TRÈS SECRET

Nº de dossier : 2800-173
(TD R526)

COLLABORATION DU SCRS AVEC LE CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS CANADA (CSTC)

(ÉTUDE DU CSARS 2012-05)

Comité de surveillance des activités de renseignement de sécurité
6 mars 2013

TABLE DES MATIÈRES

1 INTRODUCTION

La relation entre le Service canadien du renseignement de sécurité (SCRS) et le Centre de la sécurité des télécommunications Canada (CSTC) a considérablement changé au cours des cinq dernières années. Même si autrefois ces deux entités fonctionnaient principalement comme deux solitudes au sein du domaine du renseignement canadien, l'intensification de la demande du gouvernement pour des renseignements en vertu des articles 12 et 16 a obligé le SCRS et le CSTC à mieux coordonner leurs stratégies et leurs processus de collecte de renseignements. Cet examen porte sur les avantages pour le SCRS que représente une collaboration accrue avec le CSTC, et sur les initiatives opérationnelles et non opérationnelles.

L'examen commence par un aperçu du mandat du CSTC et des caractéristiques uniques de l'alliance internationale dont le CSTC est membre. L'examen se penche ensuite sur l'état de la coopération entre le SCRS et le CSTC, . Comme c'est le cas chez un nombre croissant d'alliés du Canada, on a rapproché le monde du renseignement électromagnétique et le monde du renseignement d'origine humaine afin de suivre l'évolution des menaces et de maximiser l'efficacité du renseignement. Dans l'ensemble, le Comité a été impressionné par les avantages que représente une collaboration plus étroite avec le CSTC pour le SCRS et convient qu'une collaboration plus étroite est à la fois souhaitable et utile.

L'examen porte ensuite sur certains des défis que pose l'accroissement de la coopération. Il s'agit notamment de coordonner les services organisationnels; d'assurer un transfert interorganisationnel des connaissances adéquat; de gérer les risques opérationnels; ; et de veiller à ce que les directives et les politiques destinées à orienter l'échange de renseignements entre le SCRS et le CSTC soient adéquates.

La dernière section de l'examen cerne une anomalie dans leur relation, à savoir un manque de coopération en matière de cybersécurité. L'étude se termine par une recommandation encourageant le SCRS à établir des principes généraux plus rigides à l'égard de la coopération avec le CSTC.

2 MÉTHODOLOGIE ET PARAMÈTRES

Cet examen a porté sur la récente évolution de la relation entre le SCRS et le CSTC. Le CSARS a examiné les changements apportés aux ententes et aux politiques régissant le partenariat, ainsi que les pratiques et les procédures en matière d'échange de renseignements. Plus particulièrement, le CSARS a évalué un échantillon d'initiatives opérationnelles conjointes du SCRS et du CSTC afin de donner un aperçu de la façon dont ces opérations ont amélioré les activités de collecte du SCRS, et a examiné un large éventail de documents ministériels afin d'aider à mettre en contexte la coopération sans précédent entre ces partenaires.

Le CSARS a également assisté à plusieurs séances d'information avec des employés de niveau opérationnel et des cadres supérieurs, et a eu l'occasion de parler à un employé du CSTC travaillant au Service dans le cadre du programme de détachement.

La période d'examen de base s'est déroulée du 1er janvier 2011 au 31 mars 2012, bien que certains renseignements collectés hors de cette période aient été pris en considération afin de mieux comprendre les enjeux importants.

3 COMPRENDRE LE CSTC

Le CSTC est le principal fournisseur de renseignements étrangers destinés au gouvernement du Canada. Issu des développements cryptographiques de la Deuxième Guerre mondiale[1], le CSTC a été officiellement fondé en 1946 sous le nom de « Direction générale des communications » au sein du Conseil national de recherches du Canada. Le CSTC a reçu son nom actuel en 1975 après son transfert au portefeuille de la Défense nationale. Le gouvernement du Canada a reconnu publiquement l'existence du CSTC en 1983, mais ce n'est que lorsque le Canada est intervenu en Afghanistan que le CSTC a suscité l'attention du public[2].

