COMMISSAIRE DU CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS

RAPPORT ANNUEL 2014-2015

Canada

Bureau du commissaire du
Centre de la sécurité des télécommunications
C.P. 1474, succursale « B »
Ottawa ON K1P 5P6

Téléphone : 613-992-3044
Télécopieur : 613-992-4096
Site Web : www.ocsec-bccst.gc.ca

Nº de catalogue D95F-PDF
ISSN 1700-0882

Commissaire du Centre de la
sécurité des télécommunications

L'honorable Jean-Pierre Plouffe, C.D.

CANADA

Communications Security
Establishment Commissioner

The Honourable Jean-Pierre Plouffe, C.D.

Juin 2015

Ministre de la Défense nationale
Édifice MGén George R. Pearkes, 13e étage
101, promenade Colonel By, tour Nord
Ottawa ON K1A 0K2

Monsieur le Ministre,

Conformément au paragraphe 273.63(3) de la *Loi sur la défense nationale*, j'ai l'honneur de vous transmettre le rapport annuel faisant état de mes activités et constatations pour la période allant du 1er avril 2014 au 31 mars 2015, aux fins de présentation au Parlement.

Je vous prie d'agréer, Monsieur le Ministre, l'assurance de ma haute considération.

Jean-Pierre Plouffe

C.P. / P.O. Box 1474, Succursale « B » / Station "B"
Ottawa ON Canada K1P 5P6
Tél. : 613-992-3044 Télec : 613-992-4096

TABLE DES MATIÈRES

BIOGRAPHIE DE L'HONORABLE JEAN-PIERRE PLOUFFE, C.D.


Couvrette/Ottawa

L'honorable Jean-Pierre Plouffe a été nommé commissaire du Centre de la sécurité des télécommunications le 18 octobre 2013 pour un mandat de trois ans.

Né le 15 janvier 1943 à Ottawa, en Ontario, M. Plouffe a fait ses études à l'Université d'Ottawa où il a obtenu sa licence en droit ainsi qu'une maîtrise en droit public (droit constitutionnel et international). Il a été admis au Barreau du Québec en 1967.

M. Plouffe a débuté sa carrière au cabinet du juge-avocat général du ministère de la Défense nationale. Il a pris sa retraite des Forces armées canadiennes en 1976, alors qu'il était lieutenant-colonel. Par la suite, il a été avocat de la défense en pratique privée au sein du cabinet Séguin, Ouellette, Plouffe et associés, à Gatineau, au Québec, ainsi qu'avocat de la défense à la cour martiale. M. Plouffe a ensuite travaillé en tant qu'avocat de la défense à l'aide juridique.

M. Plouffe a été nommé juge militaire de la force de réserve en 1980, puis juge à la Cour du Québec en 1982. Il a ensuite été nommé juge à la Cour supérieure du Québec en 1990, puis juge à la Cour d'appel de la cour martiale du Canada en mars 2013. Il a pris sa retraite en tant que juge surnuméraire le 2 avril 2014.

MESSAGE DU COMMISSAIRE

L'année qui vient de s'écouler a été marquée par un vigoureux débat entourant les activités du Centre de la sécurité des télécommunications (CST ou Centre) et de mon bureau, chargé de l'examen de ces activités. Alimentées par les documents classifiés dévoilés sans autorisation par Edward Snowden et par les projets législatifs en réaction au meurtre de deux soldats canadiens sur le territoire national, les discussions ont porté en grande partie sur la question du contrôle des organismes voués à la sécurité et au renseignement. Les Canadiens méritent qu'on leur donne l'assurance que les activités de ces organismes – y compris toutes les autorisations supplémentaires qui peuvent leur être accordées – ne portent pas atteinte de façon déraisonnable à leur vie privée. Mon mandat est au cœur du débat, de même que le mandat de mes collègues du Comité de surveillance des activités de renseignement de sécurité et de la Commission civile d'examen et de traitement des plaintes relatives à la GRC.

Dans ce contexte chargé, je dois prendre du recul. Pour m'acquitter de mes fonctions en tant que commissaire du CST, je m'inspire des nombreuses années où j'ai été juge pour examiner les faits impartialement, poser des questions de manière objective et voir les choses à travers le prisme du droit plutôt que de l'émotion. Mais je demeure profondément conscient du fait que le travail du CST suscite de fortes réactions lorsque les Canadiens estiment que leur vie privée pourrait être violée et lorsque le voile du secret sous lequel le CST s'acquitte nécessairement de son travail fausse l'idée qu'ils se font de ses activités – et par là même des activités de mon bureau.

Je continue d'être préoccupé par le débat public qui tire des conclusions ou se forge des opinions à partir d'une information incomplète. En l'absence du contexte intégral, qui ne peut être dévoilé à ceux qui sont à l'extérieur du « périmètre de sécurité », une information incomplète peut semer la confusion et être mal interprétée. La nature de son mandat oblige le CST à exercer en grande partie ses activités dans le secret. Mais mon bureau a pleinement accès au CST en raison de la *Loi sur les*

enquêtes, qui autorise le commissaire et son personnel à examiner de manière approfondie l'organisation de l'intérieur pour savoir et comprendre ce qui s'y passe. Le rôle de mon bureau est de représenter l'intérêt du public dans la reddition des comptes du CST, mais d'une façon qui ne porte pas atteinte au travail important que fait le Centre, en vertu de la loi, pour protéger les intérêts nationaux du Canada et que les Canadiens attendent de lui. C'est là l'intention du législateur.

Les parlementaires auraient cependant été incapables de prédire la façon dont la technologie est en train de remodeler la société. Les technologies d'Internet et des télécommunications ont estompé les frontières internationales et fait bouger les frontières sociales. Ce contexte et le climat de menace actuelle requièrent la collaboration entre les organismes canadiens de sécurité et de renseignement. À vrai dire, nombre d'examens menés par mon bureau cette année reflètent le thème de la coopération, que ce soit entre le CST et le Service canadien du renseignement de sécurité ou d'autres institutions gouvernementales, ou entre le CST et ses homologues en Australie, en Nouvelle-Zélande, au Royaume-Uni et aux États-Unis, ou encore entre les organismes d'examen du renseignement.

Alors que le gouvernement et les Canadiens cherchent la meilleure façon permettant aux organismes de sécurité et de renseignement de travailler ensemble tout en assurant parallèlement des contrôles adéquats et une protection appropriée de la vie privée des Canadiens, certains commentateurs ne voient pas d'un bon œil les pouvoirs accrus proposés par le projet de loi C-51, *Loi antiterroriste, 2015*. Quant aux effets éventuels de cette loi sur le CST et son travail, nous ne pouvons savoir pour l'instant avec précision quelle sera l'incidence des mesures qu'elle prévoit.

Il faut s'assurer que les exigences opérationnelles ne l'emportent pas sur la protection de la vie privée des Canadiens et cela peut être compensé par un renforcement de l'examen. Comme je l'ai écrit en mars 2015 au comité de la Chambre des communes chargé d'examiner le projet de loi C-51, compte tenu de leur mandat législatif actuel, la coopération en place entre les organismes d'examen est limitée. Force est de constater

qu'une autorisation explicite pour les organismes d'examen de coopérer et de communiquer l'information opérationnelle viendrait renforcer la capacité de l'examen et son efficacité. Cette autorisation revêt d'autant plus d'importance que l'on voit s'instaurer progressivement une plus grande collaboration et un plus grand partage d'information entre les organismes de sécurité et de renseignement.

Il y a longtemps que la question de la collaboration entre les organismes d'examen a été soulevée. En effet, dans son rapport d'enquête de 2006 sur Maher Arar, le juge Dennis O'Connor recommandait qu'on établisse des passerelles dans la loi pour atteindre quatre objectifs : « l'échange d'information, le renvoi d'enquêtes à un autre organisme, la tenue d'enquêtes conjointes, ainsi que la coordination lors de la préparation des rapports ». Mon prédécesseur et moi nous sommes déjà attaqués au premier objectif, en communiquant certaines informations au Comité de surveillance des activités de renseignement de sécurité, et j'ai commencé à travailler à l'atteinte du dernier objectif – en vertu des pouvoirs actuel.

Tout au long de l'année écoulée, le CST a interagi avec mon bureau sans détours. Sa transparence avec moi témoigne du sérieux et de la confiance avec lesquels le Centre aborde le mandat dont il est investi par la loi.

La transparence continue d'être un élément clé de ma démarche, en raison de son importance pour maintenir la confiance du public. Mon rôle consiste en partie à faire connaître au Parlement et aux Canadiens les activités du CST et je pense qu'il est capital que j'étaie mes constatations du maximum d'explications possible, en tenant compte des limites imposées par la *Loi sur la protection de l'information*. En tant qu'organisme indépendant et externe, mon bureau peut demander au CST de justifier pourquoi certains renseignements doivent être considérés comme classifiés, et il l'a fait. À vrai dire, j'ai inclus l'an dernier des statistiques se rapportant à des communications privées interceptées de façon non intentionnelle et recueillies dans le cadre des activités de collecte de renseignements électromagnétiques étrangers du CST. Le rapport de cette année renferme davantage de statistiques. Je vois ces initiatives comme des mesures importantes pour contribuer à démystifier le travail du CST et mieux éclairer le débat public.

J'aimerais exprimer ma gratitude à M. John Forster, qui a quitté ses fonctions à la tête du CST en janvier 2015. M. Forster était ouvert et franc avec moi lorsqu'il y avait des questions à discuter qui pouvaient se révéler épineuses. Alors que j'accueille la nouvelle chef du CST, Greta Bossenmaier, j'espère pouvoir poursuivre une relation franche et professionnelle avec elle. Quant à mon compte rendu aux Canadiens concernant les activités du CST, il continuera d'être marqué par le même esprit d'ouverture.

Enfin, dans le cadre de l'un de mes examens cette année, je signale une fois de plus qu'un article de la partie V.1 de la *Loi sur la défense nationale* doit être modifié. Mon intervention s'ajoute à celle de tous mes prédécesseurs demandant qu'on modifie la partie V.1 pour lever les ambigüités. Il convient de rappeler que la partie V.1 de la *Loi sur la défense nationale* a été rédigée et adoptée rapidement en 2001, dans la foulée des événements du 11 septembre. Compte tenu des circonstances et de la menace évidente qui pesait sur la sécurité à l'époque, le Parlement n'avait d'autre choix que d'agir sans délai. Des modifications clarifieraient la loi et, à mon sens, elles ne devraient pas susciter de controverse. Je suis déçu des occasions manquées pour régler cette question importante.

MANDAT DU COMMISSAIRE DU CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS

Le mandat dont j'ai été investi en vertu de la *Loi sur la défense nationale* est le suivant :

1. procéder à des examens concernant les activités du CST pour en contrôler la légalité;

2. faire les enquêtes que j'estime nécessaires à la suite d'une plainte écrite (pour obtenir davantage d'information, consultez le site Web du Bureau); et

3. informer le ministre de la Défense nationale (qui est responsable du Centre devant le Parlement) et le procureur général du Canada de toutes les activités du Centre qui, à mon avis, pourraient ne pas être conformes à la loi.

J'ai en outre pour mandat, en vertu de la *Loi sur la protection de l'information*, de recevoir de l'information émanant de personnes astreintes au secret à perpétuité qui souhaitent communiquer des renseignements opérationnels spéciaux du Centre en faisant valoir la primauté de l'intérêt public. (Pour obtenir davantage d'information, consultez le site Web du Bureau.)

Mandat du CST

Lorsque la *Loi antiterroriste, 2001* est entrée en vigueur le 24 décembre 2001, elle a ajouté la partie V.1 à la *Loi sur la défense nationale* et établi le mandat à trois volets du CST :

- la partie *a*) autorise le CST à acquérir et à utiliser des renseignements électromagnétiques étrangers dans le but de fournir des renseignements étrangers, en conformité avec les priorités du gouvernement du Canada en matière de renseignement;
- la partie *b*) autorise le CST à aider à protéger les renseignements électroniques et les infrastructures d'information importantes pour le gouvernement du Canada; et
- la partie *c*) autorise le CST à fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité, notamment pour qu'ils obtiennent et déchiffrent les communications recueillies en vertu de leurs autorités respectives.

Afin de mettre l'accent sur l'examen de la légalité des activités du CST et sur la protection de la vie privée des Canadiens, la *Loi sur la défense nationale* exige que le commissaire du CST soit un juge surnuméraire ou un juge à la retraite d'une cour supérieure.

Pour que je puisse m'acquitter de mon mandat, la *Loi sur la défense nationale* me confère :

- une autonomie complète sans lien de dépendance avec le gouvernement et un budget distinct accordé par le Parlement;
- un accès sans entraves à tous les dossiers, systèmes et installations du CST; et
- un accès sans entraves au personnel du CST, et notamment le pouvoir d'assigner à comparaître pour obliger des particuliers à répondre à des questions.

Pour être efficaces, les agents chargés de l'examen doivent posséder une expertise spécialisée afin d'être en mesure de comprendre les aspects des activités du CST d'ordre technique, juridique ou se rapportant à la vie privée. Ils doivent posséder une cote de sécurité du niveau requis pour examiner les dossiers et les systèmes du Centre. Enfin, ils sont liés par la *Loi sur la protection de l'information* et ne peuvent divulguer à des personnes non autorisées les renseignements particuliers auxquels ils ont accès.

L'annexe A renferme le texte des articles pertinents de la *Loi sur la défense nationale* et de la *Loi sur la protection de l'information* se rapportant à mon rôle et à mon mandat en tant que commissaire du CST (p. 61).

Notre approche

L'objet de mon mandat en matière d'examen consiste :

- à déterminer si le CST se conforme à la loi et, si je pense qu'il pourrait ne pas avoir agi en conformité avec la loi, à en aviser le ministre de la Défense nationale et le procureur général du Canada;

- à déterminer si les activités que mène le CST en vertu d'une autorisation ministérielle sont bien celles autorisées par le ministre de la Défense nationale et à vérifier que les conditions d'autorisation requises par la *Loi sur la défense nationale* sont remplies;
- à vérifier que le CST, dans ses activités de collecte de renseignements électromagnétiques étrangers et de sécurité des technologies de l'information (TI), ne cible pas des Canadiens; et
- à promouvoir l'élaboration et l'application efficaces de mesures satisfaisantes pour protéger la vie privée des Canadiens dans toutes les activités que le CST entreprend.

Protection de la vie privée des Canadiens

Le CST se voit interdire par la loi, dans le cadre de ses activités de collecte de renseignements électromagnétiques étrangers et de sécurité des TI, de cibler des Canadiens – où qu'ils se trouvent dans le monde – ou toute personne au Canada. Dans le cadre de mon examen des activités du Centre, je dois notamment déterminer si ce dernier prend des mesures satisfaisantes pour respecter les attentes raisonnables des Canadiens en matière de vie privée concernant l'utilisation et la conservation des communications privées qu'il a recueillies. J'examine l'utilisation, la divulgation et la conservation des communications privées par le CST. Je vérifie que l'information concernant l'identité des Canadiens est protégée et n'est partagée qu'avec les partenaires autorisés pour comprendre les renseignements électromagnétiques étrangers ou pour assurer la protection des TI. Je vérifie également que les métadonnées sont utilisées pour comprendre l'infrastructure mondiale d'information, obtenir du renseignement étranger ou pour protéger les cybersystèmes, mais *non* pour obtenir de l'information sur un Canadien.

