 does reflect S Group's considerable responsibility for TEMPEST aspects during the production of the Canadian version of ALVIS, CID/610. In addition, in the acquisition of new crypto, communications, computer or other information-processing equipment, "built-in" emanation suppression had to be specified. Initially, however, the most pressing task was to find out what equipment and what locations were emanating intelligence-bearing information, and to devise and implement corrective measures. Method b), corrective measures, initially involved the shielding of cables, the employment of filters in power leads, bonding of the metallic sections of equipments and proper grounding. After 1949 additional information became available, and as new crypto equipment appeared, instructions were provided covering correct installation procedures to avoid TEMPEST hazards.

24.7 In the late 1940s and early 1950s, as indicated earlier, jurisdiction in the various areas of COMSEC was in dispute. The Communications Research Committee (CRC) exercised control of "cipher security policy" from the Committee's inception in June 1946, and its sub-committee, the Communications-Electronic Security Group (CSG), was formed in June 1948 "to deal with cipher security problems of user departments". The Services, for instance, felt that the CSG could recommend measures to be taken, but everyone wanted to be responsible for internal jurisdiction and directives within their own departments. Although agreement was reached in many areas, it would be ten years before any of the departments would formally involve CBNRC in TEMPEST investigations. Various local factors needed to be considered, such as the layout and complexity of the equipment, building construction, existing cabling, lighting circuits, telephone lines and even water pipes. The RCN considered the inspection of installations "an individual Service matter"; the Army "were firmly against the idea of a joint team" to check cipher facilities; the "RCAF felt a joint team, which would pool the best personnel of the three Services, would be much better than individual Service teams"; and "External Affairs felt that a number of teams would be required, if all the sites were to be checked in a reasonable period of time". Nevertheless, it was agreed that the radiation teams would require specialized training and standard equipment if they were to be really effective in their work.

24.8 Thus, in the beginning, T Group's TEMPEST responsibilities extended only to the crypto and communications installations in CBNRC. Cipher equipment parts and leads were grounded and shielded, and special enclosures were constructed to eliminate unwanted radiated and conducted signals. As T&D (Test and Design) progressed, they became the acknowledged Canadian experts in the field and their services were sought. By January 1949 they were assisting the Army with ROCKEX equipment. Two months later they designed an electronic relay to replace the telegraph relay used as an output device from the ROCKEX machine to the teletype ancillaries. The line relay had been found to "radiate badly".

Widening Responsibilities

24.9 Tests to determine the presence and strength of insecure radiation were conducted once a year within the CBNRC-controlled area, beginning in the LaSalle Academy in 1949. Standard communications receivers covering frequencies from 15 KHz to 400 MHz were used until 1955, when special radio interference/field intensity meters having an upper frequency of 1,000 MHz were procured for TEMPEST purposes. In 1957 additional equipment was purchased extending the upper frequency limit to 11,200 MHz. (Later information from the London Communications Security Agency (LCSA) recommended that tests for insecure radiation should cover all frequencies from DC to 100,000 MHz.) With these resources, T Group began testing electronic and electromechanical equipment to detect intelligence-bearing electromagnetic and acoustic emanations. All available TEMPEST information was obtained from LCSA. Before long CBNRC was being asked for assistance by other departmental communications offices. CB had been calling upon the various departmental authorities since 1949, and more urgently since 1954, to check closely on their crypto/communications installations, but all had been content to ask T Group for information and, in some cases, to send certain equipment to CB to be modified. Each expressed the view that it could handle its own problems, preferring not to establish a central team to perform the inspections and recommend remedial measures. The Army, in particular, had insisted on going its own way, conceding that all parties should pool whatever data their investigations yielded. CBNRC was asked to write up a report on the problem and to recommend test equipment which the various departments might acquire to test their own communications facilities. This was done, and in March 1955 the Army Member of the CSG reported that he intended to procure the recommended equipment, but that the Army still planned to deal with the problem on an "intra-Army basis". In August the RCN requested that a Canadian Interdepartmental publication be prepared to provide standard procedures for carrying out radiation tests. The RCAF Member said that since conditions varied so greatly from location to location it would be difficult to lay down hard and fast rules on the matter. The Army Member said that the CBNRC report and another from LCSA seemed to contain all available information. The Army intended to select one or two men, have them obtain practical experience at CBNRC or GCHQ, and then check out all their installations in Canada.