3.1 Mandat du CSTC

Le CSTC recueille, analyse et produit des rapports sur le renseignement électromagnétique (SIGINT), terme donné aux renseignements recueillis au moyen de l'interception et de l'étude des transmissions radio, par fil, par radar, par télécommunications et par d'autres moyens électroniques[3]. Les responsabilités du CSTC découlent de trois mandats :

A) Acquérir et utiliser l'information provenant de l'infrastructure mondiale d'information dans le but de fournir du renseignement étranger, en conformité avec les priorités du gouvernement du Canada en matière de renseignement;

B) Donner des conseils, des directives et des services qui faciliteront la protection des renseignements électroniques et des infrastructures d'information revêtant une importance pour le gouvernement du Canada;

C) Fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité, dans l'exercice des fonctions que la loi leur confère[4].

En vertu de la loi canadienne, les activités du CSTC ne doivent pas être dirigées contre des Canadiens ou des personnes se trouvant au Canada. Toutefois, lorsqu'il recueille des SIGINT en vertu du mandat A, le CSTC peut acquérir fortuitement des renseignements personnels sur des Canadiens. Ces renseignements peuvent être conservés s'ils sont jugés essentiels à la compréhension des renseignements étrangers, et ils peuvent être inclus dans les rapports communiqués au SCRS, pourvu qu'ils soient limités[5]. Les activités menées en vertu du

[1] Le terme cryptographie renvoie à la science de la protection de l'information par le chiffrement. Cette science s'est accélérée au cours de la Deuxième Guerre mondiale en raison de l'émergence d'organismes professionnels voués à la création de codes (cryptographie) et au bris de codes (cryptanalyse).

[2] Le 16 novembre 2011, le CSTC a été établi en tant qu'organisme autonome. Ce changement administratif a fait en sorte que le chef du CSTC est devenu un administrateur général et un administrateur des comptes, qui relève directement du ministre de la Défense nationale. Avant ce changement, le chef relevait du conseiller à la sécurité nationale. Le Bureau du Conseil privé sur les questions stratégiques et opérationnelles relevait du sous-ministre de la Défense, sur les questions administratives et financières. Cette nouvelle désignation n'a entraîné aucun changement de mandat, et le CSTC est demeuré dans le portefeuille de la Défense nationale.

[3] Le SIGINT est constitué du renseignement individuel ou en combinaison sur les communications (COMINT), du renseignement électronique (ELINT) et du renseignement tiré de signaux d'instrumentation étrangers (FISINT). Se reporter aux « Normes canadiennes de sécurité SIGINT », Coopération du SCRS dans le dossier 520-47 du CSTC, vol. 3.

[4] Loi sur la défense nationale, par. 273.64(1), dernière modification le 6 mars 2012.

[5] Les renseignements « limités » masquent le nom des Canadiens ou des entités canadiennes.

mandat C (Soutien à l'accès légal) exigent que le CSTC agisse à titre d'agent du ministère ou de l'organisme qui demande de l'aide; toutefois, le CSTC ne conserve pas les renseignements.

Le CSTC participe à une collaboration internationale et à des échanges de renseignements dans le cadre d'un accord spécial SIGINT avec la National Security Agency (NSA) des États-Unis, le Government Communications Headquarters (GCHQ) du Royaume-Uni, la Defence Signals Directorate (DSD) de l'Australie et le Government Communications Security Bureau (GCSB) de la Nouvelle-Zélande. Les méthodes de collecte utilisées par cette alliance sont de nature très délicate,

3.2 Fusion du SIGINT et du HUMINT

Les services de renseignement SIGINT et d'origine humaine (HUMINT) sont depuis longtemps considérés par les professionnels du renseignement comme des entités exerçant généralement des rôles mutuellement exclusifs, quoique complémentaires. Le SCRS, qui compte sur HUMINT, a comme mandat principal le renseignement de sécurité; il a également un mandat limité l'autorisant à recueillir des renseignements étrangers et peut recueillir ces renseignements seulement *au sein* du Canada. Le CSTC – un organisme du SIGINT – a pour mandat principal le renseignement étranger et ne peut pas diriger ses activités contre des Canadiens ou des personnes se trouvant au Canada. Pendant près de deux décennies, ces organismes de renseignement ont fonctionné en grande partie de façon isolée.