En utilisant une variété de méthodes, nous effectuons de façon continue l'examen :

- d'activités choisies en fonction d'une analyse du risque, pour assurer la conformité à un niveau détaillé;
- des systèmes électroniques, des outils et des bases de données;

- d'un éventail d'activités pour vérifier la conformité en rapport avec des questions plus vastes, comme la protection de la vie privée ou les métadonnées; et
- du contenu des politiques, des procédures et des contrôles pour déterminer comment ces instructions sont appliquées par les employés du CST et pour déceler des lacunes systémiques existantes ou éventuelles.

(Pour obtenir davantage d'information sur la méthode préventive et axée sur le risque adoptée par le commissaire pour sélectionner les examens et établir les priorités, consultez le site Web du Bureau.)

Chaque examen comporte une évaluation des activités du CST selon une série de critères standards décrits ci-après :

- **Obligations légales** : Je m'attends à ce que le CST mène ses activités en conformité avec la *Loi sur la défense nationale,* la *Charte canadienne des droits et libertés*, la *Loi sur la protection des renseignements personnels*, le *Code criminel* et toute autre législation pertinente.
- **Exigences ministérielles** : Je m'attends à ce que le CST mène ses activités en conformité avec les instructions ministérielles, conformément à toutes les exigences et dans le respect des limites précisées dans une autorisation ou une directive ministérielle.
- **Politiques et procédures** : Je m'attends à ce que le CST dispose de politiques et de procédures pertinentes pour orienter ses activités et donner des instructions suffisantes sur les obligations légales et les exigences ministérielles, notamment en matière de protection de la vie privée des Canadiens. Je m'attends à ce que les employés du CST soient au courant des politiques et procédures et qu'ils s'y conforment. Je m'attends aussi à ce que le Centre dispose d'un cadre et de mécanismes de validation de la conformité efficaces pour assurer le maintien de l'intégrité de ses opérations. Le Centre doit en outre être en mesure de rendre compte de façon adéquate des décisions importantes prises et de l'information liée à la conformité et à la protection de la vie privée des Canadiens.

(Pour obtenir davantage d'information sur la méthode et les critères d'examen du commissaire, consultez le site Web du Bureau.)

Rapports sur les constatations

Les résultats des examens individuels font l'objet de rapports classifiés au ministre de la Défense nationale. Ces rapports documentent les activités du CST, renferment les constatations relatives aux critères d'examen et dévoilent la nature et l'importance de tout écart par rapport aux critères. S'il y a lieu, je formule des recommandations à l'intention du ministre de la Défense nationale qui visent à améliorer les protections de la vie privée ou à corriger les écarts entre les activités du CST et mes attentes, en appliquant des critères standards.

Aucune influence n'est exercée par le CST ou par un ministre sur le contenu de mes rapports d'examen. Je détermine le contenu de mes rapports, qui sont fondés sur des faits et les conclusions tirées de ces faits. Me conformant à la pratique standard de divulgation adoptée par les vérificateurs, je transmets les ébauches de rapports d'examen au Centre pour confirmation de l'exactitude des faits. Il s'agit d'une étape essentielle du processus d'examen puisque mes recommandations s'appuient sur les faits mis au jour au cours de mes examens.

Le rapport annuel du commissaire déposé devant le Parlement est un document public. Le CST examine l'ébauche pour vérifier qu'elle ne renferme pas d'information classifiée qui pourrait contrevenir à la *Loi sur la protection de l'information*. Par souci de transparence et pour faciliter la compréhension par le public, j'insiste pour que toute l'information qui, à mon avis, doit y figurer, soit bien incluse dans mon rapport. Le rapport est remis au ministre de la Défense nationale qui, en vertu de la loi, le dépose au Parlement.

Par souci de transparence également et tout en respectant un cadre de sécurité rigoureux, mon bureau publie sur notre site Web le titre de tous les rapports d'examen présentés au ministre de la Défense nationale (qui ont été expurgés de toute information classifiée) – 90 à ce jour – pour montrer l'ampleur et le niveau de détail des examens du commissaire.

Le modèle logique de **l'annexe B** présente un organigramme du programme d'examen (p. 65).

BUREAU DU COMMISSAIRE

En 2014-2015, j'ai été épaulé dans mon travail par un effectif de 11 personnes, auxquelles s'ajoutent plusieurs experts dans des domaines spécialisés recrutés selon les besoins. Les dépenses de mon bureau se sont élevées à 2 043 560 $, ce qui correspond à la dotation globale approuvée par le Parlement.

L'annexe C présente l'état des dépenses de 2014-2015 pour le Bureau du commissaire du CST (p.67).

MISE À JOUR SUR LES EFFORTS DU CST POUR DONNER SUITE AUX RECOMMANDATIONS PRÉCÉDENTES

Depuis 1997, mes prédécesseurs et moi-même avons présenté 90 rapports d'examens classifiés au ministre de la Défense nationale qui est responsable du CST. Au total, les rapports renfermaient 156 recommandations. Le CST a accepté et mis en œuvre ou travaille à la mise en œuvre de 93 p. 100 (145) de ces recommandations, y compris les huit recommandations de cette année.

Les commissaires surveillent la façon dont le CST donne suite aux recommandations et répond aux constatations négatives de même qu'aux suivis mentionnés dans les examens antérieurs. Au cours de l'année écoulée, le CST a informé mon bureau que le travail avait été accompli en réponse à six recommandations antérieures.

L'an dernier, j'ai fait rapport sur l'examen mené par l'ancien commissaire Décary concernant le partage par le CST de renseignements électromagnétiques étrangers avec ses partenaires étrangers. J'ai expliqué que le régime d'autorisations ministérielles est un instrument canadien qui s'applique au CST; il ne saurait s'appliquer aux alliés ou à leur régime souverain respectif puisque ces parties traitent l'information en fonction de leurs propres pouvoirs nationaux. En conséquence, le CST ne communique pas au ministre de la Défense nationale les détails, par exemple, concernant les communications touchant des Canadiens ou de l'information concernant des Canadiens qui a été transmise au CST par ses alliés. Par conséquent, pour aider le ministre de la Défense nationale à s'acquitter de son obligation redditionnelle à l'égard du CST et pour compléter les mesures déjà en place en vue de protéger la vie privée des Canadiens, le commissaire Décary a recommandé que le CST fasse rapport de ces détails au ministre sur une base annuelle. Le CST a prévenu mon bureau que le rapport annuel 2013-2014 présenté par le chef du CST au ministre de la Défense nationale incluait des statistiques sur les communications que le CST acquiert de ses partenaires étrangers.

Partenaires de la Collectivité des cinq (Five Eyes)

Les partenaires de la Collectivité des cinq sont le CST et les principales agences internationales des pays de la Collectivité des cinq : la National Security Agency des États-Unis, les Government Communications Headquarters du Royaume-Uni, la Signals Directorate de l'Australie et le Government Communications Security Bureau de la Nouvelle-Zélande. Ce groupe est également connu sous le terme d'« alliés ».

Lors de mon examen des activités du Bureau de l'anti-terrorisme du CST de l'an dernier, j'ai constaté qu'un échantillon des activités relatives aux métadonnées comprenant de l'information sur des Canadiens était dans l'ensemble conforme à la politique opérationnelle. J'ai toutefois découvert que des éléments de la politique du CST liés aux activités relatives aux métadonnées ne correspondaient pas aux pratiques standards. J'ai recommandé que le CST modifie sa politique pour ces activités afin de refléter les pratiques actuelles, spécifiquement pour la tenue de dossiers. J'ai continué à me pencher sur cette question dans le cadre de mon examen des activités du CST relatives aux métadonnées liées aux renseignements électromagnétiques étrangers et j'ai découvert que le CST avait mis un terme à certaines de ses activités d'analyse des métadonnées qui avaient fait l'objet de la recommandation. Le CST met à jour en conséquence son cadre de politique.

Le CST a également donné suite à trois des cinq recommandations découlant de mon examen des autorisations ministérielles du Centre relatives à la collecte de renseignements électromagnétiques étrangers en 2012-2013. Il a informé mon bureau qu'il avait amélioré sa politique de façon à répondre à ma recommandation demandant qu'il adopte des lignes directrices détaillées concernant les approbations complémentaires requises pour certaines activités sensibles. Les deux autres recommandations mises en œuvre par le CST se rapportaient aux communications privées. D'abord, j'avais recommandé que les analystes du CST identifient immédiatement les communications privées en indiquant qu'elles sont essentielles aux affaires internationales, à la

défense ou à la sécurité, comme l'exige la *Loi sur la défense nationale*, et, dans le cas contraire, qu'elles soient détruites. Ensuite, j'avais recommandé que les analystes du CST évaluent régulièrement, au minimum tous les trimestres, les communications privées non encore utilisées dans un rapport pour déterminer si elles étaient strictement nécessaires et demeuraient essentielles aux affaires internationales, à la défense ou à la sécurité, ou si elles devaient être détruites. De façon à respecter ces recommandations, le CST a élaboré une politique de même qu'un système de notification automatisé en vertu duquel les analystes reçoivent un avis lorsqu'une communication privée qui a été marquée en vue de sa conservation n'a pas été utilisée dans un délai prescrit. Le service de notification permet aux analystes de déterminer s'il est nécessaire de conserver les communications privées. Dans le cas contraire, elles sont automatiquement détruites.

Enfin, dans mon examen annuel des incidents relatifs à la vie privée et des erreurs de procédure signalés par le CST en 2013 qui ont eu une incidence ou auraient pu avoir une incidence sur la vie privée de Canadiens, j'ai recommandé que le CST demande à ses alliés de confirmer qu'ils avaient donné suite aux demandes du Centre voulant que l'on règle les incidents relatifs à la vie privée se rapportant à des Canadiens, et que le Centre consigne les réponses dans le Dossier relatif aux incidents liés à la vie privée. Le CST a accepté cette recommandation et est en train de mettre à jour ses procédures pour y donner suite.

En outre, mon bureau et moi-même surveillons 15 recommandations en cours que le CST s'engage à respecter – sept recommandations remontant aux années précédentes et huit de cette année.

APERÇU DES CONSTATATIONS ET DES RECOMMANDATIONS DE 2014-2015

Au cours de l'exercice 2014-2015, j'ai présenté neuf rapports classifiés au ministre de la Défense nationale concernant mon examen des activités du CST. Trois rapports – un sur les autorisations ministérielles régissant la collecte de renseignements électromagnétiques étrangers et deux sur des vérifications ponctuelles de communications privées interceptées, utilisées et conservées en vertu de ces autorisations – sont regroupés en un seul puisque les communications privées examinées lors des vérifications ponctuelles sont celles interceptées en vertu des autorisations ministérielles.

Les examens de l'an dernier ont été menés en vertu de deux volets de mon mandat :

- m'assurer que les activités du CST sont conformes à la loi – comme il est stipulé à l'alinéa 273.63(2)*a*) de la *Loi sur la défense nationale*; et
- m'assurer que les activités du CST menées sous le régime d'une autorisation ministérielle sont dûment autorisées – comme l'établit le paragraphe 273.65(8) de la *Loi sur la défense nationale*.

Le premier examen présenté porte sur les activités du CST relatives aux métadonnées liées aux renseignements électromagnétiques étrangers. Il est le premier d'une série d'examens exhaustifs en cours portant sur les activités du CST relatives aux métadonnées.

Un des examens porte sur l'assistance du CST au Service canadien du renseignement de sécurité (SCRS) en vertu de l'article 16 de la *Loi sur le SCRS*. Deux autres examens portent sur des activités particulières : les activités de sécurité des technologies de l'information (TI) menées par le CST pour protéger les systèmes et les réseaux informatiques du gouvernement du Canada; ainsi que les relations du CST avec les détachements de soutien cybernétique du Groupe des opérations d'information des Forces canadiennes.

Comme les années précédentes, mon bureau a effectué son examen annuel des autorisations ministérielles visant la collecte de renseignements électromagnétiques étrangers. Toutefois, du fait que les autorisations ministérielles permettent au CST d'intercepter de façon non intentionnelle une communication étrangère en provenance ou à destination du Canada, ce qui en fait une « communication privée » au sens du *Code criminel*, il s'agit d'une activité qui nécessite une vigilance continue afin d'en assurer la légalité et la protection de la vie privée. Par conséquent, pour s'assurer que les recommandations formulées l'an dernier ont été mises en œuvre, mon bureau a également effectué cette année des vérifications ponctuelles, à titre de suivi, portant sur les communications privées interceptées, utilisées, conservées et détruites par le CST.

Les deux autres examens sont également des examens que j'effectue chaque année parce qu'ils touchent des domaines présentant un risque élevé pour le droit à la vie privée, à savoir les renseignements divulgués par le CST sur l'identité de Canadiens, ainsi que les incidents et les erreurs de procédure signalés par le Centre concernant la vie privée.

Les résultats

Chaque année, je présente une déclaration générale sur mes constatations concernant la légalité des activités du CST. À l'exception d'un examen lié aux métadonnées dont j'analyse encore les conséquences juridiques, toutes les activités du CST examinées au cours de l'année écoulée étaient conformes à la loi.

De même, cette année, j'ai formulé huit recommandations pour promouvoir la conformité à la loi et renforcer la protection de la vie privée, ainsi que pour clarifier la *Loi sur la défense nationale*. Les recommandations se rapportent au renforcement des lignes directrices ministérielles et de la politique, de même qu'aux éclaircissements concernant les relations du CST avec d'autres organisations, y compris ses alliés.

Cinq recommandations se rapportent aux processus. La première recommandation préconise que le CST utilise son système actuel de

registre centralisé pour consigner les décisions et les mesures prises concernant les nouveaux systèmes de collecte ou ceux qui ont été actualisés, de même que les décisions et les mesures prises concernant la minimisation des métadonnées. Deux recommandations se rapportent à la mise à jour de la documentation habilitante pour les processus liés à l'article 16 de la *Loi sur le SCRS*. Une recommandation demandait que l'on mette à jour ou que l'on crée des protocoles d'entente entre le SCRS et le CST en lien avec l'assistance que le CST porte au SCRS en vertu de la partie *c*) de son mandat. La cinquième recommandation liée à des processus concernait l'ajout de mises en garde à certains matériaux partagés avec les partenaires du CST pour s'assurer qu'ils ne soient pas utilisés sans l'autorisation expresse de ce dernier.

Deux recommandations portent sur la mise à jour et la clarification de certains instruments. La première se rapporte à la mise à jour de la directive ministérielle applicable aux activités relatives aux métadonnées, révisée pour la dernière fois en 2011, afin de tenir compte de l'évolution des pratiques dans ce domaine et de préciser la terminologie qui a changé au fil du temps. La seconde préconise la modification de la *Loi sur la défense nationale* pour lever une ambigüité concernant les activités du CST relatives à la sécurité des technologies de l'information (TI) qui sont menées en vertu d'une autorisation ministérielle.

La dernière recommandation se rapporte à la présentation de rapports au ministre sur les communications privées interceptées de façon non intentionnelle par le CST au cours de ses activités de cyberdéfense. Ces rapports devraient mettre en lumière les différences importantes entre les communications privées interceptées en vertu d'une autorisation ministérielle applicable à la sécurité des TI et celles interceptées en vertu d'une autorisation ministérielle régissant la collecte de renseignements électromagnétiques étrangers. En vertu de l'autorisation ministérielle applicable à la sécurité des TI, le CST intercepte de nombreux courriels en provenance ou à destination du Canada et renfermant un code malveillant, si bien que les attentes en matière de vie privée sont à cet égard moins importantes.