s.15(1) - DEF

s.15(1) - IA

24.10 Another inhibiting factor had been the fact that information on radiation was highly classified. SIGINT authorities hoped not to reveal to "potential enemies" any more information on the subject than they already possessed, for fear that they might take precautionary measures to prevent their equipment from radiating compromising signals, and so close off a valuable source of information. This caution was at such a level in 1948 and 1949 that crypto operators at CB were deliberately kept ignorant of the TEMPEST modifications made to cipher machines and, as a consequence, inadvertently counteracted the corrective measures on some occasions. The information was later downgraded to SECRET in order that it might be disseminated to those requiring it - based, of course, on the "need-to-know". The downgrading resulted from the consideration that security was of paramount importance and, although in the long run the intelligence community might suffer from corrective measures taken by the "enemy" which would preclude "our side" from exploiting their radiation weaknesses, it was considered necessary that all possible protection be given to classified information. No doubt, too, it was also realized that other countries were becoming aware of the dangers of electronic and acoustic emanations.

24.11 In 1954 the Department of External Affairs was planning to acquire off-line cipher equipment for its missions throughout the world, and consulted CBNRC regarding the advisability of purchasing a large number of ROCKEX Mark IV machines. T Group made an "informal commitment" to carry out tests on the device and to attempt to minimize the radiation danger. CBNRC was subsequently asked by the Chairman of the Cipher Policy Committee (CPC) to initiate tests and, if possible, to modify a Mark IV to improve the security of the machine. A small double-screened room had been acquired in 1953 to enable T Group to test devices in isolation without interference from nearby equipment. Initial tests using MF/HF communications receivers were carried out, and a modification devised for the Mark IV which lengthy testing proved to be effective in reducing the radiation problem. LCSA examined the proposed modification and agreed it would improve the security of ROCKEX IV very considerably. The detection radius was limited to 8 - 10 feet. Shielding of the ancillary printer and reperforator magnets further reduced this distance.

External Affairs bought 35 Mark IIIs, which were delivered between August and November 1956. In the following years GCHQ designed and produced a ROCKEX Mark V, which was a TEMPEST version of the Mark III. External Affairs, CBNRC and other users bought Mark Vs. Modifications were developed for converting the Mark IIIs to Mark Vs.

Organization for Dealing with TEMPEST

24.12 In April 1959 a separate section was formed within T Group to carry on a continuous study of radiation problems. Greatly improved techniques for testing had been developed, staff had been thoroughly trained in the use and servicing of the latest equipment, and several pieces of specialized equipment had been constructed in the Group. Laboratory tests to determine the extent of radiation had been made for various equipments including ROCKEX. At the request of other departments T Group investigated the radiation characteristics of a commercial tape recorder and reproducer (Stenorette), a wire recorder (Pierce), a UK-designed off-line cipher device (SINGLET), and a Norwegian on-line crypto equipment (ETCRRM). Reports were issued on each, and this was effectively CBNRC's foothold in the door as the centre of Canadian expertise on TEMPEST.

Page 1415

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 1416

is withheld pursuant to section

est retenue en vertu de l'article

15(1) - DEF

of the Access to Information

de la Loi sur l'accès à l'information

Interdepartmental Activities

24.15 The CSG set up a Radiation Working Party (CSGRWP) composed of representatives of the three Services, the Department of External Affairs and later the RCMP, with the Steering Member and Secretary provided by CBNRC T Group. The Working Party held its First Meeting on 2 March 1960 and, after reviewing the existing situation, drew up a list of crypto centre locations in the Ottawa area to be examined in a priority order based on sensitivity. The CSB, at its 26th meeting on 5 April, approved the recommendation that the Director CBNRC be asked to assume responsibility in Canada for carrying out field tests and for providing government departments with technical advice and assistance on radiation problems. Nine crypto centres were listed for immediate attention, and CB was able to complete preliminary field tests at all locations by the end of April. A consolidated report was submitted to the CSG summarizing the results of the site surveys and remedial recommendations. The CSB further agreed that CBNRC be authorized to request additional staff (5 positions) and facilities - equipment ($63,400) and annual recurring costs for personnel and travel. T Group were to conduct preliminary field tests for radiation at crypto locations in the Ottawa area and report to the RWP, who would submit a provisional report on faulty installations with recommendations for interim remedial measures. This was to be followed by a formal paper containing positive statements about the problem, with short-term and long-term proposals for the CSPC to study.

