Canadian SIGINT Contributions to the UKUSA Partnership

Coridon Henshaw

Overview

Within the archipelago of Canadian intelligence organizations, responsibility for signals intelligence (SIGINT) processing rests with the Communications Security Establishment (CSE). Founded in 1947 as the Communications Branch of the National Research Council (CBNRC), the CSE acquired its current name in 1975 when its operations were transferred from the NRC to the Department of National Defence (Robinson 2001). Today, the CSE is “Canada’s largest and costliest intelligence organization,” likely the most secretive intelligence organization in Canada, “and [also] the main provider of foreign intelligence to the Canadian government.” (Rudner 2001 p.97) The CSE's SIGINT mandate[1] gives it responsibility to monitor, in support of Canadian policy objectives, a wide range of electronic signals including communications, “non-communications emissions such as radar,” and telemetry. CSE's mandate to monitor is “restricted to foreign emissions under the Canadian government definition,” although, notably, the definition of 'foreign emissions' has never been made public. (Robinson 2001)

Since the dawn of Canadian SIGINT capabilities during World War II, Canadian SIGINT work has been conducted in close cooperation with SIGINT agencies in the United Kingdom and the United States; the CSE has continued this tradition of cooperation as a member of the UKUSA partnership. The UKUSA partnership is an “international collaboration” based on a collection of highly secret memoranda of agreement between the United States, the UK, Canada, Australia, New Zealand and several additional minor players. Under the UKUSA agreements, the signatory countries exchange and share SIGINT intercepts, analysed intelligence products and SIGINT monitoring technologies. (Rudner 2001 p.97) The participation of CSE (on behalf of Canada) within the UKUSA alliance means that the CSE 'exports' Canadian SIGINT intercepts and analyzed intelligence to the alliance in exchange for access to SIGINT intelligence and intercepts

1 The CSE has an information security (defensive cryptography, anti-hacking, network security, etc) mandate independent of its SIGINT responsibilities. Discussion of the CSE's INFOSEC mandate is beyond the scope of this paper.

from other UKUSA partners. The net result of this cooperation is that the “UKUSA alliance provides CSE with a shared global capacity to collect and deliver real-time” SIGINT “intercepts on targeted objectives to selected clients within the Government of Canada” (Rudner 2001 p.103) on a scale that would not be possible if the CSE were to rely solely on its own resources. This paper will discuss known CSE intercept sites, likely CSE contributions to the UKUSA partnership as extracted from these monitoring sites, and the prospects for the CSE's future contributions to UKUSA given the transition of communications from radio/satellite to fibre optics. While it is possible to make educated guesses on what CSE contributes to UKUSA, due to a lack of published information, it is not possible to make any assessment of the true 'balance of trade' between the CSE and UKUSA as it is unknown what intelligence data the CSE actually receives from its UKUSA partners.

CSE Intercept Sites

SIGINT interception for CSE use is conducted from four fixed installation sites in Canada and an indeterminate number of covert or low-profile listening posts overseas . The four fixed installations—at Leitrim (Ontario), Alert (Nunavut), Gander (Newfoundland) and Masset (BC)—are operated by “about 1,000” Department of National Defence military personnel belonging to the Canadian Forces Information Operations Group (CFIOG) “working under the overall direction of CSE.” (Rudner 2001 p.108) (Robinson 2001) Interception efforts at these sites are designed to collect “terrestrial, microwave, radio, and satellite communications along with other electromagnetic emissions.” The intercepted information is then processed by means of a “technologically advanced computer” system which is “programmed to search for specific telephone numbers, voice recognition patterns, or key words, and to decrypt text.” (Rudner 2001 p.103)

Topologically, CFS Leitrim is the headquarters for SIGINT collection while the sites at

Gander, Masset and Alert are outstations. The Gander, Masset and Alert sites have been “fully automated” since the late 1990's and are controlled from CFS Leitrim. (Rudner 2001 p.108) Even though CFS Alert is remotely controlled, it remains staffed so as to facilitate equipment maintenance, and also, presumably, for security reasons. Permanent staffing levels at Gander and Masset are unknown, although Google Earth imagery has shown a small number of cars to be present at both sites.