POINTS SAILLANTS DES EXAMENS ET DES RAPPORTS PRÉSENTÉS AU MINISTRE EN 2014 2015

1. Examen des activités du CST relatives aux métadonnées liées aux renseignements électromagnétiques étrangers

Contexte

Au cours des deux dernières années, la collecte et l'utilisation de métadonnées ont été au cœur du débat public concernant le CST, ses activités et mon examen de ces activités.

Mon bureau a effectué le premier examen ciblé sur les métadonnées en 2006. Au fil des années, les commissaires ont continué d'examiner et de surveiller l'utilisation des métadonnées par le CST et formulé plusieurs recommandations. Par exemple, par suite d'un examen mené en 2008, le CST a suspendu certaines activités relatives aux métadonnées comportant de l'information à propos de Canadiens et il a apporté d'importants changements à ses politiques et à ses pratiques avant de reprendre ces activités. Depuis ce temps, mon bureau a continué de se pencher sur diverses activités relatives aux métadonnées menées par le CST.

La planification de cet examen exhaustif des métadonnées était en cours avant les révélations sans autorisation d'Edward Snowden en juin 2013. Ces révélations ont suscité un regain d'intérêt de la part du public pour la problématique liée aux métadonnées, confirmant ainsi l'importance de notre décision d'entreprendre un examen plus vaste de la collecte, de l'utilisation et du partage des métadonnées par le CST, en particulier dans un contexte de renseignements électromagnétiques étrangers. Cet examen m'a donné la possibilité de passer en revue à grande échelle les activités du CST relatives aux métadonnées, afin d'évaluer les changements survenus et de déterminer si les activités sont conformes à la loi et si, en les menant, le CST protège la vie privée des Canadiens.

Métadonnées

On entend par métadonnées l'information associée à une communication qui est utilisée pour identifier, décrire, gérer ou acheminer cette communication. Elles englobent, sans pour autant s'y limiter, un numéro de téléphone, une adresse de courriel ou une adresse de protocole Internet (IP) ainsi que de l'information concernant un réseau et la géolocalisation. Les métadonnées ne comprennent pas le contenu d'une communication.

En vertu des alinéas 273.64(1)*a*) et *b*) de la *Loi sur la défense nationale*, le CST est habilité à recueillir, utiliser, partager et conserver des métadonnées. Mais le CST est autorisé à utiliser les métadonnées uniquement pour comprendre l'infrastructure d'information mondiale, fournir des renseignements sur des entités étrangères situées à l'extérieur du Canada, ou protéger les réseaux et les systèmes informatiques importants pour le gouvernement du Canada. Une directive ministérielle fournit des lignes directrices supplémentaires et impose des limites aux activités du CST relatives aux métadonnées liées aux renseignements électromagnétiques étrangers.

Comme dans le cas de ses autres activités, le CST se voit interdire, dans le cadre de ses activités relatives aux métadonnées, de cibler un Canadien ou toute autre personne au Canada. Toutefois, certaines métadonnées recueillies par le CST renferment de l'information sur des Canadiens et le CST doit prendre des mesures pour protéger la vie privée dans le cadre de l'utilisation de ces métadonnées. Le ministre de la Défense nationale a donné des instructions au chef du CST concernant les activités relatives aux métadonnées, y compris en ce qui a trait à la protection de la vie privée des Canadiens, par l'intermédiaire de la directive ministérielle publiée en 2011 et intitulée *Collecte et utilisation des métadonnées par le Centre de la sécurité des télécommunications*.

La directive ministérielle définit la notion de métadonnée, décrit les activités relatives aux métadonnées que peut entreprendre le CST en vertu de l'alinéa 273.64(1)*a*) de la *Loi sur la défense nationale*, et établit les protections en matière de vie privée que doit appliquer le CST lorsqu'il entreprend des activités relatives aux métadonnées. La directive ministérielle limite les activités du CST et ne l'autorise pas à entreprendre des activités qu'il ne pourrait mener sous le régime de la *Loi sur la défense nationale*. Grâce à diverses politiques internes, le chef du CST a en outre élaboré des lignes directrices qu'il a transmises aux employés du Centre concernant les procédures et les pratiques à observer dans le cadre des activités qui utilisent les métadonnées.

Ce premier rapport concernant mon examen exhaustif des métadonnées, que j'ai présenté au ministre de la Défense nationale, mettait l'accent sur l'utilisation des métadonnées par le CST dans un contexte de renseignements électromagnétiques étrangers. Dans le cadre d'un second rapport, j'examinerai les enjeux mis en évidence dans l'*Examen des*

activités du Bureau de l'anti-terrorisme du CSTC au cours de l'exercice 2013-2014 et je regarderai également de près certaines activités qui incluent une analyse des métadonnées et d'autres qui comprennent de l'information concernant des Canadiens. Un troisième rapport, attendu au cours de l'année à venir, mettra l'accent sur l'utilisation des métadonnées par le CST dans le contexte de la sécurité des technologies de l'information (TI).

Constatations et recommandations

Au cours de cet examen, le CST a fourni volontiers de l'information et son aide à la fois de manière proactive et en réponse à des demandes précises formulées par mon bureau. La forte médiatisation des activités relatives aux métadonnées menées par les organismes du renseignement dans la foulée des révélations sans autorisation d'Edward Snowden a exercé des pressions particulières à la fois sur le CST et sur mon bureau tout au long de cet examen. Reconnaissant l'importance de répondre aux demandes de mon bureau en temps opportun, le CST l'a en outre informé de manière proactive des incidents qu'il avait découverts au cours de l'examen, ce qui a conduit à une enquête plus approfondie, dont je fais la description ci-après.

J'ai constaté que la collecte et l'analyse des métadonnées avaient évolué considérablement depuis le dernier examen approfondi des activités relatives aux métadonnées et qu'elles demeurent essentielles pour tous les aspects de la mission du CST concernant les renseignements électromagnétiques étrangers. Le CST utilise les métadonnées, par exemple, pour géolocaliser une communication, cibler les communications d'entités étrangères à l'extérieur du Canada et éviter de cibler un Canadien ou une personne au Canada.

Puisque la collecte et l'analyse des métadonnées par le CST continuent d'évoluer, il sera important pour mon bureau de s'assurer de bien comprendre les changements touchant les processus du CST et leur impact éventuel sur la vie privée des Canadiens et la conformité à la loi.

Le paysage juridique canadien a également évolué depuis que mon bureau a effectué la dernière analyse approfondie de la collecte et de l'utilisation des métadonnées par le CST. Deux arrêts récents de la Cour suprême du Canada sont dignes de mention à cet égard, à savoir les arrêts *Wakeling* et *Spencer*. Dans *Wakeling* c. *États-Unis d'Amérique*, 2014 CSC 72, le principal enjeu était de déterminer la constitutionnalité de la législation fédérale autorisant le

partage de renseignements licitement interceptés à partir d'un dispositif d'écoute entre les organismes d'application de la loi canadiens et étrangers. La Cour a statué que la divulgation est raisonnable en vertu de l'article 8 de la *Charte canadienne des droits et libertés* si elle répond à un critère en trois volets : la divulgation est autorisée par la loi, la loi autorisant la divulgation est raisonnable et la divulgation se fait de manière raisonnable. Dans l'arrêt *R.* c. *Spencer*, 2014 CSC 43, la Cour suprême a statué qu'il fallait tenir compte des attentes raisonnables d'une personne en matière de vie privée dans le contexte de l'utilisation d'Internet. La Cour a considéré que, selon l'ensemble des circonstances, l'anonymat peut être le fondement d'un intérêt en matière de vie privée qui enclenche la protection constitutionnelle contre l'article 8 de la *Charte*.

Mon bureau continuera de surveiller la façon dont le CST donne suite aux avancées technologiques et à leurs conséquences sur la vie privée, de même que la jurisprudence récente qui pourrait avoir une incidence sur sa collecte, son utilisation et sa divulgation de métadonnées.

J'ai constaté que la directive ministérielle sur les métadonnées manque de clarté concernant le partage de certains types de métadonnées avec les partenaires de la Collectivité des cinq et d'autres aspects des activités du CST relatives aux métadonnées. La directive ministérielle de 2011 sur les métadonnées met à jour la directive originale portant le même titre qui a été émise en 2005. Bien qu'elle intègre plusieurs changements linguistiques qui améliorent le document de 2005, la directive de 2011 manque cependant de clarté concernant des aspects cruciaux de la collecte, de l'utilisation et de la divulgation de métadonnées par le CST dans le contexte des renseignements électromagnétiques étrangers. Par exemple, certains termes clés ne sont pas définis et on n'établit pas de distinctions entre d'autres termes qui, bien qu'ayant une définition similaire, renvoient clairement à des concepts distincts.

La directive ministérielle manque de spécificité concernant l'application à certains processus des dispositions relatives à la vie privée. En outre, la directive ne fournit pas une orientation claire concernant une activité particulière relative aux métadonnées qui est menée de manière systématique par le CST dans le contexte de sa mission concernant les renseignements électromagnétiques étrangers. Il n'est pas clair non plus si certains termes, dans la directive, sont encore applicables à l'utilisation des

métadonnées par le CST dans le contexte de la collecte de renseignements électromagnétiques étrangers. C'est pourquoi **j'ai recommandé** que le CST obtienne une directive ministérielle mise à jour donnant des lignes directrices claires en ce qui concerne la collecte, l'utilisation et la divulgation de métadonnées dans le contexte de renseignements électromagnétiques étrangers.

En janvier 2014, alors que j'en étais aux étapes préliminaires de cet examen, la Canadian Broadcasting Corporation (CBC) a fait état d'un scandale se rapportant à la présentation par le CST de diapositives contenant du matériel classifié aux partenaires de la Collectivité des cinq sous le titre *Les analytiques du profilage IP et les effets sur la mission*. La présentation, qui se rattache à l'une des révélations non autorisées en lien avec les documents tirés des systèmes de la National Security Agency par Edward Snowden, a été conçue à l'origine en mai 2012. J'ai déclaré publiquement que j'étais au courant des activités mentionnées dans le reportage (j'ai également abordé la question dans le rapport annuel public de l'an dernier).

Puisque le reportage analysait une activité du CST qui incluait des métadonnées canadiennes, j'ai décidé d'enquêter plus en détail sur ce sujet dans le cadre de l'examen continu de l'utilisation des métadonnées par le CST dans un contexte de renseignements électromagnétiques étrangers. À ma demande, le Centre a renseigné mon bureau sur ce diaporama présenté dans le reportage. Mon bureau a organisé par la suite plusieurs réunions de suivi avec les dirigeants du CST, dont l'analyste qui avait conçu la présentation et élaboré la technique dont il était question. Au cours de ces réunions et de ces démonstrations, le CST a expliqué en profondeur l'activité et ses objectifs, montré les résultats de l'activité décrite dans la présentation et répondu à de nombreuses questions précises posées par mon bureau. J'ai constaté que ces activités étaient autorisées en vertu de l'alinéa 273.64(1)*a*) de la *Loi sur la défense nationale*. À l'issue de notre enquête, j'ai conclu que le CST avait pris des mesures pour protéger la vie privée des Canadiens dans le cadre de cette activité.

De plus, alors que j'effectuais cet examen exhaustif des métadonnées, le CST a découvert de son propre chef que certaines métadonnées n'étaient pas minimisées comme elles le devaient. La minimisation est le processus en vertu duquel l'information sur l'identité canadienne que renferment les métadonnées est rendue non identifiable avant d'être communiquée. La directive ministérielle sur les métadonnées donne des lignes directrices au CST concernant les mesures de protection de la vie privée que le ministre s'attend à voir appliquer

par le Centre pour le traitement de cette information. Or, la minimisation de certains types de métadonnées est l'une de ces mesures de protection de la vie privée. Par conséquent, le fait que le CST n'a pas minimisé de manière adéquate l'information sur l'identité de Canadiens contenue dans certaines métadonnées avant d'être communiquée est contraire à la directive ministérielle et à la politique opérationnelle du CST.

Information sur l'identité de Canadiens

Dans le contexte des renseignements personnels ou commerciaux, on entend par information concernant l'identité de Canadiens toute information qui peut être utilisée pour identifier une personne, organisation ou société canadienne, par exemple tout chiffre, symbole ou autre élément d'information uniquement attribué à un individu.

J'ai constaté que le CST avait pris des mesures correctives et suspendu proactivement le partage de certains types de métadonnées de façon à protéger la vie privée des Canadiens, tout en cherchant une solution aux problèmes qu'il avait rencontrés à cet égard. Le CST a informé le ministre de la Défense nationale et moi-même de ces questions.

Cet examen a révélé que le système de minimisation de certains types de métadonnées du CST était décentralisé et dépourvu d'un contrôle et d'une hiérarchisation des priorités adéquats. Aussi, le CST n'avait pas de procédure adéquate de tenue des dossiers.

Suite à cette constatation, **j'ai recommandé** que le CST utilise son système actuel de registre centralisé pour consigner les décisions et les mesures prises concernant les nouveaux systèmes de collecte ou ceux qui ont été actualisés, de même que les décisions et les mesures prises concernant la minimisation des métadonnées renfermant de l'information sur l'identité de Canadiens.

Somme toute, d'après mon examen, même si je ne crois pas que ces actes aient été délibérés, ils soulèvent tout de même des questions juridiques que je continue d'analyser et d'évaluer.

Enfin, les partenaires de la Collectivité des cinq du CST reconnaissent la souveraineté respective des autres pays et respectent les lois de chacun en

s'engageant à ne pas cibler les communications des autres. Le CST est convaincu que ses partenaires de la Collectivité des cinq se conformeront aux déclarations d'ordre général des ententes qu'ils ont signées entre eux et ne dirigeront pas leurs activités vers des Canadiens ou des personnes au Canada. Au cours de l'exercice écoulé, j'ai mentionné dans mon rapport que j'avais obtenu, grâce à la coopération du chef du CST, une documentation détaillée se rapportant aux politiques et aux procédures respectives des partenaires de la Collectivité des cinq concernant le traitement de l'information sur des Canadiens.

L'an dernier également, j'ai annoncé que nous explorerions les options en vue de collaborer avec les organismes d'examen des pays de la Collectivité des cinq pour passer en revue les activités de partage de l'information entre leurs agences respectives responsables du renseignement et vérifier l'application des politiques respectives. Cette année, en janvier 2015, je me suis rendu à Washington D.C. pour rencontrer l'inspecteur général de la National Security Agency des États-Unis afin de demander personnellement des garanties, en plus de celles que m'avait fournies le CST. Je suis satisfait des garanties obtenues.

Conclusion

Dans le cadre de ce premier rapport sur mon examen exhaustif des activités du CST relatives aux métadonnées, j'ai examiné des activités particulières dans un contexte de renseignements électromagnétiques étrangers. Le Centre n'a pas hésité à donner à mon bureau de la documentation, des réponses écrites aux questions et un appui général et à lui accorder des entretiens tout au long de l'examen, en particulier en réponse aux incidents survenus au cours de cet examen. Je ne pense pas que le personnel du CST avait l'intention d'agir d'une façon qui n'était pas conforme aux instructions ministérielles ou à la politique opérationnelle. Néanmoins, j'évaluerai avec soin les conséquences sur le plan juridique des incidents mentionnés dans ce rapport.

