



Commissaire
du Centre de
la sécurité des
télécommunications

RAPPORT ANNUEL
2015 – 2016

20

années d'examen

Canada

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

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

© Sa Majesté la Reine du Chef du Canada, représentée par le
Bureau du commissaire du Centre de la sécurité des
télécommunications, 2016

N° de catalogue : D95F
ISSN 1700-0882

Communications Security
Establishment Commissioner



Commissaire du Centre de la
sécurité des télécommunications

The Honourable Jean-Pierre Plouffe, CD

L'honorable Jean-Pierre Plouffe, CD

Juin 2016

Ministre de la Défense nationale
Édifice MGén George R. Pearkes, 13^e étage
101, promenade Colonel By, tour Nord
Ottawa (Ontario) 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 1^{er} avril 2015 au 31 mars 2016, aux fins de présentation au Parlement.

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

A handwritten signature in blue ink, appearing to read 'J. Plouffe'.

Jean-Pierre Plouffe

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

TABLE DES MATIÈRES

Message du commissaire.....	3
Le mandat et les activités d'examen du commissaire.....	7
Évolution du travail du bureau au cours des 20 dernières années.....	11
Le point sur les efforts déployés par le CST pour donner suite aux recommandations.....	12
Aperçu des constatations et des recommandations de 2015–2016.....	14
Vingt années de changement grâce à l'examen.....	15
Points saillants des rapports présentés au ministre en 2015–2016.....	17
1. Examen du soutien apporté par le CST au Service canadien du renseignement de sécurité en vertu de la partie c) de son mandat concernant un certain type de rapport mettant en cause des Canadiens.....	17
2. Examen des activités du CST relatives aux métadonnées liées aux renseignements électromagnétiques étrangers (volet 2).....	21
Mise à jour concernant la non-minimisation d'informations sur l'identité de Canadiens avant leur communication aux alliés.....	24
3. Examen d'une méthode particulière de collecte de renseignements électromagnétiques étrangers adoptée par le CST sous le régime d'une autorisation ministérielle.....	26
4. Examen combiné annuel des autorisations ministérielles du CST relatives à la collecte de renseignements électromagnétiques étrangers et à l'interception de communications privées.....	29
5. Examen annuel des activités de cyberdéfense du CST menées sous le régime d'une autorisation ministérielle.....	34
6. Examen annuel de la divulgation d'information sur l'identité de Canadiens, 2014–2015.....	40
7. Examen annuel du Dossier relatif aux incidents liés à la vie privée et du Dossier des erreurs de procédure mineures tenus par le CST, 2015.....	43
Un thème récurrent : Modifications apportées à la <i>Loi sur la défense nationale</i>	46
Plaintes concernant les activités du CST.....	48

Mandat sous le régime de la *Loi sur la protection de l'information*.....48

Activités du bureau du commissaire.....49

Plan de travail – Examens en cours et prévus.....52

Annexe A : Biographie de l'honorable Jean-Pierre Plouffe, CD..... 54

Annexe B : Extraits de la *Loi sur la défense nationale* et de la *Loi sur la protection de l'information* relatifs au mandat du commissaire..... 55

MESSAGE DU COMMISSAIRE



En accordant de nouveaux pouvoirs aux organismes de sécurité et de renseignement, la législation visant à lutter contre le terrorisme adoptée l’an dernier a suscité des interrogations quant à l’exercice d’une surveillance adéquate. Les atrocités commises par le groupe terroriste qui se fait appeler État islamique et la violence des attentats perpétrés par ses partisans, qui recrutent dans leurs rangs des extrémistes au Canada et des combattants étrangers canadiens, attisent le débat. C’est dans ce contexte

que, m’acquittant de mes fonctions en tant que commissaire, j’ai informé le ministre de la Défense nationale et le procureur général du Canada que le Centre de la sécurité des télécommunications (CST) menait des activités relatives aux métadonnées qui, à mon avis, n’étaient pas conformes à la loi. Il s’agissait d’une première pour le bureau et l’annonce de cette constatation a coïncidé avec le dépôt au Parlement de mon rapport annuel précédent — six mois plus tard qu’à l’ordinaire en raison du déclenchement des élections fédérales. J’ai néanmoins trouvé encourageant de voir par la suite une plus grande transparence des activités du CST.