Located on the north east of Queen Charlotte Island (Google Earth coordinates 54.0288, -132.0653), the CFS Masset interception site is equipped with an AN/FRD-10 HF direction finding (HF-DF) receiver, modified at least to allow remote control, and no other obviously visible SIGINT hardware. The FRD-10 was designed to receive and locate HF radio transmissions[2] and is not useful for monitoring more modern, higher frequency, communications such as those used by satellite systems. (Robinson 2005)

In the east of Newfoundland (Google Earth coordinates 48.9497, -54.5246) sits the CFS Gander intercept site. Like CFS Masset, Gander is equipped with an AN/FRD-10 (Robinson 2005). In addition, approximately 4km north-north east of the AN/FRD-10, there appears to be one satellite dish hidden under a radome. (Google Earth coordinates 48.9862, -54.5037) The connection of this facility, if any, to Canada's SIGINT infrastructure cannot be determined.

In the far north of Nunavut, CFS Alert (Google Earth coordinates 82.4163, -62.6051) is the northernmost permanently populated place on Earth—Canada's northernmost SIGINT station. There is little confirmed information available regarding SIGINT capabilities at CFS Alert. Alert is believed to be equipped with a AN/FRD-13 Pusher HF-DF system (a smaller version of the AN/FRD-10 arrays located used at Gander and Masset) as well as assorted receivers suited for intercepting HF and VHF[3] transmissions (Proc 2007). Signs of HF and VHF interception

2 The HF band is defined as covering frequencies from 3 Mhz to 30 MHz.
3 The VHF band is defined as covering frequencies from 30 MHz to 300 Mhz.

capabilities, other than an AN/FRD-13, can easily be confirmed through inspection of photographs taken by Urosveic of the Alert antenna complex situated on Polaris Hall. Further, the location of Alert could make this site useful for monitoring traffic from Russian polar communications satellites located in polar or Molniya orbits. There is, however, no evidence of satellite monitoring capabilities at Alert.

As for interception capabilities at Letrim (in the south of Ottawa at 43371, -75.5871) itself, Google Earth imagery captured in 2007 indicates that Leitrim is equipped with six satellite dishes and what may be either an active AN/FRD-13 HF-DF installation or the remains of a decommissioned AN/FRD-13 installation. Of the satellite dishes, two are of "no more than roughly 12m" in diameter" (EUP p.57) and are concealed by radomes. The remaining four dishes are of notably smaller diameter; two of these are under radomes while the other two are unprotected. The lack of a concealing radome on two dishes suggests they are used for communications (for example, to control Alert, Gander and Masset) rather than as interception tools. Unconcealed satellite dishes are of dubious use for interception purposes as a trained observer can determine which satellite a given dish is monitoring—and, more to the point, determine which satellites are *not* being monitored from a given listening post. While an AN/FRD-13 HF-DF system was known to have been constructed at Leitrim (Robinson 2005), its current status is unclear; as the installation site is rather overgrown the Leitrim AN/FRD-13 may no longer be in use.

Very little information is available regarding CSE interception capabilities outside Canada. It is known, however, that, during the 1970s, the CSE did install mini-listening posts in Canadian diplomatic missions for the purpose of intercepting microwave and mobile phone communications within the host country. It must be noted, however, that the impetus, training, targeting cues and equipment used by embassy-based SIGINT operations was provided by US

NSA. (Rudner 2001 p.p. 106-107.) In this light, it is unclear whether CSE embassy-based SIGINT should necessarily be considered a CSE project/capability per se rather than an NSA project conducted by proxy.

More recently, the CSE has publicly admitted its involvement in intelligence operations targeted at Taliban forces in Afghanistan. (CCSE p.2) It is self-evident that CFIOG and/or the CSE must have a deployable strategic interception capability established in Afghanistan to collect raw data to be analysed by the CSE's analytic wing.

Finally, CSE/CFIOG should be assumed to operate some cable taps on Canadian soil against “foreign emission” targets on Canadian territory, such as foreign diplomatic missions. The extent of such monitoring, how it is conducted, where it is conducted and by whom (CSE, CFIOG, other agencies, etc.) has not been admitted and cannot be determined.

CSE contributions to UKUSA

Owing to the secrecy of the UKUSA pacts and UKUSA operations, little confirmed information is available regarding CSE contributions to UKUSA. Enough information is available, however, to make a number of educated guesses.

From 1957, when the CBNRC/CSE abandoned efforts at cryptanalysis and signals decryption to when the CSE upgraded its computers and returned to the decryption game in 1985, Canadian contributions to UKUSA would largely have been limited to something close to “that of a mere supplier of raw intercepts” collected first by virtue of the quiet RF radio environment in the Canadian hinterlands and Canada's geography in relation to to the USSR and (from the 1970's onward) by SIGINT listening posts in Canadian diplomatic missions. (Rudner 2001 p.103, p.111) While the CBNRC/CSE no doubt produced and exported UKUSA at least some fully analysed intelligence product, the fact that most governmental/military traffic of intelligence interest during the Cold War period will have likely been encrypted, it is fair to assume that the bulk of actual

analysed intelligence produced from CBNRC/CSE intercepts will have been created by other UKUSA partners with cryptanalysis/decryption capabilities.