24.16 At this point CBNRC borrowed a 2 1/2-ton truck from the Army, modified it for testing operations, and fitted it out with very sensitive detecting and measuring devices[2]. When it was ready in September 1960, it was agreed that T Group should proceed with the second stage of the site surveys, rather than wait till authorities completed the implementation of the recommendations arising out

[2] See para. 24.13 for earlier field test

of the preliminary field tests. Surveys were conducted at the Rideau Annex, at the External Affairs Comcentre in the East Block of the Parliament Buildings, at the RCN and RCAF Comcentres in the NDHQ "temporary buildings" on Cartier Square, and at the RCAF Comcentre at Beaver Barracks. As funds became available, CBNRC bought a vehicle more suited to TEMPEST work - a 40-foot mobile home, well-appointed for travelling about the countryside, and equipped with a double-cell steel shielded enclosure. Called the Mobile Survey Laboratory (MSL), it was received in April 1961 and was taken to the Halifax area in late 1962, where radiation surveys were made of the CANFLAGLANT and CANMARLANT Comcentres. A complement of five staff members was required for such a task.

24.17 While the MSL was being fitted out with TEMPEST gear, arrangements were made to have NSA carry out radiation surveys of the Canadian Embassy and Canadian Joint Staff (CJS) premises in Washington. CBNRC staff participated in the surveys conducted at both sites, which took place in May 1961. T Group also provided advice to DND on the layout and equipping of the crypto centre in the new Canadian Joint Staff (CJS) Building in London. The MSL was equipped and ready to travel in 1962 when the screened enclosure at CJS(L) was ready for testing, but the "mobile lab" was too large to be loaded aboard an aircraft. With CBNRC staff assisting, GCHQ checked out the CJS(L) installation on our behalf. (Later the MSL did travel across Canada and to the US, field testing numerous Comcentre locations, and in later years a smaller vehicle was obtained and transported overseas to service Canadian Government installations abroad.)

Tests and Evaluations

24.18 In general, it was necessary to provide the user with a realistic appreciation of the dangers, to establish sound criteria and testing procedures, and to describe practical measures to be taken to overcome the dangers when recognized. Although CBNRC was not involved in the design of crypto equipment,

Page 1419

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

s.15(1) - DEF

s.15(1) - IA

implementation of the policies contained in CCB 470/2 could involve some financial expenditure, the approval of the Intelligence Policy Committee (IPC) had to be obtained.

24.20 It was considered necessary to reveal some general aspects of the radiation hazard to NATO nations; this resulted in the publication in March 1959 of AMSP 522, which dealt in general terms with the teletype problem only. For national purposes, NSA in May 1961 published NAG-1A/TSEC, entitled "Radiation Standard for Communications and Other Information Processing Equipment - Interim". (This was based on US MIL-STD-128, and was superseded in November 1963 by US Federal Standard 222, and in December 1970 and October 1974 by NACSEM 5100.) Copies were released to Canada. It covered specific COMSEC aspects of the radiation problem.

24.21

24.22 Other government departments leaned heavily on CBNRC for guidance and assistance. T Group responded by producing in 1962 the first Canadian document on the subject - CID/09/5 "Radiation (Electromagnetic and Acoustic Emanations)". Endorsed by the CSPC, the manual outlined the problem of interrelated spatial, conduction, magnetic and

s.15(1) - DEF

acoustical radiation, and recommended practices for the secure installation and operation of crypto and information-processing equipment. For the most part, it was still in use more than twenty years later (its successor, CID/09/5A, was published in 1985).