Au cours du prochain exercice, mon bureau continuera de travailler sur deux autres rapports qui portent sur l'utilisation des métadonnées par le CST : dans le cadre du premier rapport, j'examinerai les enjeux identifiés dans un rapport de 2014 intitulé *Examen des activités du Bureau de l'anti-terrorisme du CSTC* et je me pencherai aussi sur d'autres activités relatives aux métadonnées. Le deuxième rapport, attendu au cours de la prochaine

année, portera sur l'utilisation des métadonnées par le CST dans un contexte de protection des TI.

2. Examen des activités relatives à la sécurité des technologies de l'information menées par le CST en vertu d'une autorisation ministérielle

Contexte

La *Loi sur la défense nationale* confère au CST le mandat de mener des activités de sécurité des technologies de l'information (TI), plus précisément pour donner des avis, des conseils et des services pour aider à protéger les renseignements électroniques et les infrastructures d'information importantes pour le gouvernement du Canada. Ces activités, connues comme la partie *b*) du mandat du CST, ne doivent pas cibler des Canadiens, où qu'ils soient, ou toute personne au Canada, et doivent être soumises à des mesures pour protéger la vie privée des Canadiens lors de l'utilisation et de la conservation de l'information interceptée (alinéas 273.64[2]*a*] et *b*] de la *Loi sur la défense nationale*).

Une autorisation émise par le ministre sous le régime du paragraphe 273.65(3) de la *Loi sur la défense nationale* permet au CST, tout en effectuant des activités de sécurité des TI, dans les situations précisées à l'alinéa 184(2)*c*) du *Code criminel*, d'intercepter des communications privées. Une autorisation ministérielle est valide pendant une période d'un an.

Le principal objectif de cet examen était d'évaluer si les activités de sécurité des TI du CST sont conformes à la loi et dans quelle mesure le CST protège la vie privée des Canadiens au cours de ces activités. Nous avons accordé une attention particulière à l'interception et à l'utilisation par le CST de communications privées de même qu'à l'information concernant des Canadiens.

Il s'agit du second examen depuis que le CST a restructuré ses activités de sécurité des TI et qu'il a apporté des changements à certaines pratiques, politiques et procédures, qui ont été mentionnés dans le rapport annuel 2010-2011 de mon prédécesseur. L'examen portait sur deux types d'activités relatives à la sécurité des TI menées par le CST en vertu d'une autorisation ministérielle en 2009-2010, 2010-2011 et 2011-2012.

Dans le cadre du premier type d'activités pour la sécurité des TI, le CST devait analyser le système informatique d'une institution du gouvernement du Canada (c'est-à-dire un client du CST) dans des circonstances contrôlées et, à la demande d'un client, évaluer les vulnérabilités et tester la réaction de l'environnement du client aux cybermenaces. Une autorisation ministérielle était requise pour cette activité puisqu'elle aurait pu entraîner l'interception non intentionnelle de communications privées. Le CST a indiqué qu'il avait cessé d'offrir ces services en novembre 2012 du fait que cette activité était d'une échelle limitée et n'était plus nécessaire en raison des progrès technologiques.

Le deuxième type d'activités pour la sécurité des TI examiné par mon bureau était les opérations de cyberdéfense menées sous le régime d'une autorisation ministérielle puisqu'elles risquent l'interception non intentionnelle de communications privées. Ces activités détectent et atténuent l'activité malveillante ciblant des systèmes et des réseaux informatiques du gouvernement du Canada. Tout comme le premier type d'activités pour la sécurité des TI, le plein consentement d'un client est nécessaire afin de mener les opérations de cyberdéfense.

Cyberincident

Acte malveillant ou événement suspect qui perturbe ou constitue une tentative de perturber le fonctionnement des dispositifs et des réseaux de communication électroniques importants pour le gouvernement du Canada.

Les opérations de cyberdéfense du CST incluent le développement et l'utilisation d'outils de défense du réseau; la détection et l'analyse de trafic malveillant sur le réseau et l'établissement de rapports à cet égard; ainsi que la prestation d'avis aux clients du gouvernement du Canada sur la réduction du risque ou l'étendue du préjudice. Les outils de cyberdéfense déclenchent des alarmes lorsqu'une activité malveillante est détectée. Ces alarmes sont ensuite acheminées pour analyse plus approfondie afin de circonscrire et de confirmer les menaces pesant sur le réseau.

La politique du CST décrit les mesures nécessaires de protection de la vie privée et les systèmes du CST peuvent automatiser une grande partie de ces exigences d'ordre juridique et stratégique. Par exemple, un système peut demander à un analyste de déterminer le nombre de communications

privées parmi les données qu'il a l'intention d'utiliser et de conserver. L'analyste détermine alors ce nombre. D'autres systèmes peuvent calculer le nombre de communications privées. En pareil cas, il incombe à l'analyste de s'assurer que le nombre de communications privées est exact.

Mon bureau a examiné les dossiers papier et électroniques, les fichiers, la correspondance et d'autres documents pertinents pour les activités de sécurité des TI menées par le CST, notamment les politiques, les procédures et les avis juridiques. Des entretiens ont été menés avec les gestionnaires et d'autres membres du personnel participant aux activités.

Le CST a fait la démonstration de ses activités de sécurité des TI, de même qu'il a présenté des séances d'information détaillées sur les outils et les bases de données connexes. Mon bureau a testé le contenu de ces systèmes, avec des représentants du CST agissant sous notre direction, pour assurer la conformité aux exigences juridiques et ministérielles ainsi qu'aux politiques et procédures connexes.

Constatations

D'après l'information examinée et les entretiens menés, les activités de sécurité des TI du CST ont été dûment autorisées et réalisées conformément à la loi, selon l'interprétation du ministère de la Justice et conformément aux autorisations et instructions ministérielles.

À la demande de mon bureau, la liste des incidents relatifs aux opérations de cyberdéfense fournie au départ par le CST renfermait uniquement les incidents que le CST avait identifiés du fait qu'ils renfermaient des communications privées. Or, mon bureau a découvert plusieurs communications privées qui n'avaient pas été incluses dans ce nombre. En outre, nos questions ont mis au jour des incidents qui étaient identifiés incorrectement, c'est-à-dire qu'ils portaient la mention « communication privée » alors que ce n'était pas le cas, ou le contraire. En conséquence, mon bureau a décidé d'examiner tous les incidents de l'exercice 2011-2012, que ces derniers soient identifiés ou non comme une « communication privée ».

Ces erreurs humaines, associées à des erreurs systémiques que le CST devait localiser, ont retardé l'examen. En réponse aux erreurs que mon bureau a découvertes, les responsables de la sécurité des TI ont immédiatement

apporté deux grandes améliorations au système. Il est encourageant de voir que le CST s'est empressé d'apporter les améliorations voulues aux systèmes afin de promouvoir et d'assurer la conformité. Je me pencherai sur ces améliorations au moment d'un examen ultérieur pour vérifier si ces systèmes fonctionnent correctement.

Le CST dispose d'un nombre suffisant de politiques et de procédures pour satisfaire aux exigences de la loi 1) qui lui interdisent de diriger ses activités d'interception pour la sécurité des TI vers un Canadien ou toute personne au Canada et 2) qui l'obligent à protéger la vie privée des Canadiens dans l'utilisation et la conservation des communications privées et de renseignements interceptés lorsque cette interception est nécessaire pour identifier, isoler ou prévenir des activités dommageables pour les systèmes ou les réseaux informatiques du gouvernement du Canada. Notre observation des gestionnaires chargés de la sécurité des TI et d'autres employés ainsi que nos entretiens avec eux ont montré qu'ils connaissent les politiques et les procédures visant à assurer la conformité à la loi et la protection de la vie privée des Canadiens. Les gestionnaires du CST ont surveillé systématiquement les activités de sécurité des TI aux fins de la conformité et de la protection de la vie privée des Canadiens.

Les politiques et procédures se rapportant à la conservation des communications privées n'ont toutefois pas toujours été observées. Le CST pourrait améliorer certaines politiques et procédures concernant la conservation des communications privées ainsi que les exigences minimales et les pratiques de tenue de dossiers.

Enjeux juridiques et recommandations

Au cours de cet examen, deux questions juridiques se sont posées, qui ont été discutées entre mon bureau et le CST et qui font l'objet de mes recommandations.

Le premier enjeu a trait aux ambigüités découlant du libellé du paragraphe 273.65(3) de la *Loi sur la défense nationale*. Cette loi a été modifiée par la *Loi antiterroriste* en 2001 afin, entre autres, de soumettre à une loi le CST de même que ses activités. Concernant les autorisations ministérielles régissant la sécurité des TI, il a été établi que le ministre de la Défense nationale pouvait autoriser le Centre à intercepter des communications privées dans le seul but de protéger les systèmes et les réseaux

informatiques du gouvernement du Canada contre tout méfait ou toute utilisation non autorisée ou toute perturbation de leur fonctionnement, dans les situations précisées à l'alinéa 184(2)*c*) du *Code criminel*.

Le paragraphe 184(1) du Code établit l'infraction qui consiste à intercepter une communication privée et le paragraphe 184(2) définit les situations dans lesquelles l'interception en question n'est pas une infraction. L'alinéa 184(2)*c*) s'applique aux personnes qui assurent un service téléphonique, télégraphique ou tout autre service de communication au public et qui interceptent des communications privées alors qu'elles assurent le service.

Étant donné que le CST agit rarement dans les cas prévus à l'alinéa 184(2)*c*) du *Code criminel*, on peut faire valoir qu'une autorisation ministérielle applicable à la sécurité des TI émise sous le régime du paragraphe 273.65(3) de la *Loi sur la défense nationale* ne viserait pas les principales activités de cyberdéfense du CST. En conséquence, si une communication privée était interceptée pendant une activité du CST qui n'est pas prévue « dans les cas visés à l'alinéa 184(2)*c*) du *Code criminel* », le Centre pourrait tomber sous le coup de l'application de la partie VI du *Code criminel*.

Je suis d'avis que le paragraphe 273.65(3) de la *Loi sur la défense nationale* ne reflète pas avec exactitude les activités du CST puisque le Centre entreprend des activités qui ne font pas partie des « cas visés à l'alinéa 184(2)*c*) du *Code criminel* ». **En conséquence, j'ai recommandé** que le paragraphe 273.65(3) de la *Loi sur la défense nationale* soit modifié aussitôt que possible pour lever toute ambigüité concernant l'autorisation du CST à mener des activités de sécurité des TI présentant un risque d'interception de communications privées.

Le second enjeu a trait à la pratique du CST, dans le cadre de ses opérations de cyberdéfense en vertu d'une autorisation ministérielle, qui consiste à traiter tous les courriels à destination ou en provenance du Canada interceptés de façon non intentionnelle comme des communications privées selon la définition du *Code criminel*.

Cette question avait été soulevée au préalable par l'ancien commissaire Gonthier, dans le cadre de l'*Étude sur les activités relatives à la sécurité des technologies de l'information menées par le CST*. Dans cette étude réalisée en 2009, il concluait que « la protection d'un code malveillant en

tant que communication privée pourrait inutilement limiter la capacité du CST à mener à bien la partie *b*) de son mandat. » Bien qu'il ne s'agisse pas ici à proprement parler d'une question de conformité à la loi, cela soulève la question de savoir si cette pratique reflète avec exactitude le risque pour la vie privée et la façon dont ce risque est décrit au ministre.

La plupart des communications privées que mon bureau a examinés et que le CST a interceptées étaient des courriels non sollicités envoyés par l'auteur d'une cybermenace à un employé du gouvernement du Canada et ne renfermaient rien de plus qu'un code malveillant ou un élément d'ingénierie sociale. Autrement dit, il n'y avait pas d'échange d'information personnelle ou autre information significative entre l'auteur de la cybermenace et l'employé du gouvernement du Canada.

Ingénierie sociale

L'expression « ingénierie sociale » désigne généralement une pratique trompeuse au cours de laquelle les auteurs d'une cybermenace manigancent ou inventent un stratagème pour piéger d'autres personnes afin de les inciter à leur donner accès à un réseau qui autrement serait protégé, par exemple, en donnant à un courriel une forme qui fait croire qu'il provient d'une source de confiance.

D'après les avis juridiques que j'ai reçus et avec lesquels je suis d'accord, une communication qui ne contient rien de plus qu'un code malveillant et/ou un élément d'ingénierie sociale envoyé à un système ou à un réseau informatique du gouvernement du Canada de façon à lui porter atteinte n'est pas une communication privée au sens du *Code criminel*. Le Centre n'aurait donc pas besoin d'une autorisation ministérielle pour intercepter ces communications lorsqu'il mène à bien la partie *b*) de son mandat. Et il n'a peut-être pas besoin non plus de rendre compte au ministre de l'interception de ce genre de communications.

Ces courriels, utilisés ou conservés par le CST, sont inclus dans le nombre de communications privées signalées au ministre, conformément à l'autorisation ministérielle, pour des raisons de reddition de comptes. Il en résulte un grand nombre de communications que le CST traite comme des communications privées, ce qui fausse forcément le risque que les activités de cyberdéfense du CST font peser sur la vie privée.

J'ai recommandé par conséquent que les rapports du CST au ministre concernant les communications privées interceptées de façon non intentionnelle sous le régime d'autorisations ministérielles mettent en lumière les différences importantes entre les courriels à destination ou en provenance du Canada interceptés dans le cadre des opérations de cyberdéfense et les communications privées interceptées dans le cadre des activités de collecte de renseignements électromagnétiques étrangers, y compris les attentes moins élevées à l'égard de la protection de la vie privée attachées aux communications privées interceptées au cours des opérations de cyberdéfense.

Conclusion

Une des recommandations découlant de cet examen fait écho à une préoccupation évoquée en permanence par mes prédécesseurs et qui est aussi la mienne concernant le libellé ambigu de la *Loi sur la défense nationale* en lien avec le mandat du CST. L'examen et la modification de la *Loi sur la défense nationale* renforceraient les mesures pour protéger la vie privée des Canadiens lorsque le CST protège les systèmes et les réseaux informatiques du gouvernement du Canada.

Dans mes examens ultérieurs, j'ai l'intention de suivre de près les améliorations apportées aux systèmes concernant les communications privées interceptées non intentionnellement par le CST au cours de ses activités de sécurité des TI. Je surveillerai également de près les politiques et procédures de tenue des dossiers des communications privées par le CST.

3. Examen des détachements de soutien cybernétique des Forces armées canadiennes

Contexte

Le Groupe des opérations d'information des Forces canadiennes (GOIFC) peut, en accord avec le mandat du CST relatif à la collecte de renseignements électromagnétiques étrangers et au nom du Centre, répondre aux demandes de type militaire adressées au CST par les Forces armées canadiennes (FAC) concernant les renseignements électromagnétiques étrangers. Les détachements de soutien cybernétique du GOIFC agissent en tant qu'intermédiaires pour fournir aux clients des FAC les rapports du CST concernant les renseignements électromagnétiques étrangers.