Until the 1960's, the majority of exported raw SIGINT intercepts likely would have been captured HF radio traffic. Until the 1960's, most long-distance telecommunications traffic worldwide “was carried by” HF radio. HF radio signals—often known as short-wave signals—have a planet-spanning range by virtue of being being able to bounce repeatedly between the ground and ionosphere. Signals from a sufficiently powerful HF transmitter can, in good conditions, be received on the other side of the world. Because of their extreme range, all that is required to intercept any HF signal broadcast in a large region is a sufficiently large antenna coupled to a sufficiently sensitive receiver located, ideally, in a “'quiet' radio environment” where minimal radio interference is present. (Rudner 2001 p.101) In the case of Canadian SIGINT operations, Masset, Gander, Alert, and other now-closed SIGINT stations, fulfilled the requirements for a quiet radio environment while the AN/FRD-10 and AN/FRD-13 systems fulfilled the requirements for sensitive receivers. Combined, the virtues of geography and high-quality receivers meant that Canada was well-suited to deliver raw intercepts of HF communications in the northern USSR, East Asia, and from ships active in adjacent waters. Specific targets during this period included “Soviet air force and air defence communications across the northern USSR.” (Rudner 2002 p.101) The resulting intercepts were “strategically vital” in the “polar theatre by way of providing distant early warning of the Soviet order of battle and potential first strike capability.” (Rudner 2001 p.106)

Since the 1960's, HF radio has increasingly fallen into disuse in favour of higher frequency transmissions in the VHF band and beyond. The move to higher frequencies will have caused a paradigm shift in SIGINT operations because higher frequency signals have less range. Where HF signals can bounce between the ground and ionosphere to provide a potentially global

range, VHF and higher frequencies are limited to line of sight between transmitter and receiver, or roughly 100km if reliable reception is to be expected[4]. Intercepting VHF and beyond requires either extremely sensitive, and extremely expensive, SIGINT surveillance satellites (which Canada does not possess) or close-range covert monitoring equipment located within the line of sight of each transmitter of interest. (EUP p.33) The need for close proximity monitoring VHF and higher frequency communications was almost certainly the impetus for the 1970's project of installing clandestine monitoring stations in Canadian diplomatic posts overseas:

> since most countries' microwave telecommunications networks converged on their capital cities, clandestine embassy-based listening posts were especially well situated to monitor their host nation's domestic and even international communications. (Rudner 2004 p.576)

Presumably, raw intercepts collected by these posts will have been provided to the UKUSA partners. Since the decline of HF use, raw intercepts gathered from embassy posts likely comprised the bulk of useful intercepts exported by CBNRC/CSE to the UKUSA partners.

In 1984, the CSE installed its first SIGINT satellite monitoring dish at Leitrim. Reportedly, this installation was part of a coordinated UKUSA effort to create an linked network of ground stations to "maintain global [interception] coverage" of Intelsat traffic. The CSE satellite monitoring station is "ostensibly targeted on Latin American satellite communications." (Rudner 2001 p.110-111) While it is easy to assume that Leitrim satellite SIGINT is fed to UKUSA partners, it must be noted that there is no geographic reason for Leitrim to engage in satellite SIGINT in the UKUSA context. (EUP p.57) Geographically, any satellite that could be monitored from Leitrim could be monitored just as easily from stations in the United States. Given the US-centric nature of the UKUSA agreement, there is little reason for the Americans to out-source satellite SIGINT collection which they could perform themselves. It is possible,

4 Under fortuitous circumstances, VHF signals can bounce back from the upper atmosphere and be received at distances beyond line of sight. This effect is dependent on such things as solar activity, meteors, and other unpredictable phenomenon. Interception of VHF at ranges beyond line of sight is possible on an irregular, recurring, basis but is by no means predictable or reliable.

however, that the Leitrim SIGINT site is intended to serve as a backup to US monitoring stations in the event of planned system maintenance, failure or attack. That said, in the final assessment, the quantity and importance of Canadian contributions of satellite SIGINT to UKUSA are indeterminate given the US-centric nature of the alliance. It's possible that the four interception dishes present at Leitrim as of this writing may well be used primarily for CSE-internal purposes rather than as part of a broader UKUSA operation.