Le 19 juin 2016, cela fera vingt ans que le Bureau du commissaire du Centre de la sécurité des télécommunications contribue à faire en sorte que le CST se conforme à la loi, ce qui inclut la protection de la vie privée des Canadiens. Alors que je réfléchis sur mon expérience au cours de mon mandat de commissaire, qui s’achèvera en octobre 2016, le présent rapport annuel m’offre la possibilité de faire état des progrès importants et de certaines réalisations clés du bureau au cours des 20 dernières années. Le bureau peut être fier du rôle qu’il a joué dans la protection de la vie privée des Canadiens, car, en plus de son appui au ministre dans sa reddition de comptes et le contrôle du CST, il a su convaincre le public que le CST fait l’objet d’un examen rigoureux pour déterminer si ses activités sont conformes à la loi et s’il prend des mesures adéquates pour protéger la vie privée des Canadiens. En fait, comme l’honorable juge Dennis O’Connor l’a écrit dans son rapport en 2006 à l’issue de la Commission d’enquête sur les actions des responsables canadiens

relativement à Maher Arar, le bureau « fonctionne très bien. Je ne vois donc aucune raison d'intervenir dans ses activités. »

Bien que le bureau puisse s'enorgueillir de certaines réalisations d'importance majeure au cours de ses 20 années d'existence, un travail important l'attend. Le nouveau gouvernement a pris des engagements, à savoir accroître la transparence, renforcer la reddition de comptes des organismes de sécurité et de renseignement et assurer un meilleur équilibre entre la sécurité collective et les droits et libertés des citoyens, ce qui inclut à coup sûr l'adoption de mesures satisfaisantes pour protéger la vie privée des Canadiens. À cette fin, j'ai envoyé une lettre à M. David McGuinty, député — à qui le premier ministre a confié un rôle de direction au sein du comité parlementaire sur la sécurité nationale qu'il a proposé — dont j'ai envoyé copie aux ministres de la Défense nationale et de la Sécurité publique ainsi qu'au leader du gouvernement à la Chambre des communes, afin de leur présenter mes observations et commentaires d'après mon expérience en qualité de commissaire du CST.

Le modèle canadien d'examen expert des organismes de sécurité et de renseignement est efficace. Il repose sur l'existence d'un organisme d'examen indépendant propre à l'organisme examiné et indépendant du gouvernement. Ces organismes d'examen disposent de pouvoirs qui leur garantissent un accès sans entrave aux organismes qu'ils examinent, y compris à tout le personnel. Grâce à des employés dévoués comptant de nombreuses années d'expérience, on est parvenu à une connaissance approfondie de la nature sensible sur le plan opérationnel et souvent complexe sur le plan technique et juridique des activités des organismes de sécurité et de renseignement. Je sais que mon bureau a élaboré des méthodes rigoureuses lui permettant d'effectuer un examen exhaustif et robuste. Les organismes d'examen sont également habitués à la tâche délicate d'informer le public concernant leur travail, dans la mesure du possible, tout en protégeant les renseignements sensibles.

Même si j'apprécie au plus haut point le modèle d'examen que nous avons développé au Canada, des changements s'imposent à mesure que le contexte évolue, tant sur le plan technologique que sur le front des menaces pour la sécurité. La clarification de la *Loi sur la défense nationale*, comme le recommandent les commissaires depuis plus de 10 ans, appuierait le gouvernement dans les engagements qu'il a pris de renforcer la reddition de comptes et la transparence du CST. Des modifications à la loi pourraient également offrir au commissaire, qui est un juge à la retraite d'une cour supérieure, de nouvelles fonctions pour appuyer le ministre dans sa reddition de comptes et le contrôle du CST.

Par exemple, le commissaire pourrait fournir au ministre une évaluation spécialisée indépendante des autorisations ministérielles proposées, des conditions d'autorisation définies dans la Loi pour vérifier qu'elles sont remplies et des mesures de protection correspondantes de la vie privée. Cette approche cadrerait avec les modèles étrangers, tels que les réformes en cours au Royaume-Uni.

Les préoccupations que suscitent, sur le plan de la légalité et de la vie privée, la coopération et l'échange de renseignements entre les organismes de sécurité et de renseignement soulèvent une autre question, à savoir celle de la coopération entre les organismes d'examen. Certes, les organismes d'examen peuvent travailler dans une certaine mesure de manière concertée en vertu des lois en vigueur. Toutefois, comme je l'ai mentionné auparavant, il y a lieu de modifier la législation pour les autoriser expressément à échanger de l'information, à mener des enquêtes conjointes et à préparer des rapports concertés, et pour exiger que les organismes de sécurité et de renseignement coopèrent avec eux.