Les détachements de soutien cybernétique du GOIFC assurent un soutien à certains commandants des FAC concernant les renseignements électromagnétiques étrangers dans toute une gamme d'activités, allant de la planification au soutien direct des opérations de combat. Toutefois, les détachements ne participent pas à la collecte de renseignements électromagnétiques étrangers ou à la production de rapports connexes. Ils s'en tiennent essentiellement à une sensibilisation situationnelle de leurs forces opérationnelles et de renseignement respectives. Pour s'acquitter de ces fonctions, les détachements peuvent avoir accès aux systèmes de collecte de renseignements électromagnétiques étrangers du CST qui stockent les données acquises en vertu du pouvoir conféré par la partie V.1 de la *Loi sur la défense nationale*. Le CST prend des mesures pour s'assurer que l'accès à ces systèmes et l'utilisation des données acquises à partir de ces systèmes sont conformes à la législation, aux instructions ministérielles ainsi qu'aux politiques et procédures du CST.

Un rapport d'évaluation établi par la Direction générale de la vérification, de l'évaluation et de l'éthique du CST concernant les éléments de soutien des renseignements électromagnétiques, comme on appelait autrefois les détachements de soutien cybernétique, renfermait des affirmations qui ont soulevé des questions concernant la capacité des détachements à démontrer au CST et, éventuellement, à mon bureau que les activités concernant les renseignements électromagnétiques étrangers sont conformes à la loi, aux instructions ministérielles ainsi qu'à la politique et aux procédures du CST. Le CST devait prendre des mesures pour donner suite à ces questions, de même qu'aux 15 recommandations du rapport. Lorsque mon bureau a été mis au courant de ce rapport d'évaluation, il a informé le CST qu'il attendrait la mise en œuvre des mesures correctives avant de déterminer si un examen des détachements de soutien cybernétique du GOIFC était justifié. Par la suite, il a été décidé d'examiner les changements apportés par le GOIFC et le CST pour donner suite aux recommandations formulées dans le rapport d'évaluation et pour passer en revue un échantillon des activités concernant les renseignements électromagnétiques étrangers menées par les détachements de soutien cybernétique entre mars 2013 et mars 2014.

Au départ, mon pouvoir d'examiner les détachements de soutien cybernétique sous le contrôle du GOIFC en vertu de la *Loi sur la défense nationale*, a été contesté. Après un délai de six mois et plusieurs discussions entre mon bureau, le CST et les FAC, j'ai exercé le pouvoir que me confère la Loi et obtenu un accès direct au personnel des détachements de soutien cybernétique et aux locaux, pour m'assurer que les activités concernant les renseignements électromagnétiques étrangers conduites en vertu de la partie V.1 de la *Loi sur la défense nationale* sont conformes à la loi, aux instructions ministérielles ainsi qu'aux politiques et aux procédures du CST. Les FAC ont pleinement coopéré avec mon bureau.

Au total, trois visites ont été effectuées au cours de cet examen. C'était la première fois que mon bureau se rendait dans un site des FAC situé à l'extérieur de la région de la capitale nationale où ces dernières effectuent certaines activités concernant les renseignements électromagnétiques étrangers. Les sites ont été choisis en fonction du niveau de commandement, de la diversité du travail qui y est accompli et de la durée d'existence du site.

Les objectifs de l'examen étaient les suivants:

- acquérir une connaissance détaillée des activités concernant les renseignements électromagnétiques étrangers des détachements de soutien cybernétique et documenter ces activités;
- déterminer si le CST s'est assuré que les activités concernant les renseignements électromagnétiques étrangers des détachements de soutien cybernétique étaient conformes à la loi;
- évaluer la mesure dans laquelle le CST a assuré la protection de la vie privée des Canadiens dans le cadre des activités menées par les détachements de soutien cybernétique.

Constatations

Au cours de cet examen, il est devenu évident que la chaîne de commandement organisationnelle du GOIFC avait pris grand soin de s'assurer que les détachements de soutien cybernétique du GOIFC se conformaient à la loi et à la politique. Bien qu'à titre individuel, les détachements soient dirigés au quotidien par la chaîne de commandement militaire locale, la Section de la surveillance et de la conformité du GOIFC

supervise les activités de tous les sites des détachements, y compris les inspections annuelles, et cette section constitue la principale source de conseils stratégiques sur les renseignements électromagnétiques étrangers à la fois pour les détachements de soutien cybernétique et pour le GOIFC dans son ensemble.

À la différence du CST, les détachements de soutien cybernétique ne recueillent pas de données brutes, n'interceptent pas de communications privées, ne produisent pas de rapports originaux et, par conséquent, n'ont pas à traiter d'information sur l'identité de Canadiens dans le cadre de leurs activités. Les détachements reçoivent les rapports du CST concernant les renseignements électromagnétiques étrangers qu'ils diffusent au sein des FAC. Ces rapports peuvent renfermer de l'information sur l'identité de Canadiens qui aura été supprimée, c'est à dire remplacée par une mention générale telle que « un Canadien ». En cas de demande de divulgation de renseignements supprimés, les détachements se conformeraient à la procédure établie et transmetteraient la demande au Centre qui y donnerait suite. À ce jour, aucune demande de divulgation de renseignements supprimés visant l'identité de Canadiens n'a toutefois été formulée.

En outre, le CST épluche systématiquement et minutieusement les rapports mensuels sur la conformité produits par les différents détachements de soutien cybernétique qui, ensuite, sont intégrés aux rapports sur la conformité préparés par la Section de la surveillance et de la conformité du programme des renseignements électromagnétiques du CST. Ainsi, le CST s'assure activement que les activités concernant les renseignements électromagnétiques étrangers des détachements de soutien cybernétique sont conformes à la loi. Mon personnel a examiné un échantillon de rapports mensuels sur la conformité de tous les détachements et les a jugés satisfaisants.

Des politiques et procédures convenables sont en place pour orienter les activités du personnel des détachements de soutien cybernétique. Chacun des détachements de soutien cybernétique a été mis en place à des moments différents et la documentation qui les régit n'est pas cohérente. Toutefois, cette lacune ne semble pas nuire à leur fonctionnement, à leur supervision ou à leur conformité.

Les employés des détachements de soutien cybernétique interrogés et observés connaissaient les politiques et les procédures pertinentes, y compris celles se rapportant à la protection de la vie privée des Canadiens, ainsi que leur application aux activités courantes des détachements de soutien cybernétique. Les FAC ont recours à un système de formation exhaustif pour les différents postes militaires dont les titulaires sont amenés à manipuler du matériel contenant des renseignements électromagnétiques étrangers. Tout le personnel qui a accès aux systèmes de renseignements électromagnétiques étrangers participe à un programme pour confirmer qu'il comprend parfaitement les politiques spécifiques du CST.

En outre, nul n'est habilité à avoir accès à des renseignements électromagnétiques étrangers sans auparavant avoir répondu de manière satisfaisante à un questionnaire annuel du CST sur la façon de protéger la vie privée et d'assurer la conformité à la loi dans la conduite des activités du CST. La même norme s'applique à tous les employés du CST.

Enfin, j'ai examiné les activités des détachements de soutien cybernétique du GOIFC par suite du rapport d'évaluation de la Direction générale de la vérification, de l'évaluation et de l'éthique du CST. J'ai pu constater que l'on avait répondu aux questions concernant la conformité soulevées par le rapport d'évaluation. Sur les 15 recommandations du rapport, j'ai la certitude que le GOIFC ou le CST a donné suite aux quatre recommandations se rapportant à cet examen.

Conclusion

D'après l'information reçue, les documents examinés, les activités observées et les entretiens, je conclus que les activités des détachements de soutien cybernétique menées en vertu de la partie V.1 de la *Loi sur la défense nationale* étaient en conformité avec la loi, les instructions ministérielles ainsi que les politiques et procédures du CST. En outre, les activités qui sont menées à l'heure actuelle par les détachements de soutien cybernétique ne touchent pas la vie privée des Canadiens.

4. Aide apportée par le CST au Service canadien du renseignement de sécurité en vertu de la partie *c*) du mandat du CST et de l'article 16 de la *Loi sur le Service canadien du renseignement de sécurité*

Contexte

Le CST peut offrir au Service canadien du renseignement de sécurité (SCRS) une assistance technique et opérationnelle en vertu de la partie *c*) de son mandat et de l'article 16 de la *Loi sur le SCRS*. L'article 16 habilite le SCRS à prêter assistance au ministre de la Défense nationale et au ministre des Affaires étrangères dans la collecte de renseignements électromagnétiques étrangers, sur le territoire canadien, à l'appui des affaires internationales et des intérêts de défense du gouvernement du Canada. Les activités visées par l'article 16 requièrent une demande personnelle d'assistance émanant de l'un des ministres susmentionnés, le plus souvent le ministre des Affaires étrangères.

Certaines activités visées par l'article 16, par exemple l'interception de communications, exigent un mandat d'un juge de la Cour fédérale conformément à l'article 21 de la *Loi sur le SCRS*. En pareil cas, le SCRS doit obtenir un mandat de la Cour l'autorisant à exercer des pouvoirs particuliers de collecte ciblée. Le ministre de la Sécurité publique doit accorder personnellement son consentement par écrit avant que le SCRS présente une demande de mandat à la Cour.

En 2007 et au début de 2008, des discussions interministérielles ont été menées sur des changements à la procédure à observer en vertu de l'article 16 au sein du milieu de la sécurité et du renseignement. L'un des changements a été la suppression du protocole d'entente conclu par les trois ministres en 1987, à savoir le ministre des Affaires étrangères, le ministre de la Défense nationale et le solliciteur général (aujourd'hui le ministre de la Sécurité publique). Même si les discussions ont abouti à une nouvelle façon de procéder, les rôles et responsabilités des parties concernées n'ont pas été définis.

Le CST peut fournir une assistance technique et opérationnelle à l'appui d'activités visées par l'article 16, en vertu de la partie *c*) de son mandat (alinéa 273.64[1]*c*]) de la *Loi sur la défense nationale*). En pareil cas, le Centre agit en tant que mandataire du SCRS dans l'interception, le traitement et l'analyse des renseignements recueillis en vertu d'un mandat. Lorsqu'il exécute des activités en vertu de la partie *c*) de son mandat sous le régime d'un mandat délivré en vertu de l'article 16, le CST doit respecter les limites légales imposées au SCRS, tel que le précise le paragraphe 273.64(3) de la *Loi sur la défense nationale*. Ces limites figurent notamment dans la *Loi sur le SCRS* et dans les mandats délivrés en vertu de l'article 16. Les activités visées par l'article 16 ne donnent pas toujours lieu à la délivrance d'un mandat ou à l'aide du CST.

Dans le cadre de la nouvelle procédure, le CST est également guidé par les modalités non seulement de la nouvelle procédure en vertu de l'article 16 approuvée par les ministres des Affaires étrangères, de la Défense nationale et de la Sécurité publique, mais également par plusieurs protocoles d'entente conclus entre le CST et le SCRS qui portent sur la coopération opérationnelle en général et sur les activités visées par l'article 16 en particulier.

Bien que la procédure d'approbation ait été modifiée, le CST fait encore office de mandataire du SCRS dans le traitement des communications interceptées obtenues sous l'autorité d'un mandat délivré par la Cour fédérale. Le CST agit également en tant que mandataire du ministre demandeur dans la diffusion des rapports sur le renseignement étranger par suite des pouvoirs exercés en vertu d'un mandat.

Les objectifs de mon examen étaient les suivants :

- acquérir une connaissance détaillée de l'assistance apportée par le CST au SCRS en vertu de l'article 16 de la *Loi sur le SCRS* et de tout changement depuis le dernier rapport approfondi préparé par mon bureau et les documenter;
- évaluer si les activités menées par le CST sont conformes à la loi, y compris aux conditions des mandats délivrés à l'intention du SCRS par la Cour fédérale.

Constatations et recommandations

Tous les mandats délivrés au SCRS par la Cour fédérale sous le régime de l'article 16 et pour lesquels il a demandé l'appui du CST ont été examinés et plusieurs d'entre eux ont été analysés de manière approfondie. Pour chaque mandat sélectionné aux fins de cet examen, j'ai été en mesure de vérifier que :

- le CST avait une copie du mandat et disposait d'une information claire et suffisante concernant l'aide demandée par le SCRS;
- les communications acquises par le CST pour le SCRS étaient exclusivement celles mentionnées dans les mandats;
- les communications n'étaient pas acquises avant l'entrée en vigueur des mandats et ne l'étaient plus à l'expiration des mandats;
- le CST acquérait uniquement les types de communications et d'information dont l'interception ou l'obtention était autorisée par les mandats; et
- le CST a respecté les limites imposées au SCRS par la loi, par exemple les conditions stipulées dans les mandats.

Le CST a reçu copie des mandats du SCRS lorsqu'ils étaient délivrés par la Cour fédérale.

Lors de cet examen, je me suis intéressé à la technologie, aux bases de données et aux systèmes connexes utilisés par le CST pour les activités menées sous le régime de l'article 16, aux rapports sur le renseignement étranger en résultant, à l'ampleur de l'utilisation de la technologie et aux efforts visant à protéger la vie privée des Canadiens, ainsi qu'aux activités du CST en réponse aux constatations et aux recommandations connexes formulées précédemment par les anciens commissaires.

J'ai constaté que, au cours de la période à l'étude, le CST disposait de politiques et de procédures opérationnelles s'appliquant de façon générale à son assistance dans le cadre de ces mandats et des activités connexes. Ces politiques et procédures fournissaient des instructions aux employés du Centre concernant la conformité à la loi et la protection de la vie privée des Canadiens en ce qui a trait à l'assistance apportée par le CST au SCRS. Le CST a indiqué que ses processus internes, y compris son assistance apportée au SCRS pour la procédure de renouvellement de

mandat, n'avaient pas changé considérablement, malgré la modification apportée à la procédure interministérielle. J'ai aussi constaté que le CST respectait la condition indiquée dans les mandats sous le régime de l'article 16 et stipulant l'obligation de protéger la vie privée des Canadiens en cas de mesures intrusives, en observant la politique du CST qui demande de détruire toute information sur des Canadiens à moins que cette information :

- ne se rapporte à des activités susceptibles de constituer une menace pour la sécurité du Canada, au sens de la *Loi sur le SCRS*;
- ne puisse être utilisée à des fins de prévention, d'enquête ou de poursuite en cas d'acte criminel présumé; ou
- ne se rapporte à des personnes, à des sociétés ou à des États étrangers pour lesquels le ministre demandeur avait sollicité par écrit l'assistance du CST, en vertu de l'article 16 de la *Loi sur le SCRS*.

J'ai constaté que les employés du CST qui ont été interrogés étaient bien au courant des politiques et procédures et montraient qu'ils connaissaient leurs responsabilités respectives. Les entretiens avec les gestionnaires du CST, les chefs d'équipe et les employés nous ont aussi montré que les gestionnaires surveillent de manière systématique l'assistance apportée par le CST au SCRS pour voir si elle est conforme aux autorisations en vigueur.

J'ai constaté que l'assistance apportée par le CST au SCRS et toutes les activités connexes étaient conformes aux exigences énoncées dans le cadre redditionnel et les directives ministérielles sur la protection de la vie privée des Canadiens visant le CST. J'ai également constaté que le CST s'est conformé à la loi et a pris des mesures pour protéger la vie privée des Canadiens.

J'ai formulé quatre recommandations, deux se rapportant à la mise à jour ou à la création d'une documentation concernant la procédure habilitante; une concernant la mise à jour ou la création de protocoles d'entente interministériels entre le SCRS et le CST, au besoin; et une demandant que le Centre rédige des mises en garde à annexer à du matériel opérationnel particulier qui peut être partagé avec des alliés pour s'assurer que le matériel ne soit pas utilisé sans son autorisation expresse.