The most notable change to CSE capabilities in the 1980's with regard to the UKUSA alliance was the recreation of a cryptanalysis infrastructure at CSE. In 1985, CSE bought a Cray X-MP/11 vector supercomputer for cryptanalysis. (Rudner 2001 p.111) For the first time since at least 1957, the CSE had the technological capability to decrypt and analyse cryptographically protected signals internally rather than merely shipping the raw intercepts to the American NSA (or possibly the British GCHQ) for decryption. While hard details on contemporary CSE computational capacity have not been published, all appearances are that CSE has continued to keep its technological capacity up to date: when, for instance, the alleged “NSA main computer” was inoperable “for four days in January 2000,” the “CSE was likely to have been involved,” alongside other UKUSA partners, in processing SIGINT intercepts on behalf of the NSA. (Rudner 2001 p.113) This would not have been possible if CSE computational capabilities were not capable of processing at least some modern encrypted signals of the kind the NSA would find worth breaking. As such, it can fairly be assumed that the CSE has been capable of producing, and very likely has produced and exported, exporting analysed intelligence product based on decrypted SIGINT from approximately 1985 onwards.

Conclusion

From providing a geographically useful location for early Cold War HF monitoring of the USSR, to more recent computational assistance to the NSA, the CSE has had a fairly long history

of SIGINT monitoring and making substantive contributions to the UKUSA alliance. Whether the CSE will continue to make useful SIGINT contributions to UKUSA is uncertain due to changes and advances in communications technology. The shift of increasing percentages of long-range communications to and from fixed sites away from radio and satellite to fibre optics will limit the utility of conventional SIGINT methods in the upcoming century. While fibre optic links can be tapped, this requires physical access to the fibre in order to attach a monitoring device. Doing such things in Canada with legal permission is easy; doing such things in a clandestine fashion overseas is extremely difficult. As such, the shift to fibre could well mean the contraction of the CSE's sphere of detection from its high point of being able to monitor the entire northern USSR from Alert to something akin to an oversized police force able to monitor only foreign traffic originating, terminating, or transiting through fibre optic lines on Canadian soil. Time, and technology, will tell.

Bibliography

CCSE. "Speech to Université Laval Students - 6 February 2007." 30 July 2007. <http://www.cse-cst.gc.ca/documents/publications/ccse-speech-e.pdf>

(EUP) European Parliament. (2001). *Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)*. 30 July 2007. <http://www.fas.org/irp/program/process/rapport_echelon_en.pdf>

Google. Satellite imagery of CFS Gander SIGINT station. 30 July 2007 <http://maps.google.ca/maps?f=q&hl=en&geocode=&q=Gander,+nl&ie=UTF8&ll=48.951317,-54.524642&spn=0.005066,0.010085&t=k&z=17&om=1>

Google. Satellite imagery of CFS Leitrim. 30 July 2007 <http://maps.google.com/maps?t=k&hl=en&ie=UTF8&ll=45.337004,-75.5873&spn=0.005347,0.010085&z=17&om=1>

Google. Satellite imagery of CFS Masset SIGINT station. 30 July 2007 <http://maps.google.ca/maps?q=Masset,+BC&ie=UTF8&oe=UTF-8&ll=54.028003,-132.066607&spn=0.009062,0.02017&t=h&z=16&om=1>

Proc, Jerry. "CFS Alert." 15 Feb 2007. 30 July 2007. <http://jproc.ca/rrp/alert.html>

Richelson, Jeffrey. "Desperately seeking signals." *Bulletin of the Atomic Scientists* 56.2 (2000): 47-51.

Robinson, Bill. *Lux Ex Umbra: Monitoring Canadian signals intelligence (SIGINT) activities past and present.* 30 July 2007 <http://luxexumbra.blogspot.com>

Robinson, Bill. (2001). "Communications Security Establishment Unofficial Webpage." 30 July 2007. <http://web.archive.org/web/20040402074658/http://watserv1.uwaterloo.ca/%7Ebrobinso/cse.html>

Robinson, Bill. (2005). "The FRD-10: An endangered species." In *Lux Ex Umbra: Monitoring Canadian signals intelligence (SIGINT) activities past and present.* 30 July 2007. <http://luxexumbra.blogspot.com/2005/06/frd-10-endangered-species.html>

Rudner, Martin. (2001). "Canada's Communications Security Establishment from Cold War to Globalization." Intelligence & National Security, 16:1, 97-128

Rudner, Martin. (2004). "Britain Betwixt and Between: UK SIGINT Alliance Strategy's Transatlantic and European Connections." Intelligence and National Security 19.4. 571-609.

Urosveic, Alex. "High alert." *Toronto Sun* November 14, 2004 Rpt. online. 30 July 2007 <http://www.canoe.ca/NewsStand/TorontoSun/News/highalert.html>