Avant l'adoption en 2001 de la *Loi antiterroriste*, le *Code criminel* interdisait au CSTC d'intercepter toute communication en provenance ou à destination du Canada et dont l'auteur avait une attente à l'égard de la protection de sa vie privée. Toutefois, depuis 2001, le CSTC peut intercepter des communications canadiennes d'un seul pôle, sous réserve de conditions strictes, afin d'obtenir des renseignements étrangers ou de protéger les systèmes ou les réseaux informatiques du gouvernement[6]. Ce nouveau pouvoir a fait en sorte de déplacer de plus en plus le CSTC vers des secteurs autrefois dominés par le SCRS,

[6] Deux nouveaux pouvoirs de collecte de renseignements ont été accordés au CSTC, le premier permettant au CSTC de recueillir les communications de renseignements étrangers ciblés, même si ces communications entrent au Canada ou en sortent. La condition primordiale de la collecte de telles communications privées est que l'interception doit viser des entités étrangères à l'étranger. Le deuxième nouveau pouvoir permet au CSTC d'intercepter des communications privées afin d'aider le gouvernement à protéger ses systèmes et réseaux informatiques. Se reporter à « Autorisations ministérielles du CSTC : Nouveaux pouvoirs », sur le site Web du CSTC.

[7] « La loi antiterroriste et l'évolution au CST », site Web du CSTC.

En 2007, le SCRS et le CSTC ont corédigé une lettre destinée au greffier du Conseil privé dans laquelle ils décrivaient les possibilités uniques pour le gouvernement de localiser physiquement les administrations centrales du CSTC et du SCRS. Peu de temps après, un groupe de travail mixte a été mis sur pied afin d'examiner la signification d'une collaboration accrue pour les deux organisations, qui se doit de demeurer à l'intérieur des paramètres législatifs existants.

3.3 Aperçu de la coopération

Les efforts entrepris en 2007 ont porté leurs fruits et ont transformé la relation d'un engagement sporadique en une collaboration quotidienne. Il existe maintenant une participation de haut niveau (c.-à-d. le directeur du SCRS et le chef du CSTC) et un nouveau protocole d'entente qui décrit les modalités de coopération en matière de collecte, de partage et de soutien opérationnel. La refonte du programme de détachement du SCRS et du CSTC en 2011 a symbolisé cette collaboration. Même si les détachements n'étaient pas nouveaux, du point de vue du SCRS, il était évident que les personnes détachées agissaient principalement à titre d'émissaires, plutôt qu'à titre de véritables employés. Par conséquent, le nouveau programme a transformé les employés détachés en employés à part entière, bénéficiant de tous les accès et de toutes responsabilités dont bénéficient leurs collègues, encore une fois parallèlement aux pratiques de détachement entre les

Le SCRS et le CSTC communiquent quotidiennement à de multiples niveaux de travail, dans toutes les directions opérationnelles. En raison de l'expérience du Service dans la gestion de ces relations afin d'exécuter

En outre, le SCRS et le CSTC participent régulièrement aux forums internationaux aux côtés d'organismes alliés. Qu'il s'agisse de cyberattaques engagées par des gouvernements étrangers ou de l'évolution de l'espionnage à l'aide de moyens technologiques, les partenaires alliés conviennent que les limites strictes autrefois tracées entre HUMINT et SIGINT sont de moins en moins distinctes.

3.4 Opérations à l'étranger

Malgré les défis abordés dans les sections suivantes de cet examen, le Comité a été impressionné par les avantages que représente une collaboration plus étroite avec le CSTC en matière de renseignement. En fait, le CSARS est d'avis qu'il est dans l'intérêt de la sécurité nationale du Canada que ce partenariat en évolution se consolide, tout en respectant les limites pratiques prescrites par les mandats respectifs de chaque organisation.

4 DÉFIS ACTUELS À L'ÉGARD DE LA RELATION ENTRE LE SCRS ET LE CSTC

4.1 Les limites des services partagés

Comme il a été mentionné précédemment, la lettre de 2007 au greffier du Conseil privé a souligné un certain nombre d'avantages liés à l'emplacement commun des administrations centrales du CSTC et du SCRS. Les économies de coûts découlant de la coopération mutuelle entre les organismes (à l'époque) étaient les plus importantes. Quelques années plus tard, cet optimisme a été affiché de nouveau par le conseiller à la sécurité nationale, qui a affirmé que la collaboration au sein de la communauté de la sécurité et du renseignement était plus importante que jamais. Par conséquent, on croyait généralement qu'une fois que le SCRS et le CSTC travailleraient en collaboration, la communication deviendrait plus facile, ce qui se traduirait par des synergies opérationnelles efficaces[14].