Conclusion

J'ai conclu que le CST avait mené ses activités en conformité avec la loi et les instructions ministérielles et qu'il intégrait des mesures pour protéger la vie privée des Canadiens. Néanmoins, j'ai recommandé que les ententes interministérielles et les politiques internes du Centre soient mises à jour en temps opportun pour tenir compte des procédures et des pratiques actuelles. Du fait que le SCRS travaille à la mise à jour de certains protocoles d'entente, j'ai informé la présidente par intérim du Comité de surveillance des activités de renseignement de sécurité de mes recommandations.

5. Examen combiné annuel des autorisations ministérielles relatives à la collecte de renseignements électromagnétiques étrangers et de communications privées, 2013-2014

Contexte

La *Loi sur la défense nationale* interdit au CST de viser des Canadiens dans le cadre de ses activités. En vertu de la Loi, le ministre de la Défense nationale peut, dans le seul but d'obtenir des renseignements étrangers, autoriser par écrit le Centre à intercepter des communications privées, c'est-à-dire des communications en provenance ou à destination du Canada. La loi précise les conditions en vertu desquelles une autorisation ministérielle peut être émise (voir l'encadré à la page 42). Les autorisations ministérielles visent une « activité ou une catégorie d'activités » permettant d'acquérir des renseignements électromagnétiques étrangers – le comment. Elles ne renvoient pas à un individu ou à un sujet spécifique – le qui ou le quoi. (Pour obtenir davantage d'information sur les autorisations ministérielles de même que sur les pouvoirs et les limites applicables aux activités du CST, consultez le site Web du Bureau et le site Web du CST.)

Conditions régissant les autorisations ministérielles applicables à la collecte de renseignements électromagnétiques étrangers

En vertu de la *Loi sur la défense nationale*, les quatre conditions régissant une autorisation ministérielle sont les suivantes :

- l'interception doit viser des entités étrangères situées à l'extérieur du Canada;
- les renseignements ne peuvent raisonnablement être obtenus d'une autre manière;
- la valeur des renseignements étrangers que l'on espère obtenir justifie l'interception envisagée; et
- il existe des mesures satisfaisantes pour protéger la vie privée des Canadiens.

La loi oblige également le commissaire du Centre de la sécurité des télécommunications à examiner les activités exercées en vertu d'une autorisation ministérielle et à faire rapport annuellement au ministre de la Défense nationale sur son examen. Un examen combiné annuel des autorisations ministérielles relatives à la collecte de renseignements électromagnétiques étrangers constitue donc pour moi une façon de m'acquitter de ce volet de mon mandat. Cette année, j'ai examiné les trois autorisations ministérielles relatives à la collecte de renseignements électromagnétiques étrangers en vigueur du 1er décembre 2013 au 30 novembre 2014 se rapportant à trois activités ou catégories d'activités. J'ai également effectué des vérifications ponctuelles des communications privées utilisées et conservées.

L'objet de l'examen combiné des autorisations ministérielles était :

- de vérifier que les activités menées en vertu d'une autorisation ministérielle étaient autorisées;
- de mettre en évidence tout changement important – au cours de l'année visée par l'examen, comparativement aux années précédentes – dans les documents d'autorisation eux-mêmes et dans les activités ou catégories d'activités du CST décrites dans l'autorisation; et
- d'évaluer l'incidence, le cas échéant, de ces changements sur le risque de non conformité et d'atteinte à la vie privée et, en conséquence, de relever tout sujet nécessitant un examen de suivi.

Au cours des années précédentes, dans le cadre de l'examen combiné annuel des autorisations ministérielles régissant la collecte de renseignements électromagnétiques étrangers, les commissaires ont examiné des échantillons de communications privées interceptées de façon non intentionnelle, utilisées et conservées par le CST au cours de la période de validité de l'autorisation ministérielle. L'an dernier, mon bureau a examiné les 66 communications privées utilisées dans des rapports ou conservées jusqu'à la fin de la période de validité de l'autorisation ministérielle. Mon rapport de l'an dernier sur le même sujet incluait quatre recommandations liées à la protection de la vie privée :

- que les analystes du CST identifient immédiatement les communications privées en indiquant qu'elles sont essentielles aux affaires internationales, à la défense ou à la sécurité, comme l'exige la *Loi sur la défense nationale* et, si ce n'est pas le cas, qu'elles soient détruites;
- que les analystes du CST évaluent régulièrement, au minimum tous les trimestres, si la conservation des communications privées identifiées non encore utilisées dans un rapport est strictement nécessaire et que ces dernières demeurent essentielles aux affaires internationales, à la défense ou à la sécurité, ou si certaines doivent être détruites;
- que le CST rende accessible au ministre de la Défense nationale une information plus détaillée concernant le nombre de communications recueillies et le nombre de communications privées interceptées qu'il acquiert et conserve pendant toute la période de validité de l'autorisation ministérielle; et
- que le CST publie une politique décrivant les circonstances précises et le traitement d'un type particulier de communications.

Afin de vérifier que les recommandations ont été mises en œuvre, j'ai décidé d'effectuer tout au long de l'année des vérifications ponctuelles des communications privées interceptées, utilisées et conservées au cours de certaines périodes déterminées par mon bureau. Le CST ignorait quand ces vérifications ponctuelles seraient menées ou la période sur laquelle porterait l'examen.

Il y avait 16 communications privées qui avaient été utilisées dans les rapports ou conservées à la fin de la période de validité de l'autorisation ministérielle, c'est-à-dire le 30 novembre 2014. Le CST continue d'utiliser la même méthode que les années précédentes pour dénombrer et signaler les communications privées identifiées. Mes employés vérifient le contenu des systèmes et des bases

de données du CST, écoutent les enregistrements de conversations interceptées, lisent le contenu écrit et examinent la transcription connexe des communications, et ils interrogent les employés du Centre.

J'ai examiné les communications privées interceptées, utilisées et conservées entre le 1er avril 2014 et le 20 juin 2014 et entre le 1er septembre 2014 et le 15 octobre 2014. Au cours de ces vérifications ponctuelles, je voulais que mon personnel se fasse une idée plus exacte du nombre de communications privées relatives aux renseignements électromagnétiques étrangers interceptées tout au long de l'année :

- en vérifiant si les analystes du CST avaient immédiatement identifié les communications privées en question en indiquant qu'elles étaient essentielles – comme le demandait l'une de mes recommandations de l'an dernier;
- en évaluant si elles répondaient aux critères du caractère essentiel – aspect permanent des examens des communications privées interceptées; et
- en vérifiant que les analystes évaluent régulièrement si la conservation continue d'une communication privée identifiée demeure strictement nécessaire – aspect qui figure également dans l'une de mes recommandations de l'an dernier.

Constatations

J'ai constaté que les activités menées en vertu des autorisations ministérielles régissant la collecte de renseignements électromagnétiques étrangers en 2013-2014 étaient autorisées, comme l'exige la *Loi sur la défense nationale*.

J'ai examiné l'information clé se rapportant à l'interception et à la protection de la vie privée des Canadiens pour chacune des trois activités ou catégories d'activités, afin d'effectuer des comparaisons. Il m'est apparu que les autorisations ministérielles de collecte de renseignements électromagnétiques étrangers de 2013-2014 ne renfermaient aucun changement important par rapport à l'année précédente et que le CST n'avait pas apporté de changements importants aux technologies mises en œuvre lors de ces activités.

Pour les vérifications ponctuelles, mon bureau a demandé au CST de lui fournir une liste de toutes les communications privées tirées de

renseignements électromagnétiques étrangers interceptées et identifiées entre le 1er avril 2014 et le 20 juin 2014 et entre le 1er septembre 2014 et le 15 octobre 2014. Mon bureau a vérifié cette liste en examinant la base de données et en confirmant le nombre de communications privées interceptées et identifiées.

Pour les périodes susmentionnées, le CST n'a conservé que deux communications privées qui ont été utilisées dans le cadre d'un seul rapport. Toutes les autres communications privées identifiées, qui avaient été interceptées de façon non intentionnelle par le CST, ont été détruites. Je suis convaincu que les deux communications privées utilisées étaient essentielles aux affaires internationales, à la défense ou à la sécurité comme l'exige la *Loi sur la défense nationale* et que le rapport connexe renfermait des renseignements étrangers. Je n'ai rien trouvé qui puisse donner à penser que des communications privées identifiées et conservées ou détruites par le Centre avaient été interceptées de manière intentionnelle, ce qui serait illégal.

Mon bureau a également interrogé le personnel de collecte de renseignements électromagnétiques étrangers qui avait connaissance des communications privées ainsi que des systèmes et des bases de données du CST. Je n'ai constaté aucun cas où un analyste avait conservé une communication privée plus longtemps qu'il n'était strictement nécessaire, c'est-à-dire plus longtemps qu'il ne fallait pour déterminer si elle était essentielle aux affaires internationales, à la défense ou à la sécurité, ce qui était l'objet de mon examen précédent des autorisations ministérielles régissant la collecte de renseignements électromagnétiques étrangers et les communications privées.

Conclusion

Je conclus que selon les paramètres et les résultats de mes examens des autorisations régissant la collecte de renseignements électromagnétiques étrangers ainsi que des vérifications ponctuelles des communications privées, le CST a pris des mesures pour mettre en œuvre rapidement les recommandations découlant de mon examen précédent. Je n'ai formulé aucune recommandation et continuerai d'effectuer des vérifications ponctuelles des communications privées interceptées sous le régime des autorisations ministérielles régissant la collecte de renseignements électromagnétiques étrangers.

6. Examen annuel de la divulgation des renseignements sur l'identité de Canadiens, 2013-2014

Contexte

L'examen annuel des renseignements divulgués par le CST sur l'identité de Canadiens à partir des rapports inclut les renseignements divulgués à des clients du gouvernement du Canada et à des alliés du CST. Cet examen a aussi inclus des renseignements divulgués à des destinataires n'appartenant pas à la Collectivité des cinq par l'intermédiaire d'un client du gouvernement du Canada ou d'un allié. La période d'examen allait du 1er juillet 2013 au 30 juin 2014.

La *Loi sur la défense nationale* et la *Loi sur la protection des renseignements personnels* exigent que le CST prenne des mesures pour protéger la vie privée des Canadiens, notamment leurs renseignements personnels. Des rapports du Centre portant sur les renseignements électromagnétiques étrangers peuvent renfermer de l'information permettant d'identifier des Canadiens si cette information est essentielle à l'interprétation de ces renseignements. Toutefois, à quelques exceptions près qui sont énoncées dans la politique du CST, toute information identifiant un Canadien dans un rapport doit être supprimée et remplacée par une mention générale de type « un Canadien ».

Lorsqu'il reçoit une demande subséquente de communication des détails de l'information supprimée, le CST doit vérifier que le client du gouvernement du Canada ou l'allié qui fait la demande a le pouvoir et la justification opérationnelle nécessaires pour obtenir l'information sur l'identité du Canadien. Ce n'est qu'après cette vérification que le CST peut fournir l'information. Une demande de diffusion d'information sur l'identité d'un Canadien tirée d'un rapport du CST peut entraîner la diffusion de plus d'une identité.

Lorsqu'il reçoit une demande subséquente de communication des détails de l'information supprimée, le CST doit vérifier que le client du gouvernement du Canada ou le partenaire étranger qui fait la demande a le pouvoir et la justification opérationnelle nécessaires pour obtenir l'information sur l'identité du Canadien. Ce n'est qu'après cette vérification que le CST peut fournir l'information. Une demande de diffusion d'information sur l'identité d'un Canadien tirée d'un rapport

du CST peut entraîner la diffusion de plus d'une identité.

Constatations

Mon bureau a effectué des examens annuels réguliers des renseignements divulgués par le CST concernant l'identité de Canadiens à des clients du gouvernement du Canada et il estime que le CST est rigoureux et minutieux dans la façon dont il traite ces demandes. Par conséquent, mon bureau n'a examiné ce genre de renseignements communiqués à des clients du gouvernement du Canada que sur une période de six mois. Mais nous avons continué, dans le cadre de cet examen, à analyser toutes les demandes de divulgation reçues des alliés sur une période d'un an, de même que celles émanant d'organismes du gouvernement du Canada ou d'alliés et portant sur la divulgation de renseignements sur l'identité de Canadiens à des destinataires n'appartenant pas à la Collectivité des cinq.

J'ai constaté que la divulgation par le CST à des clients du gouvernement du Canada et à des alliés de renseignements sur l'identité de Canadiens tirés de rapports était conforme à la loi et aux instructions ministérielles et que le CST avait pris les mesures appropriées pour protéger la vie privée des Canadiens.

Au cours de la période de six mois, le CST a reçu de clients du gouvernement du Canada 710 demandes d'information sur l'identité de Canadiens supprimée dans des rapports concernant les renseignements électromagnétiques étrangers ou la sécurité des technologies de l'information. Ce nombre ne représente pas la quantité d'information concernant une personne identifiable qui a été divulguée, mais plutôt le nombre de fois que les clients du gouvernement du Canada ont présenté des demandes distinctes de divulgation d'information concernant l'identité de Canadiens supprimée des rapports, fournissant une justification opérationnelle unique à chaque fois. De ces 710 demandes, mon bureau a passé en revue un échantillon de plus de 20 p. 100, ainsi que tous les rapports qui renfermaient de l'information supprimée sur l'identité ayant fait l'objet de la demande. Le CST s'est assuré que tous les organismes ou ministères ayant présenté une demande étaient habilités à le faire et avaient présenté la justification opérationnelle requise avant la diffusion de l'information. Les demandes non étayées par un pouvoir ou une justification opérationnelle adéquates ont été refusées.

Le CST a aussi reçu des demandes de divulgation de renseignements sur

l'identité de Canadiens émanant de ses alliés. Mon bureau a examiné toutes les demandes et les rapports connexes. Les demandes ont abouti à un nombre à peu près égal de refus et d'autorisations de divulgation de renseignements sur l'identité de Canadiens.

Six demandes de divulgation d'information sur l'identité de Canadiens à des destinataires n'appartenant pas à la Collectivité des cinq ont été présentées, soit cinq par un client du gouvernement du Canada et une par un allié. Aucune n'a été refusée.

En février 2011, le Cabinet a approuvé un cadre pour réduire les risques inhérents au partage d'information avec des entités étrangères qui pourrait aboutir à des mauvais traitements envers un individu. Cela devait se faire par l'intermédiaire d'une instruction ministérielle adressée aux ministères et organismes du gouvernement du Canada. En conséquence, le ministre de la Défense nationale a émis en 2011 une directive à l'intention du CST exigeant que ce dernier élabore des politiques pour orienter le partage d'information avec des entités ne faisant pas partie de la Collectivité des cinq, notamment des autorisations d'approbation prenant en compte le risque de mauvais traitements. Le Centre s'est conformé à cette exigence.

Une évaluation du risque de mauvais traitements doit être effectuée avant que le CST ne divulgue l'information sur l'identité de Canadiens à des destinataires n'appartenant pas à la Collectivité des cinq, que ce soit à travers les alliés ou un client du gouvernement du Canada. Mon bureau a examiné toutes ces demandes de même que quelques évaluations correspondantes du risque de mauvais traitements.