Je suis favorable à l'engagement pris par le gouvernement d'établir un comité parlementaire axé sur la sécurité nationale et dont les membres possèderaient l'habilitation de sécurité requise. De concert avec les organismes d'examen experts, un tel comité offrirait un cadre exhaustif pour la reddition de comptes concernant les activités de sécurité et de renseignement et pourrait contribuer à renforcer la confiance du public. Les rôles respectifs, toutefois, doivent être définis clairement pour éviter la confusion, le dédoublement des efforts et le gaspillage de ressources. Mon bureau pourrait demander des ressources supplémentaires pour travailler avec le nouveau comité parlementaire et appuyer la tenue d'examens conjoints.

Enfin, un mot concernant la transparence — qui est la pierre angulaire de ma démarche en tant que commissaire. La transparence est essentielle pour démystifier le travail du CST, pour contribuer à un débat public plus éclairé, pour améliorer la reddition de comptes et pour atteindre l'objectif ultime du bureau, qui est le maintien de la confiance du public dans le travail important accompli par le CST. C'est pourquoi j'ai continué à exhorter le CST à rendre public le maximum d'information possible tout en respectant les restrictions imposées par la *Loi sur la protection de l'information* et à examiner soigneusement si certains renseignements doivent demeurer classifiés.

Au cours de l'exercice écoulé, j'ai été heureux d'être invité à comparaître à deux reprises devant le Comité sénatorial permanent de la sécurité nationale et de la défense pour expliquer les activités de mon bureau et mes conclusions. À mesure que le gouvernement poursuit son programme de sécurité globale, j'espère avoir l'occasion de contribuer davantage à l'élaboration de propositions propres à renforcer à la fois la reddition de comptes de la part du CST et la confiance du public.

LE MANDAT ET LES ACTIVITÉS D'EXAMEN DU COMMISSAIRE

Mandat

Le mandat du Centre de la sécurité des télécommunications (CST), énoncé à la partie V.1 de la *Loi sur la défense nationale* (LDN), est le suivant :

1. procéder à des examens concernant les activités du CST pour en contrôler la légalité;
2. faire les enquêtes que le commissaire estime nécessaires à la suite d'une plainte écrite; et
3. informer le ministre de la Défense nationale (responsable du CST devant le Parlement) et le procureur général du Canada de toutes les activités du CST qui, à son avis, pourraient ne pas être conformes à la loi.

En vertu de l'article 15 de la *Loi sur la protection de l'information*, le commissaire a également pour mandat de recevoir de l'information émanant de personnes astreintes au secret à perpétuité qui souhaitent communiquer des renseignements opérationnels spéciaux du CST en faisant valoir la primauté de l'intérêt public.

La LDN exige que le commissaire du CST soit un juge surnuméraire ou un juge à la retraite d'une cour supérieure. Elle confère au commissaire une autonomie complète, de même qu'un accès sans entrave à tous les systèmes et installations du CST ainsi qu'à son personnel, notamment le pouvoir d'assigner à comparaître pour obliger des particuliers à répondre à des questions. Le Commissaire a un budget distinct accordé par le Parlement.

Le processus d'examen

Le processus d'examen décrit l'approche du commissaire pour passer en revue les activités du CST. Celles-ci incluent la collecte de renseignements étrangers sur des cibles étrangères situées à l'extérieur du Canada, c'est-à-dire de l'information sur les moyens, les intentions ou les activités de cibles étrangères se rapportant aux affaires internationales, à la défense ou à la sécurité. Le CST est également l'organisme technique du Canada responsable de la cyberdéfense et de la cryptographie mais

aussi des autres technologies de sécurité de l'information requises pour protéger les systèmes et les réseaux informatiques du gouvernement renfermant des renseignements nationaux et personnels sensibles. Le CST a en outre pour mandat de mettre à profit ses capacités uniques afin de fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité dans l'exercice des fonctions que la loi leur confère.