Corrective Measures

24.23 There was feverish activity in the early 1960s on two fronts in the war on TEMPEST problems: the testing of equipment and installations to detect vulnerabilities; and experimentation to devise countermeasures. T Group was in the middle of both campaigns. As surveys in the immediate Ottawa area were completed, tests were conducted further afield. Tasks begat tasks, however. Each survey revealed weaknesses that had to be corrected. Remedial measures would be taken, and then a repeat survey would be requested to ensure that the new arrangement was secure and that the corrective action had been effective.

24.24

s.15(1) - DEF

24.25 A primary cause of concern was the radiation from selector magnets in teleprinter and reperforator equipment. T Group designed and built shielded enclosures for magnets on both Creed (British) and Teletype (US) equipment, and this developed into a major project. The magnet shields were the 100 Kit for the Teletype Model 15 printer and reperforator and the 200 Kit for the Model 28 printer and reperforator; the 500 Kit was a photo-electric keyer for the transmitter-distributor and keyboard contacts; and the 600 Unit was a high to low level converter. Shielded enclosures were also developed for various devices such as recording equipment.

24.26

Expansion of TEMPEST Effort

24.27 With the ever-increasing number of COMSEC and communications devices being submitted for testing, and especially in view of the exploding workload associated with the Canadian production of ALVIS equipment, laboratory facilities had to be expanded. The screened room was moved and enlarged. Divorcing the technical/engineering responsibilities from T to form S Group in February 1964 enabled the latter to concentrate more fully on TEMPEST. The workload expanded, and in the next two years S Group was able to add six new staff members, although T Group had to surrender four positions to make this possible.

24.28 In order not to impede the program for the production of Canadian ALVIS equipment, the EAD (Electronic and Acoustic Detection) testing of prototype/pre-production models, and later of production models of the device, had to be given priority over other laboratory testing. As production progressed, several high precedence projects had to be postponed to enable S Group to keep up with the TEMPEST testing of CID/610. Soon the equipments were rolling off the production line faster than S laboratory could test them. The arrangement had been that CBNRC would test and evaluate the first ten off production, and one in every thirty thereafter, to ensure that the rigid production standards were being met and maintained as far as the cryptosystem and radiation characteristics were concerned. By the time fifty machines were rolling off the production line each month, S Group found that with no increase in staff its facilities were inadequate. Authorization was obtained to reduce the sampling rate to one in sixty, taking into account the fact that the test results to date had been so good. TEMPEST testing was completed in October 1967. The total production of CID/610s was 872 machines.

24.29 Although static installations were far more numerous, attention was also paid to mobile crypto facilities. In order to cater to tactical environments, the installers of cipher devices frequently departed from the normal interfacing arrangements, and this occasionally gave rise to unwanted coupling and degradation of the overall TEMPEST integrity. CBNRC was called upon in the early 1960s to inspect shipboard and aircraft installations, and more frequently in the late 1960s and early 1970s to test out aircraft and vehicle installations and to provide advice and support. Prior discussion and assistance during fitting reduced the amount of subsequent testing and re-engineering required to obtain a secure installation. This was particularly important when interfacing voice security equipment with special radios in vehicles, and in the case of cipher equipment (such as the TSEC/KW-7) installed in vehicles used as messages centres for tape relay operation (e.g. in the 4th Canadian Mechanized Brigade Group (4 CMBG)). There were instances, such as a proposed combination of a crypto device (KW-7) with a TEMPEST-modified radio for a "TACSAT Remote Facility", when CBNRC recommended that the combination of equipments not be used for processing classified information.

Acoustic Problems

24.30 Towards the end of 1965, S Group began to devote more attention to acoustics, as various government agencies expressed concern about acoustical radiation. This field had up till then been almost neglected, as emphasis had been put on electromagnetic emanations and conducted signals. NSA, too, considered acoustics investigation lowest in priority on their list, except where overseas sensitive locations were concerned. When CBNRC was asked for advice on protection "against possible coupling of structure-borne acoustic perturbations", it became necessary to acquire additional facilities and to build up a capability for assessing acoustics vulnerability. In time (1967), S Group designed its own anechoic chamber with advice from NRC's Applied Physics Division; it was constructed by the Council's Plant Engineering Division. However, little could be accomplished in the acoustics field, because other areas claimed the attention and efforts of the small