Les seuls incidents relatifs à la vie privée que mon bureau a découverts, lorsqu'il a épluché toutes les demandes de divulgation, avaient déjà été relevés par le CST et consignés dans le Dossier relatif aux incidents liés à la vie privée que mon bureau examine séparément (voir examen n^{o}7).

Le CST dispose de politiques et de procédures exhaustives qui orientent sa divulgation de renseignements sur l'identité de Canadiens provenant des rapports à des clients du gouvernement du Canada. Pour moi, il est très encourageant de voir que le CST a mis à jour ses politiques pour englober les divulgations à des alliés et à des destinataires n'appartenant pas à la

Collectivité des cinq par l'intermédiaire de clients et d'alliés du gouvernement du Canada.

Mon bureau a examiné tous les formulaires de demande, les rapports, la documentation interne et les approbations, et il a interrogé au besoin le personnel du CST. L'examen de ces documents a révélé que les employés du CST qui mènent à bien les activités liées à la divulgation de renseignements sur l'identité de Canadiens se conforment aux politiques et aux procédures. En outre, dans le cas des demandes examinées, j'ai pu constater que les employés du CST et les gestionnaires responsables de la divulgation de renseignements sur l'identité de Canadiens étaient cohérents et rigoureux dans l'application de toutes les instructions ministérielles, politiques, procédures et normes pertinentes se rapportant à la divulgation d'information sur l'identité de Canadiens, y compris la protection de la vie privée.

Le CST a maintenant complété l'automatisation complète de ses processus de gestion de l'information et des dossiers pour la divulgation de l'information sur l'identité des Canadiens à ses clients du gouvernement du Canada. Ce système semble bien fonctionner. Le CST a indiqué qu'il entreprenait maintenant l'automatisation d'un système similaire pour le processus applicable à toutes les demandes émanant d'alliés. Je surveillerai le cours des choses au moment des examens annuels ultérieurs.

Conclusion

Mon examen n'a pas donné lieu à des recommandations. Le CST a mené ses activités de manière méthodique et s'est conformé à la loi, aux instructions ministérielles ainsi qu'à ses politiques et procédures internes. Au cours de cet examen, j'ai pris connaissance d'information en lien avec le Service canadien du renseignement de sécurité, que j'ai soumise à la présidente intérimaire du Comité de surveillance des activités de renseignement de sécurité pour qu'elle assure le suivi qu'elle juge approprié. J'ai l'intention de continuer à effectuer un examen annuel des renseignements divulgués. Je surveillerai également l'avancement et l'incidence de l'automatisation du processus de traitement des demandes de divulgation de renseignements sur l'identité de Canadiens émanant d'alliés.

7. Examen du Dossier relatif aux incidents liés à la vie privée et du Dossier des erreurs de procédure mineures tenus par le CST, 2014

Contexte

Le CST exige que ses employés responsables des renseignements électromagnétiques étrangers et de la sécurité des technologies de l'information signalent et documentent les incidents relatifs à la vie privée de façon à prévenir d'autres incidents et à renforcer la conformité aux exigences juridiques et ministérielles ainsi qu'aux politiques du Centre. Un incident relatif à la vie privée survient lorsqu'il pourrait être porté atteinte à la vie privée d'un Canadien d'une manière qui est imprévue ou contraire aux politiques du CST. Ces dernières se fondent sur les exigences législatives imposant au CST de ne pas diriger ses activités sur des Canadiens et de mettre en place des mesures pour protéger leur vie privée.

Les incidents sont documentés dans un des deux dossiers décrits ci-après en fonction de l'étendue du risque. Le Dossier relatif aux incidents liés à la vie privée est un registre des incidents ayant donné lieu à une atteinte à la vie privée. Le Dossier sur les erreurs de procédure mineures fait état des erreurs opérationnelles qui se sont produites en lien avec de l'information sur des Canadiens mais qui n'ont pas entraîné une perte de contrôle de cette information par le Centre ni sa communication à des destinataires externes qui n'auraient jamais dû la recevoir. Le CST a mis en place ces deux dossiers en 2007 en prévenant le Bureau du commissaire de l'existence de ces outils.

Au cours de l'année, chaque examen des activités du Centre que je mène inclut généralement une analyse de tout incident relatif à la vie privée se rapportant au sujet de l'examen. Il arrive cependant que les examens individuels ne permettent pas de repérer tous les incidents, ou que les incidents soient recensés au cours d'un examen, mais qu'on ne puisse pas toujours vérifier la réponse du CST, qui peut être en cours au moment de la publication du rapport. L'examen annuel du Dossier relatif aux incidents liés à la vie privée met l'accent sur les atteintes à la vie privée qui n'ont pas été étudiées au cours de mes autres examens, afin de s'assurer que le CST a pris des mesures correctives pertinentes pour toutes les atteintes relevées.

Mon examen a consisté en une analyse du Dossier relatif aux incidents liés à la vie privée, du Dossier des erreurs de procédure mineures signalées et des réponses du CST à mes questions. Mon bureau a également effectué une vérification indépendante d'un échantillon de rapports du Dossier relatif aux incidents liés à la vie privée en procédant à des recherches dans l'une des bases de données du CST.

Cet examen répond à plusieurs objectifs :

- examiner les incidents, les erreurs de procédure et les mesures subséquentes prises par le CST pour apporter des correctifs ou atténuer les conséquences des incidents;
- assurer le suivi d'incidents précis identifiés au cours des examens antérieurs et des mesures correctives connexes prises par le CST;
- déterminer quels incidents peuvent soulever des questions concernant la conformité à la loi ou la protection de la vie privée des Canadiens;
- cerner tout problème systémique donnant à penser que des mesures correctives à un niveau plus général sont requises de la part du CST; et
- contribuer à l'évaluation du cadre de validation de la conformité à la politique et des activités de surveillance du CST.

Constatations

J'ai constaté que le CST a pris des mesures correctives appropriées en réponse aux erreurs de procédure mineures et aux incidents relatifs à la vie privée qu'il a relevés et consignés en 2014. Au cours de mon examen, aucun de ces incidents ou erreurs n'a semblé indiquer des problèmes ou des lacunes systémiques nécessitant un examen de suivi.

J'avais recommandé l'an dernier que le CST demande à ses alliés de confirmer qu'ils avaient pris les mesures voulues suite aux incidents relatifs à la vie privée d'un Canadien, et que le Centre consigne au dossier la réponse émanant des alliés. Cette année, je constate que la réponse du CST et les activités de suivi de cette question sont satisfaisantes. Un examen portant sur un échantillon de demandes du CST adressées à des alliés, de même que l'examen du Dossier relatif aux incidents liés à la vie privée ont montré que le Centre prend des mesures pour mettre en œuvre

ma recommandation. Je continuerai de suivre de près ce point. Par ailleurs, le CST travaille à la révision de sa politique pour intégrer de nouvelles lignes directrices se rapportant à la façon dont il traite l'information sur l'identité dans les rapports portant sur les renseignements électromagnétiques étrangers – en renforçant la protection de la vie privée des Canadiens. Au cours de mes examens futurs, je me pencherai sur l'incidence des changements apportés à cette politique.

Une défectuosité technique survenue cette année dans un système du CST – et consignée comme un incident relatif à la vie privée distinct – a eu des répercussions sur le traitement d'autres incidents relatifs à la vie privée. À l'issue de mon examen de la documentation fournie, je suis satisfait que le CST a agi en temps opportun et a pris les mesures qui s'imposaient pour corriger la situation.

Comme je l'ai mentionné dans l'*Examen annuel d'un échantillon de renseignements concernant l'identité de Canadiens divulgués par le CSTC à des clients du gouvernement du Canada et aux partenaires étrangers* que j'ai effectué l'an dernier, mon bureau a relevé deux incidents relatifs à la vie privée se rapportant à deux Canadiens dont l'identité n'avait pas été supprimée dans le rapport du renseignement et que le CST avait par la suite consignés au Dossier relatif aux incidents liés à la vie privée. Je me suis penché sur les atteintes à la vie privée et les rapports émis à nouveau pour m'assurer que l'information sur l'identité des Canadiens était désormais supprimée et j'ai constaté que le Centre avait pris des mesures d'atténuation pertinentes.

En mai 2014, le CST m'a informé d'un incident relatif à la vie privée se rapportant à la circulation d'information entre un client du gouvernement du Canada et des alliés du CST comportant un risque de divulgation sans autorisation de renseignements se rapportant à la vie privée. À ce moment-là, mon bureau a examiné une note d'information sur la question adressée à la direction du CST et il a estimé que les actions et les engagements pris par le CST pour mettre fin à cette pratique étaient appropriés et ne soulevaient aucune question pressante. Tout en examinant le dossier des incidents relatifs à la vie privée, j'ai passé en revue des documents supplémentaires en relation avec cet incident. Je peux affirmer que le CST a pris des mesures correctives appropriées en réponse à l'incident relatif à la vie privée. La divulgation proactive de cet incident à mon bureau par le CST montre qu'il est déterminé à faire preuve de transparence et à protéger la vie privée.

Conclusion

Mon examen ne donne lieu à aucune recommandation et n'a mis au jour aucune lacune systémique. Au moment de mes examens ultérieurs, je prendrai en compte l'incidence de la politique actualisée sur la façon dont le CST traite l'information sur l'identité dans les rapports sur les renseignements électromagnétiques étrangers.

PLAINTES CONCERNANT LES ACTIVITÉS DU CST

En 2014-2015, mon bureau a été contacté par plusieurs personnes en quête d'information ou exprimant des préoccupations concernant les activités du CST. Toutefois, nous avons déterminé que les demandes de renseignements ne relevaient pas de mon mandat, ne se rapportaient pas aux activités opérationnelles du CST ou n'étaient pas sérieuses. Aucune plainte concernant les activités du CST ne justifiait mon enquête. (Pour obtenir davantage d'information sur le processus de plainte, consultez le site Web du Bureau.)

MANDAT SOUS LE RÉGIME DE *LA LOI SUR LA PROTECTION DE L'INFORMATION*

Je suis tenu, en vertu de la *Loi sur la protection de l'information*, de recevoir de l'information émanant de personnes astreintes au secret à perpétuité qui ont l'intention de communiquer des renseignements opérationnels spéciaux – par exemple, certains renseignements se rapportant aux activités du Centre – en faisant valoir la primauté de l'intérêt public. Aucune affaire de ce genre ne m'a été signalée en 2014-2015. (Pour obtenir davantage d'information sur les responsabilités du commissaire en vertu de la *Loi sur la protection de l'information*, consultez le site Web du Bureau.)

ACTIVITÉS DU BUREAU DU COMMISSAIRE

Pour atteindre mon objectif de transparence accrue, mes employés et moi-même avons fait des efforts concertés afin de sensibiliser davantage le public au travail de mon bureau. Pour atteindre notre but, nous avons

publié davantage d'information sur notre site Web et dans mon rapport public annuel, nous avons participé à des conférences et à des colloques où nous avons pris la parole, nous avons répondu aux demandes de renseignements de médias et participé à des réunions bilatérales avec nos collègues des autres organismes d'examen canadiens ou des organismes d'examen d'autres pays.

Quand j'ai indiqué dans le rapport annuel de l'an dernier que le site Web du Bureau renfermait de nouveaux renseignements détaillés afin de dissiper les malentendus et de répondre aux questions et aux critiques concernant le rôle et le travail du commissaire, je promettais d'afficher de l'information détaillée concernant la façon dont mon bureau examine les activités opérationnelles du CST. Au cours de l'exercice écoulé, j'ai ajouté des précisions sur les examens indiquant la façon dont je choisis les activités à examiner, la façon dont je mène mes examens, les critères en vertu desquels les examens sont articulés et la façon dont je fais rapport sur les constatations de mes examens. (Pour obtenir davantage d'information au sujet des examens, consultez le site Web du Bureau.)

Mon bureau a également continué de faire des présentations sur notre travail dans le cadre de l'accueil des nouveaux employés du CST. Ces séances ont cessé à la fin du printemps lorsque le Centre a commencé à emménager dans son nouvel immeuble mais devraient reprendre plus tard en 2015. Comme dans les anciens locaux du CST, nous disposerons de bureaux spéciaux, indépendants et sécurisés dans le nouvel édifice, où nous pourrons mener nos entretiens et travailler sur place au cours de nos examens.

Le directeur exécutif a participé à la Conférence sur la vie privée et la sécurité qui a eu lieu à Victoria, en Colombie-Britannique, en février. Cette importante conférence explore les sujets d'actualité et les controverses liés aux technologies de l'information et des télécommunications, à la protection de l'information, au rôle du gouvernement et des organismes gouvernementaux, ainsi qu'à la protection de la vie privée.

Tout au long de l'année, le personnel de mon bureau a également assisté à de nombreuses autres conférences portant sur les affaires internationales, la sécurité des technologies de l'information, la sécurité nationale et la protection de la vie privée, et parrainées par de nombreuses organisations différentes telles que l'Institut canadien d'administration de la justice, l'Institut de la conférence des associations de la défense et l'Association canadienne pour les études de renseignement et de sécurité.

Mon bureau a également apporté son soutien au Réseau canadien de recherche sur le terrorisme, la sécurité et la société, qui a été lancé par plusieurs universitaires avec l'aide de ministères et organismes gouvernementaux. Notre soutien a été non financier et, en fait, mon personnel a proposé de lire et de commenter certains rapports du Réseau pour engager un débat avec les chercheurs ainsi que d'assister à des réunions ou à des colloques pertinents.

Tout au long de l'année, j'ai rencontré plusieurs de mes collègues de l'examen au Canada et dans d'autres pays.

Consultation avec les organismes d'examen au Canada

Le Forum des organismes d'examen est une réunion des représentants de mon bureau, du Comité de surveillance des activités de renseignement de sécurité (CSARS), de la Commission civile d'examen et de traitement des plaintes relatives à la GRC (CCETP) et du Commissariat à la protection de la vie privée du Canada. Ce forum offre la possibilité de comparer les pratiques exemplaires dans les méthodes d'examen et de discuter des questions d'intérêt et de préoccupation mutuels mais exclut tout échange sur les détails opérationnels des examens. Le forum s'est réuni en novembre et en mars.

J'ai rencontré la présidente par intérim du CSARS pour des discussions d'ordre général concernant la collaboration entre nos organisations, et nos directeurs exécutifs respectifs ont convenu de coordonner certains éléments de base de deux examens des activités concernant à la fois le CST et le SCRS. Comme je l'ai déjà noté dans la section sur l'examen, je lui ai fait part de deux recommandations et d'une autre question qui

concernent le SCRS, à titre d'information et à des fins de suivi, si elle le juge pertinent. Les directeurs exécutifs de mon bureau, du CSARS et de la CCETP se sont également rencontrés pour discuter d'autres possibilités de collaboration et échanger des points de vue sur des questions se rapportant à l'examen des organismes de sécurité et du renseignement.

En juin 2014, le directeur exécutif de mon bureau, de concert avec son homologue du CSARS, a participé à un comité au troisième sommet annuel de haut niveau des agents principaux de la sécurité de l'information qui s'est tenu à Vancouver. Ils y ont exposé le rôle de leur organisation respective dans la reddition de comptes publique des organismes du renseignement qu'ils sont chargés d'examiner. Ce groupe spécialisé et informé, qui s'intéresse à l'environnement de la menace et au rôle des organismes du renseignement, s'est demandé si la législation et les cadres actuels rendent bien compte de l'environnement opérationnel actuel et de l'intérêt public.