L'objet du mandat d'examen du commissaire consiste :

- à déterminer si le CST se conforme à la loi et, si le commissaire est d'avis 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 enquêter sur les activités du CST menées en vertu d'une autorisation ministérielle pour en contrôler la conformité et à vérifier que les conditions d'autorisation requises par la *Loi sur la défense nationale* sont remplies;
- à vérifier que le CST, dans le cadre de ses activités de collecte de renseignements électromagnétiques étrangers et de cyberdéfense, ne cible pas des Canadiens ou d'autres personnes au Canada; et
- à promouvoir l'élaboration et l'application efficaces de mesures satisfaisantes pour protéger la vie privée des Canadiens dans toutes les activités opérationnelles que le CST entreprend.

Les activités du CST sont distinctes des activités de collecte de renseignements criminels et en matière de sécurité menées par d'autres organismes. Il s'agit dans leur cas d'information sur des activités qui pourraient menacer la sécurité du Canada ou la sécurité publique et que l'on obtient généralement en ciblant des Canadiens. Or, le CST se voit expressément interdire de cibler des Canadiens ou des personnes au Canada. Le fait de limiter la collecte de renseignements à des cibles étrangères situées à l'extérieur du Canada est compliqué par l'infrastructure d'information mondiale interconnectée et en constante évolution, de même que par les cibles étrangères, qui sont elles-mêmes à la fine pointe de la technologie. Le CST a besoin de capacités techniques très avancées pour acquérir et analyser l'information ainsi que pour détecter et atténuer les cyberactivités malveillantes. Ses méthodes ne sont efficaces que si elles demeurent secrètes.

Pour comprendre les nombreux aspects techniques, juridiques et relatifs à la protection de la vie privée des activités du CST, les agents voués à l'examen ont besoin d'une expertise spécialisée. Ils ont aussi besoin d'habilitations de sécurité du niveau requis pour examiner les dossiers et les systèmes du CST. Enfin, ils sont liés par la *Loi sur la protection de l'information* et ne peuvent divulguer à des personnes non autorisées les renseignements sensibles auxquels ils ont accès.

Le bureau effectue continuellement l'examen :

- d'activités choisies en fonction d'une analyse du risque, pour assurer la conformité à un niveau détaillé;
- des systèmes, des outils et des bases de données électroniques;
- 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 ceux-ci sont appliqués par les employés du CST et pour déceler les lacunes systémiques existantes ou éventuelles.

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

- **Obligations légales** : le commissaire s'attend à ce que le CST mène ses activités en conformité avec la *Charte canadienne des droits et libertés*, la LDN, la *Loi sur la protection des renseignements personnels*, le *Code criminel* et toute autre législation pertinente.
- **Exigences ministérielles** : le commissaire s'attend 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** : le commissaire s'attend 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 ce qui concerne la protection de la vie privée des Canadiens. Il s'attend à ce que les

employés du CST soient au courant des politiques et procédures et qu'ils s'y conforment, mais aussi à ce que le CST dispose d'un cadre efficace de validation de la conformité pour assurer le maintien de l'intégrité de ses activités opérationnelles. Le CST doit en outre être en mesure de rendre compte de façon adéquate des décisions importantes prises et de l'information se rapportant à la conformité et à la protection de la vie privée des Canadiens.

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 habituels et dévoilent la nature et l'importance de tout écart par rapport aux critères. Au besoin, le commissaire formule à l'intention du ministre des recommandations visant à améliorer les mesures de protection de la vie privée ou à corriger les problèmes se rapportant aux activités opérationnelles du CST mis au jour au cours de l'examen. Conformément à la pratique courante de divulgation adoptée par les vérificateurs, le CST reçoit les ébauches des rapports d'examen pour confirmation de l'exactitude des faits.

Le rapport annuel du commissaire est un document public présenté au ministre qui, en vertu de la loi, doit le déposer au Parlement. Le bureau du commissaire publie les titres de tous les rapports d'examen présentés au ministre — 97 à ce jour — sur son site Web.

En 2015–2016, le commissaire a été épaulé par 11 employés, eux-mêmes aidés au besoin par plusieurs spécialistes en la matière. Les dépenses du bureau se sont élevées à 2 034 877 \$, montant qui se situe dans la limite du financement approuvé par le Parlement. Pour en apprendre davantage sur le bureau du commissaire et ses dépenses, veuillez consulter le site Web à : www.ocsec-bccst.gc.ca.