Le point central de cette collaboration était une stratégie de « services partagés » – c.-à-d. la gestion des installations et/ou des fonctions de soutien organisationnel qui peuvent être assumées par le SCRS et partagées avec le CSTC, ou *vice versa.* Pour les organismes de renseignement aux prises avec des ressources de plus en plus limitées en période de contraintes budgétaires à l'échelle du gouvernement, les services partagés se prêtent à une gestion efficiente et efficace des ressources. Malheureusement, le **CSARS a conclu que les attentes initiales en matière de services partagés entre le CSTC et le SCRS étaient peut-être trop optimistes.**

Dans une large mesure, les attentes élevées ont été contrecarrées par des problèmes de gestion, des restrictions budgétaires et des complications liées à l'aménagement du site du CSTC. Les défis vont des différences salariales, des complications de la normalisation des règlements et des certifications en matière de santé, de sécurité et d'emploi, en passant par la gestion des différences entre les critères d'emploi des employés syndiqués du CSTC et ceux des employés non syndiqués du SCRS.

À l'heure actuelle, la nouvelle administration centrale du CSTC est toujours en construction; il semble que les économies initiales annoncées en 2007, et

[13] Note d'information du SCRS, « Proposition d'un nouveau modèle de gouvernance pour la collaboration entre le CSTC et le SCRS en matière de services habilitants partagés », dossier 370-625, 1er octobre 2010; et document du SCRS, « Une vision pour l'avenir – Un livre blanc », dossier 370-625, 1er octobre 2010; et réunion de gestion conjointe, « SCRS et CSTC – Compte rendu des discussions », 11 décembre 2009.

acceptées à maintes reprises comme l'une des principales raisons justifiant le partage des locaux, ne seront pas aussi importantes que prévu initialement[16].

4.2 Transfert des connaissances et gestion conjointe des risques

Les difficultés liées à la négociation de services partagés sont relativement légères lorsqu'on les compare aux efforts déployés pour améliorer l'intégration de la collecte du SCRS et du CSTC, ce qui suppose des perspectives organisationnelles et des méthodologies complètement différentes en ce qui a trait à la collecte, à la conservation, à l'analyse et à la diffusion de renseignements. En effet, le **CSARS a constaté que les lacunes dans la compréhension du mandat ou des responsabilités de l'autre organisation étaient un thème récurrent.** Cette question a été soulevée aux niveaux opérationnel et de gestion dans l'ensemble des directions opérationnelles du SCRS, et a été reconnue comme étant un obstacle à la coopération lors des réunions conjointes du SCRS et du CSTC.

La gestion des risques est un domaine auquel les deux organismes accordent beaucoup d'attention.

[15] Réunion du CSARS avec le directeur adjoint, Technologie, 19 juin 2012; et compte rendu des discussions de la réunion sur le modèle de gouvernance proposé des services partagés du SCRS et du CSTC, dossier 370-625, 27 janvier 2011.

4.3 Programme de l'article 16

Des examens antérieurs effectués par CSARS ont soulevé des préoccupations selon lesquelles la collecte par le SCRS de renseignements en vertu de l'article 16 pourrait avoir une incidence négative sur le mandat principal du Service l'autorisant à recueillir des renseignements de sécurité.

4.4 Communication de renseignements

le CSARS a toutefois constaté qu'un risque important découlant de la collaboration accrue entre le SIGINT et HUMINT était l'érosion potentielle du contrôle des renseignements.

Normalement, le Service exerce un contrôle sur l'utilisation des renseignements au moyen de mises en garde et d'assurances. Les mises en garde du SCRS précisent que les renseignements fournis sont la propriété du SCRS et ne peuvent être transmis à un autre organisme ni modifiés sans le consentement exprès du SCRS. Les assurances sont des ententes bilatérales formelles conclues avec des organismes étrangers stipulant que les renseignements du SCRS ne seront pas utilisés d'une manière contraire aux conventions internationales sur les droits de la personne. La mesure dans laquelle les mises en garde et les assurances sont efficaces dépend du degré de confiance entre le SCRS et l'organisme qui obtient les renseignements.