J'ai rencontré le nouveau commissaire à la protection de la vie privée du Canada, Daniel Therrien, quelques mois après sa nomination. En octobre, j'ai présenté une allocution à la réunion des commissaires à l'information et à la protection de la vie privée fédéraux, provinciaux et territoriaux qui s'est déroulée à Ottawa. J'ai expliqué mon mandat et mon rôle et j'ai parlé de l'intérêt commun que nous servons en assurant la protection de la vie privée des Canadiens. Ces commissaires ont un domaine de responsabilité beaucoup plus étendu que le mien dans la mesure où leur mandat s'applique à la plupart des ministères et organismes dans leurs domaines de compétence respectifs, alors que mon mandat se concentre exclusivement sur le CST. J'ai néanmoins trouvé la discussion avec les commissaires à l'information et à la protection de la vie privée instructive et utile, puisqu'elle m'a donné une idée de leurs préoccupations et de leurs points de vue particuliers.

Consultation avec les organismes d'examen étrangers

En juillet dernier, le directeur exécutif et le directeur des opérations se sont joints à moi pour assister à la 9e Conférence internationale des organismes de surveillance qui se déroulait à Londres et a attiré les représentants de 14 autres pays. Grâce à ces conférences biennales, les parlementaires et les titulaires de charge publique de haut rang travaillant dans le domaine de

l'examen et de la surveillance du renseignement ont la possibilité d'échanger des idées et de faire part de leur expérience sur des sujets d'intérêt mutuel. La conférence aide également les pays qui mettent sur pied des mécanismes d'examen et de surveillance du renseignement en tirant parti de l'expérience des pays disposant de structures en place. Les séances de la conférence ont été consacrées à des sujets comme l'avenir de la surveillance du renseignement, les attentes du public en matière de protection de la vie privée et le concept de la proportionalité. Nous avons aussi parlé des efforts pour parvenir à une plus grande transparence. L'élargissement du dialogue et de nos réseaux d'experts grâce à ces conférences a des retombées bénéfiques sur notre travail au Canada. Nous prenons ainsi connaissance des expériences et avons la possibilité de partager les pratiques exemplaires avec une large variété d'organismes voués à l'examen et à la surveillance.

En décembre, certains de mes employés et moi-même avons rencontré l'examinateur indépendant de la législation antiterroriste du Royaume-Uni, David Anderson, Q.C. M. Anderson a été chargé par le gouvernement britannique de déterminer si le Royaume-Uni a besoin d'une nouvelle législation ou de modifications à la loi pour traiter des pouvoirs d'interception des organismes de sécurité et de renseignement. Son mandat inclut également les *communications data*, soit le terme utilisé au Royaume-Uni pour ce que nous appelons au Canada les métadonnées. Dans le cadre de cet échange fructueux, nous en avons appris davantage sur les grandes lignes de son rôle en tant qu'examinateur indépendant.

Dans le rapport annuel que j'ai présenté l'an dernier, je concluais à l'issue de mon examen du partage de renseignements électromagnétiques étrangers avec des partenaires étrangers que j'explorerai les options pour collaborer avec les organismes d'examen des pays alliés afin d'examiner les activités de partage d'information entre leurs agences du renseignement respectives et de vérifier l'application de leurs politiques respectives. Lors de notre voyage à Londres pour assister à la Conférence internationale des organismes de surveillance, nous avons rencontré les représentants de l'Interception of Communications Commissioner's Office du Royaume-Uni pour discuter de notre expérience en matière de méthode d'examen ainsi que des questions relatives à la protection de la vie privée et des cadres juridiques, et faire des comparaisons. En janvier, je me suis rendu à

Washington D.C., accompagné de mon directeur exécutif et de la directrice des opérations par intérim pour rencontrer l'inspecteur général de la U.S. Intelligence Community et ensuite l'inspecteur général de la National Security Agency (NSA).

L'inspecteur général de la U.S. Intelligence Community est responsable de la conduite des audits, des enquêtes, des inspections et des examens de tout le milieu du renseignement américain. Notre réunion regroupait des inspecteurs généraux et des représentants de plusieurs autres organismes. Malgré des différences importantes entre mon bureau et les inspecteurs généraux – la principale étant que les inspecteurs généraux sont dotés d'un mandat plus étendu, alors que j'ai comme mandat spécifique le contrôle de la légalité – le principal but de notre réunion était d'en apprendre davantage sur le niveau de collaboration entre les inspecteurs généraux du milieu du renseignement et la façon dont je pourrais appliquer cet enseignement à mes efforts pour encourager la collaboration entre les organismes d'examen canadiens. Je voulais également discuter des interactions entre les inspecteurs généraux et d'autres bureaux établis récemment au sein des agences de renseignement, notamment ceux responsables des libertés civiles et de la protection de la vie privée, ou assurant la protection des dénonciateurs et des sources. J'ai été frappé par le franc-parler de mes hôtes dans les discussions portant sur ces questions et dans le partage des idées. Cette réunion hautement méritoire stimulera ma réflexion sur mon propre travail.

À la suite de la réunion avec l'inspecteur général de la U.S. Intelligence Community et ses collègues, nous avons rencontré l'inspecteur général de la NSA. Les discussions ont porté expressément sur mon rapport annuel de l'an dernier concernant le partage par le CST de renseignements électromagnétiques étrangers avec ses partenaires étrangers. Comme je l'ai indiqué dans le présent rapport, je voulais recevoir des garanties personnelles – que j'ai obtenues – de l'inspecteur général concernant les politiques et les procédures de la NSA en matière de traitement de l'information visant les Canadiens.

PLAN DE TRAVAIL – EXAMENS EN COURS ET PRÉVUS

Les commissaires adoptent une approche de prévention axée sur le risque pour leurs examens. Je procède à partir d'un plan de travail triennal mis à jour deux fois par an dont l'élaboration repose sur de nombreuses sources, notamment les séances d'information régulières du CST sur les nouvelles activités et les changements touchant les activités en place. Je prends également connaissance du rapport annuel classifié présenté par le chef du Centre au ministre de la Défense nationale et faisant état des priorités du Centre et de ses problèmes importants sur le plan juridique, politique ou en matière de gestion.

À l'exception de mon examen des activités du CST relatives aux métadonnées tirées des renseignements électromagnétiques étrangers qui, pour certains aspects, se poursuivra au cours de l'année à venir, et de mon examen de certaines activités de collecte de renseignements électromagnétiques étrangers menées sous le régime des autorisations ministérielles, tous les examens qui étaient en cours l'an dernier ont été menés à bien.

Les examens prévus pour 2014-2015 sont : un examen ciblé des activités relatives aux métadonnées en lien avec les activités de sécurité des technologies de l'information menées par le CST, un examen de certaines activités de collecte de renseignements électromagnétiques étrangers menées sous le régime des autorisations ministérielles et en vertu de directives ministérielles, un examen du partage des renseignements électromagnétiques étrangers entre le CST et les partenaires étrangers, un examen d'une activité particulière du CST à l'appui du Service canadien du renseignement de sécurité en vertu de la partie *c*) de son mandat et de l'article 12 de la *Loi sur le Service canadien du renseignement de sécurité*; et une étude du partage de l'information entre la Section responsable des renseignements électromagnétiques étrangers et celle responsable de la sécurité des technologies de l'information au sein du CST.

De plus, j'effectuerai les examens annuels portant sur : 1) les autorisations ministérielles relatives à la collecte de renseignements électromagnétiques étrangers et à la sécurité des TI; 2) les renseignements sur l'identité de Canadiens divulgués par le CST; et 3) les incidents relatifs à la vie privée et les erreurs de procédure signalés par le CST et les mesures prises subséquemment par le Centre pour y remédier. J'envisage également de poursuivre les vérifications ponctuelles des communications privées que le CST a interceptées, utilisées et conservées.

ANNEXE A : EXTRAITS DE LA *LOI SUR LA DÉFENSE NATIONALE* ET DE LA *LOI SUR LA PROTECTION DE L'INFORMATION* RELATIFS AU MANDAT DU COMMISSAIRE

Loi sur la défense nationale — Partie V.1

Nomination du commissaire et durée du mandat

273.63 (1) Le gouverneur en Conseil peut nommer, à titre inamovible pour une période maximale de cinq ans, un juge à la retraite surnuméraire d'une juridiction supérieure qu'il charge de remplir les fonctions de commissaire du Centre de la sécurité des télécommunications.

Mandat

(2) Le commissaire a pour mandat

a) de procéder à des examens concernant les activités du Centre pour en contrôler la légalité;

b) de faire les enquêtes qu'il estime nécessaires à la suite de plaintes qui lui sont présentées;

c) d'informer le ministre et le procureur général du Canada de tous les cas où, à son avis, le Centre pourrait ne pas avoir agi en conformité avec la loi.

Rapport annuel

(3) Le commissaire adresse au ministre, dans les quatre-vingt-dix jours suivant la fin de chaque exercice, un rapport sur l'exercice de ses activités. Le ministre dépose le rapport devant chacune des chambres du Parlement dans les quinze premiers jours de séance de celle-ci suivant sa réception.

(4) Dans l'exercice de son mandat, le commissaire a tous les pouvoirs conférés à un commissaire en vertu de la partie II de la *Loi sur les enquêtes*.

Assistance

(5) Le commissaire peut retenir les services de conseillers juridiques ou techniques ou d'autres collaborateurs dont la compétence lui est utile dans l'exercice de ses fonctions; il peut fixer, avec l'approbation du Conseil du Trésor, leur rémunération et leurs frais.

Fonctions du commissaire

(6) Le commissaire exerce les attributions que lui confèrent la présente partie et toute autre loi fédérale; il peut en outre se livrer à toute activité connexe autorisée par le gouverneur en conseil.

[...]

Examen des autorisations

273.65 (8) Le commissaire du Centre de la sécurité des télécommunications est tenu de faire enquête sur les activités qui ont été exercées sous le régime d'une autorisation donnée en vertu du présent article pour en contrôler la conformité; il rend compte de ses enquêtes annuellement au ministre.

Défense d'intérêt public

15. (1) Nul ne peut être déclaré coupable d'une infraction prévue aux articles 13 ou 14 s'il établit qu'il a agi dans l'intérêt public.

[...]

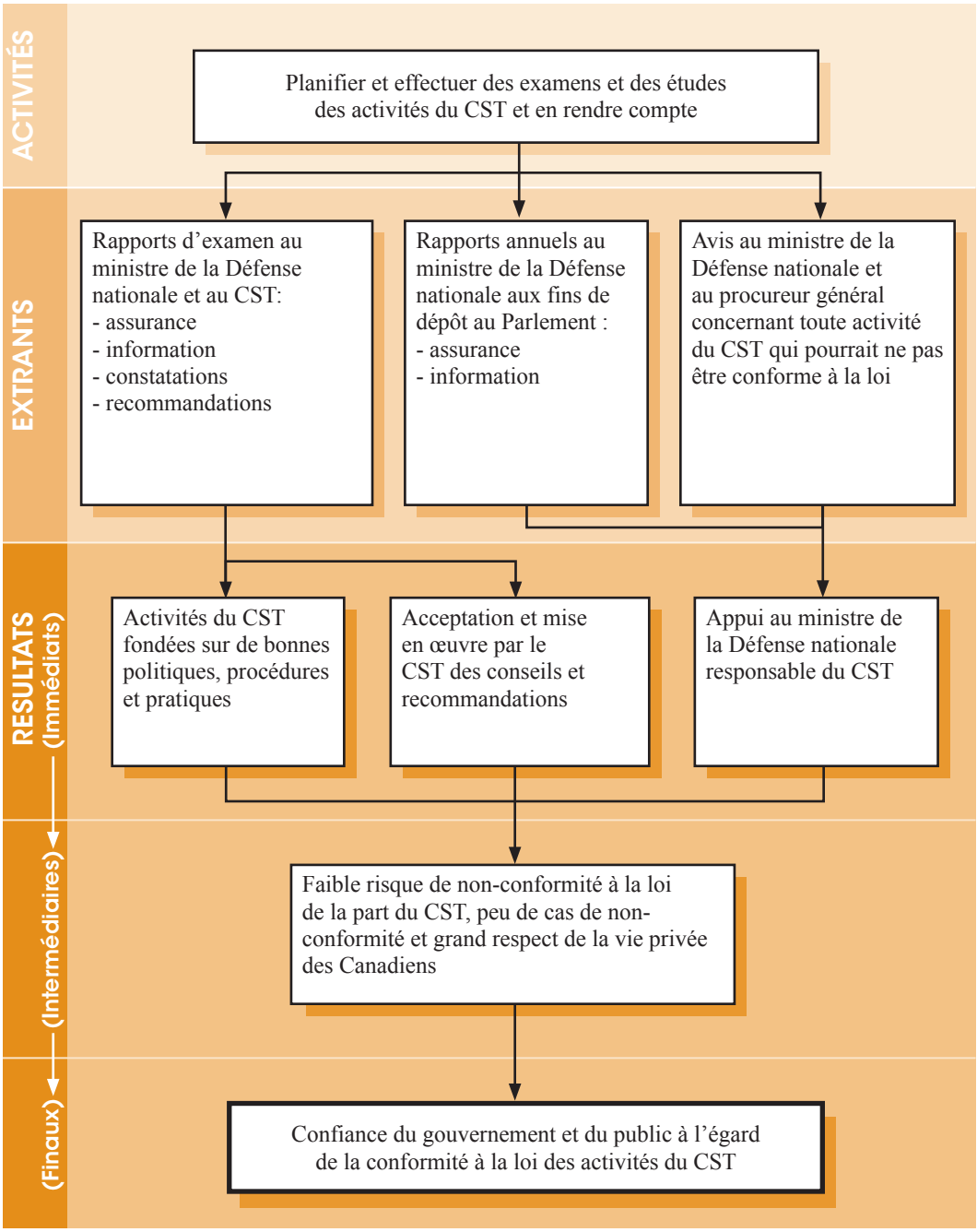
Informer les autorités

(5) Le juge ou le tribunal ne peut décider de la prépondérance des motifs d'intérêt public en faveur de la révélation que si la personne s'est conformée aux exigences suivantes : [...]

b) dans le cas où elle n'a pas reçu de réponse de l'administrateur général ou du sous-procureur général du Canada dans un délai raisonnable, elle a informé de la question, avec tous les renseignements à l'appui en sa possession, [...]

(ii) soit le commissaire du Centre de la sécurité des télécommunications si la question porte sur une infraction qui a été, est en train ou est sur le point d'être commise par un membre du Centre de la sécurité des télécommunications dans l'exercice effectif ou censé tel de ses fonctions pour le compte de celui-ci, et n'en a pas reçu de réponse dans un délai raisonnable.

ANNEXE B : PROGRAMME D'EXAMEN DU BUREAU DU COMMISSAIRE – MODÈLE LOGIQUE



ANNEXE C: ÉTAT DES DÉPENSES DE 2014-2015

Sommaire des articles courants (en dollars)

Salaires et avantages sociaux	1 241 763
Transport et télécommunications	47 916
Information	12 931
Services professionnels et spéciaux	353 986
Locations	325 649
Achats de services de réparation et d'entretien	2 029
Matériels et fournitures	12 616
Machines et équipement	1 850
Immobilisations	8 700
Autres paiements (Paiement transitoire ponctuel au titre des paiements de salaires en arriéré)	36 120
Total	**2 043 560**