TEMPEST staff on a more urgent basis. All classified information-processing equipment users were clamoring to have their installations tested, and then re-tested after recommended changes were introduced. New types of equipment appeared on the scene, and had to be tested and modified to minimize the TEMPEST hazard before being put into use. Shielded enclosures were installed, with CBNRC advice and assistance, at various locations, such as at National Defence HQ, at the DND Mapping and Charting Establishment, at the Privy Council Information Centre, and at the Canadian Government Printing Office. S Group's participation consisted in providing technical advice and support to ensure the most effective COMSEC posture for these installations, monitoring the construction of a low-cost, built-in shielded enclosure, and ensuring the continuing integrity of the installation. The major use for large screened enclosures throughout the Government was to protect computers processing classified information.

Computer Security

24.31 Computer security was coming into its own in the mid-sixties. No ADP (Automatic Data Processing), or EDP (Electronic Data Processing) systems, as they later came to be called, had built-in TEMPEST protection. All, therefore, had TEMPEST problems. Retrofitting to correct their vulnerabilities was estimated to cost ten times what it would have cost to include TEMPEST protection in the original design. S Group undertook a TEMPEST evaluation of M Group's IBM 1401 computer, with its IBM 1403 printer and IBM 1402 card-read-punch, in the fall of 1965. They were able to conclude that vulnerabilities probably existed, but their detection capability was inadequate to the task of determining the extent of compromising emanations. With the acquisition of special detection devices, S Group was able to carry out proper tests in 1966 and 1967. Towards the end of the 1960s concern about the security of data processing equipment began to increase. At first, the problem had been viewed as one of unauthorized access to computer-stored information, and as such was not defined as a COMSEC matter. This changed, however, when it was realized that the solution might involve the use of cryptographic techniques and authentication procedures, that the data was usually transmitted from one point to another (even if only over a short distance), and especially when a manual issued by the Industrial Security Branch of the Department of Supply and Services (DSS) (setting out interim policy on the security of data processing systems) contained certain statements which were in conflict with current COMSEC policy and procedures.

24.32 Although there was considerable dispute as to where the responsibility for computer security lay, S Group prepared a document in draft form entitled "CBNRC Manual 100-1 - TEMPEST Guidance for Automatic Data Processing (ADP) Facilities", and circulated it to CSPC Members on 18 July 1969. After some discussion, the guidance was published in November as a Canadian Interdepartmental Document, "CID/09/8 - Guidelines for the Application of Compromising Emanations Control Procedures and Techniques to Automatic Data Processing (ADP) Facilities". This publication endured for sixteen years before being replaced by an updated document.

Documents About Radiation

24.33 In other areas too, S Group had been kept busy putting out information on aspects of radiation. In addition to CID/09/5, mentioned in paragraph 24.22, and reports on individual radiation site surveys, several other documents had been produced. As technology advanced, TEMPEST information was expanding, and new techniques and procedures were developed to deal with more recently developed devices. In January 1966, S Group prepared an informal handbook on the subject. Three months later, they produced a "Canadianized version" of a US publication entitled "Introduction to TEMPEST", which contained a wealth of valuable information in non-technical language.

24.34 CID/09/5 had, since its issue in 1962, provided the Canadian standard for installation practices. Gord Thomson attended a meeting of the CANUKUS Radiation Working Party in England in early 1965 which had been convened to establish a common radiation standard. CCB 470/2 (referred to in paragraph 24.19) had advocated limiting all radiation emanating from various sources in a communications/ crypto centre to a maximum of 50 feet. Each nation had a standard for installation practices with respect to crypto equipment. Standards were required for ancillary equipment and internal office signalling levels. It was agreed that the radiation limits given in the US Federal Standard No. 222 (FS 222) would provide an effective control over this aspect of the problem. FS 222, "Radiation Standard for Communications and Other Information-Processing Equipment" specified rigid standards for radiation suppression. The CSG Chairman recommended that Canada adopt the radiation limits in FS 222 for ancillary equipment. In the meantime, the proposals agreed at the CANUKUS Working Party meeting had been incorporated in a paper, CSG/P/42, entitled "Policy on the Control of Radiation of Intelligence-Bearing Energy by Communications-Electronic Equipment", and this had been approved by the CSPC. As a result of this new policy paper, CBNRC was directed to proceed with a Canadian version of FS 222. This meant that CID/09/5 would also require updating.