Toutefois, les mises en garde et les assurances du SCRS n'ont jamais été conçues à des fins de collecte de SIGINT.

Les échanges de renseignements entre HUMINT et SIGINT sont des activités à faible risque. Cette affirmation se fonde sur le fait que les organismes alliés sont principalement axés sur leurs propres priorités nationales en matière de renseignement. Toutefois, le CSARS s'inquiète des cas où les

priorités de collecte des alliés se sont unies à celles du Canada, comme dans les affaires de lutte contre le terrorisme.

Il est clair pour le CSARS que les directives ministérielles et les politiques connexes du SCRS sont conçues pour prévenir l'utilisation abusive des renseignements, tant du point de vue de la sécurité que de celui des droits de la personne. Cependant, il n'est pas clairement défini comment le SCRS peut se conformer aux directives ministérielles précisant que des mises en garde doivent être formulées lors de l'échange de renseignements avec des destinataires nationaux et étrangers, lorsque le SIGINT est collecté et diffusé d'une manière contraire à cette attente[39].

Pour sa part, le SCRS a reconnu que la prise en compte des préoccupations à ce sujet complexe demeurait « un travail en cours »[36]. Étant donné que la collaboration entre le SCRS et le CSTC devrait s'intensifier, le CSARS réexaminera cette question dans le cadre d'examens ultérieurs afin d'évaluer les progrès réalisés afin de relever ce défi.

[36] Reportez-vous au courriel du LOSE au CSARS, « FWD : Étude du CSARS — Relation du SCRS avec le CSTC », 15 octobre 2012.

5 RESPONSABILITÉ EN MATIÈRE DE CYBERSÉCURITÉ

Au cours des quatre dernières années, le SCRS a reçu régulièrement des directives du gouvernement

5.1 Principaux défis

5.3 Prochaines étapes

En 2010, Sécurité publique Canada a conçu une stratégie pangouvernementale en matière de cybersécurité qui affirme qu'il ne peut y avoir d'ambiguïté quant au rôle de chacun. La Stratégie confirme les rôles respectifs du CSTC et du SCRS, le premier ayant une expertise reconnue en matière de lutte contre les cybermenaces et les attaques, tandis que le second a pour tâche générale d'analyser et de mener des enquêtes sur les menaces nationales et internationales. Nonobstant la Stratégie, l'**examen du CSARS a permis de constater qu'il reste du travail à faire pour coordonner les activités cybernétiques du SCRS avec celles du CSTC, surtout en ce qui concerne la protection de l'infrastructure de l'information revêtant une grande importance pour le gouvernement du Canada.**

Le Canada a besoin d'un système efficace pour gérer les cybermenaces, qui assurera à la fois une solide capacité de mener une enquête sur le cyberespionnage et maintiendra des systèmes robustes de cyberdéfense et d'atténuation. **Compte tenu de l'intensification inévitable de la collaboration entre le SCRS et le CSTC et de la colocation imminente de ces deux organismes, nous encourageons fortement le SCRS à établir des principes généraux de coopération plus clairs et plus solides avec le CSTC. Ces principes devraient tenir compte du volume croissant de défis qui ont surgi entre les deux organismes, tout en respectant les mandats individuels de chacun.**

6 CONCLUSION

En effet, après avoir examiné les dossiers du SCRS et parlé à un certain nombre d'employés, le CSARS estime qu'il est dans l'intérêt de la sécurité nationale du Canada que ce partenariat en évolution se poursuive afin d'atteindre des niveaux accrus de collaboration. Toutefois, cela doit se faire conformément aux mandats respectifs de chaque organisation.

Bien que le CSARS soit en contact avec le bureau du commissaire du CSTC, nos bureaux n'ont pas le pouvoir d'entreprendre un examen coopératif. Nous croyons que cela devrait préoccuper à la fois le ministre de la Sécurité publique et le ministre de la Défense nationale, qui doivent tous les deux s'appuyer sur deux processus d'examen distincts pour donner un aperçu (incomplet) des activités intégrées de leurs organismes de renseignement respectifs.