24.35 But now complications arose. Word from the US indicated that authorities there were considering some relaxation in the implementation of their national radiation policy. Fears were expressed, however, that, if Canada went along and permitted a degree of flexibility in its policy, such weakening in the rigid specifications might be interpreted by financial authorities as a lessening of the importance attached to the solution of the radiation problem. Nevertheless, it was agreed that the existing standard was excessively strict, and that the permissible limits could be adjusted to be more realistic. The preparation of the Canadian version of FS 222 was therefore halted until the revised US standard should be published. In the meantime, Canada would use the existing strict FS 222 limits. The controversy in the US continued over more than four years, as the various authorities could not agree on signal limits. In the interval, S Group had proceeded with the updating of CID/09/5. It was divided into two documents: CID/09/5 "Radiation, Electromagnetic and Acoustic Emanations", containing TEMPEST philosophy, i.e. the general and theoretical background information concerning radiation (SECRET, REGISTERED, revised version issued in March 1970); and CID/09/7 (Provisional) "COMSEC Installation Planning (TEMPEST Guidance and Criteria)", which provided the practical information required by field organizations (CONFIDENTIAL, NON-REGISTERED, issued 1 August 1968).

24.36 Finally, NSA decided in late 1970 not to issue a revised version of FS 222, but to replace it with the National COMSEC/EMSEC Information Memorandum (NACSEM) series of CELTS (Compromising Emanations Laboratory Test Standard) and other related TEMPEST publications. There followed NACSEMs 5100 through 5105, copies of which were issued to Canada via CBNRC. Rather than "Canadianize" these documents by modifying them to suit Canadian user requirements, it was decided to issue the NACSEMs to the Canadian COMSEC community in their existing form, but with the addition of a Canadian foreword to each publication which would, for example, direct the user to a Canadian rather than a US authority.

Workload Continues to Increase

24.37 Thus, the decade 1959-1969 was a hectic one for CBNRC's TEMPEST crew. Since CSB/82 had in 1959 given them responsibility for providing technical advice and support on all ELSEC (electronic emission security) matters, the workload had increased tremendously, but staff levels had risen only slightly. When they took to the road in 1960, five additional positions were authorized - five technicians being needed for a site survey using the TEMPEST vehicle. These personnel were also responsible for EAD testing in the laboratory and for writing TEMPEST reports. When the number of site surveys required two teams on the road, staff members were borrowed from other S Group sections and from

T Group. Often a TEMPEST team went out short-handed. Three units were involved: the Field Survey Unit which visited dozens of sites each year taking readings and measurements; the TEMPEST Laboratory Unit which conducted evaluations of crypto, communications and other information-processing equipment submitted by various government agencies; and the Analysis Unit which studied the results of site surveys and laboratory tests and determined the extent of vulnerability and risk. Later a fourth unit, the Acoustic Laboratory, was added. All this with a total staff of ten! Personnel were traded back and forth month by month, sometimes week by week or day by day, as the workload ebbed and flowed. To keep the strength up to ten, two technicians were taken from T Group in 1964, another in 1966 and two more in 1968; the only way to acquire more staff was by larceny. Horse-trading was furious in the latter half of the 1960s, because many of the same people were required for both crypto-checking and TEMPEST testing of Canadian-produced ALVIS equipments. Since these technicians also were involved in field survey operations, many requests for assistance had to be denied or delayed because ALVIS took precedence and no more staff could be hired. Further, when the Government austerity program temporarily reduced the overall CBNRC establishment from 600 to 583 (2.8%) in October 1969, and to 563 (3%) in 1970[4], COMSEC lost ten positions (6.2%); the TEMPEST staff was cut by one - a ten percent reduction.

24.38 Periodic TEMPEST field surveys were conducted at intercept and D/F stations such as Coverdale, Gloucester, Leitrim, Masset, Gander and Bermuda; on ship installations (HMCS Bonaventure, HMCS Ottawa, etc.) and TOBACCO systems in Halifax; on helicopter and long range aircraft installations in Halifax and Ottawa; at the underground SAGE (Semi-Automatic Ground Environment) complex at North Bay; at the Department of Justice Jurimetrics installation; at the DND/IHA (Information Handling Agency) Data Centre at Tunney's Pasture; at the Privy Council Information

[4] See end of para. 3.5

Centre and External Affairs Cipher Facility; at RCMP Comcentres in Ottawa, Vancouver, Victoria, Charlottetown, Fredericton, Moncton, and Halifax; at the 4th Canadian Mechanized Brigade Group in Lahr, Germany; and at many other locations.

24.39 Manpower became the limiting factor on the services that could be provided to customers. The demands for surveys multiplied to the point where the existing staff could not cope with them all; but requests for additional personnel were frustrated. Realizing that the staff could not continue on an overworked/understaffed basis, S Group Head proposed to the Assistant Director COMSEC in January 1975 that CBNRC withdraw from routine TEMPEST field survey projects; instead, S Group would offer to train personnel from other government departments and agencies to conduct surveys of their own installations. S Group had in fact been providing TEMPEST training courses for several years, both as part of the COMSEC Training Program and also on an ad hoc on-request basis. They began planning the development of additional TEMPEST courses for departmental COMSEC authorities. They advocated this expanded training role in accordance with the general policy that, as the national TEMPEST authority, CBNRC should direct its expertise more towards providing advice and guidance than in actual involvement in routine TEMPEST field surveys. Actual TEMPEST operations would consist in conducting simultaneous testing projects in the two shielded enclosures, and carrying out only occasional special field surveys.

24.40 Within two months an additional eight positions were allocated to S Group, and the routine TEMPEST field surveys continued. DND, RCMP and External Affairs had looked into the possibility of setting up their own TEMPEST teams and facilities, but had quickly decided that it would be too expensive and too great an undertaking. Instead, each offered to provide CBNRC with one or two positions from their own establishments if CB would continue doing the surveys. CBNRC accepted, and while the other departments were "finding" the positions (later called PYs - person years), eight positions were borrowed from other sections in S and T. Typically, however, it was several years before some of the promised positions were made available; some in fact never appeared, and the other T and S Sections were not recompensed.

24.41 By 1971 it had become obvious that additional TEMPEST test facilities would soon be required. The single laboratory facility at CBNRC would be inadequate to handle the peak workload in the time-frame available for projects such as DND's SAMSON program. SAMSON equipments and configurations would require so much TEMPEST testing, the CSG was told, that several test facilities would be required. The only existing alternative to CBNRC was the DND Quality Assurance Branch, but its facilities proved to be too small and its staff "did not possess sufficient expertise". On the other hand, it was doubtful whether there would be sufficient work on a continuing basis to justify establishing a government test laboratory large enough to cope with projects such as SAMSON. Equipment associated with satellite communications likewise would require testing at various stages of design, development and fabrication. Certain Canadian companies had expressed interest in the production of crypto equipment for sale or export on the open market; procedural or software techniques intended to provide security or privacy protection were being promoted; all these required, in addition to crypto evaluation, assessment from a TEMPEST viewpoint, especially if the interests of the security and intelligence community were affected. Much of this testing would have to be done by CBNRC. Some thought was being given, however, to having some of the equipment testing done by suitably cleared commercial firms. Nothing along these lines transpired, however, during the rest of the period covered by this History.

ELSEC Responsibilities of CBNRC

(Extract from Memo CB 3-9, dated 4 March 1960)

f) To provide technical advice and support, as required or as directed, to government departments and agencies on COMSEC and ELSEC matters generally, including advice on the interceptibility of electronic emissions and radiation hazards and associated countermeasures.

g) To prepare plans, estimates and studies associated with COMSEC/ELSEC activities and to draft technical papers and reports on varied aspects of COMSEC/ELSEC as required.

h) To conduct liaison on the technical and operational aspects of COMSEC/ELSEC with appropriate Canadian and collaborating agencies.