Évolution du travail du bureau au cours des 20 dernières années

La quantité et l'ampleur des examens accomplis ont évolué considérablement au fil des années, augmentant le volume d'information disponible à l'appui de la reddition de comptes ministérielle, du débat éclairé des parlementaires et de la vigilance du public. Au cours des cinq dernières années, les commissaires ont présenté 36 rapports d'examen détaillés au ministre (sept en 2011–2012, six en 2012–2013, sept en 2013–2014, neuf en 2014–2015 et sept cette année).

Les examens menés au cours des 20 dernières années ont donné lieu à 161 recommandations visant à promouvoir la conformité. Le CST a témoigné de son engagement à mettre en œuvre les recommandations se rapportant à la protection de la vie privée; depuis 1996, le CST a en effet accepté et mis en œuvre toutes les recommandations se rapportant à la vie privée. Cela signifie que les mesures visant à protéger la vie privée des Canadiens sont continuellement perfectionnées en fonction du contexte technologique et opérationnel en constante évolution dans lequel le CST doit effectuer son travail.

Les commissaires ont joué un rôle positif important au chapitre de la reddition de comptes, de la transparence et de la conformité des activités du CST. Le travail effectué par le bureau a amené le CST à renforcer plusieurs politiques et pratiques fondamentales se rapportant à la protection de la vie privée.

Les commissaires ont instauré des examens annuels portant sur les renseignements divulgués par le CST concernant l'identité de Canadiens ainsi que sur les incidents liés à la vie privée pour évaluer leur risque inhérent au niveau de la vie privée. Du fait que les autorisations ministérielles permettent l'interception non intentionnelle d'une communication privée – un autre risque pour la vie privée –, les autorisations et les communications privées sont également examinées chaque année.

Les recommandations découlant des examens des commissaires ont également incité le CST à apporter d'importantes révisions à ses pratiques et lignes directrices concernant le partage d'information avec les alliés. Ceci comprend notamment la précision du langage dans les échanges d'information, la présentation claire des attentes en matière de protection de la vie privée relativement à l'information canadienne partagée avec les partenaires et la diffusion des lignes directrices pour officialiser et renforcer les pratiques afin de prévenir les préoccupations éventuelles en matière de protection de la vie privée.

LE POINT SUR LES EFFORTS DÉPLOYÉS PAR LE CST POUR DONNER SUITE AUX RECOMMANDATIONS

Le CST a accepté et mis en œuvre, ou travaille à la mise en œuvre, de 94 pourcent (152) des 161 recommandations formulées depuis 1997, y compris les quatre recommandations incluses dans les rapports de cette année. Les commissaires surveillent la façon dont le CST donne suite aux recommandations, aux constatations négatives et aux questions nécessitant un suivi mentionnées dans les examens. Le bureau du commissaire surveille ainsi 14 recommandations actives auxquelles le CST donne suite — 10 recommandations non encore appliquées des années précédentes et quatre de cette année.

Au cours de l'exercice écoulé, le CST a prévenu le bureau qu'il avait donné suite à six recommandations antérieures.

Dans son rapport de fin d'exercice 2014–2015 concernant les autorisations ministérielles, le CST a mis en œuvre deux recommandations pour fournir des renseignements plus précis au ministre :

- toute variation dans le nombre de communications recueillies et le nombre de communications privées interceptées non intentionnellement qu'il acquiert et conserve est désormais signalée tout au long de la période de validité d'une autorisation ministérielle plutôt que seulement à la fin de la période (depuis l'examen des autorisations ministérielles relatives à la collecte de renseignements électromagnétiques étrangers résumé dans le rapport annuel 2013–2014); et
- il établit une différence entre les communications privées interceptées non intentionnellement dans le cadre des activités de cyberdéfense — qui mettent souvent en cause un code malveillant et des attentes plus faibles ou non-existantes en matière de protection de la vie privée — et celles interceptées dans le cadre des activités de collecte de renseignements électromagnétiques étrangers (depuis l'examen des activités de sécurité de la technologie de l'information menées en vertu d'une autorisation ministérielle résumé dans le rapport annuel 2014–2015).

Le CST a mis en œuvre deux autres recommandations en émettant une orientation stratégique pour :

- préciser les circonstances et le traitement d'un type particulier de « communication canadienne », telle que définie à la page 33 (également depuis l'examen des autorisations ministérielles relatives à la collecte de renseignements électromagnétiques étrangers résumé dans le rapport annuel 2013–2014); et
- officialiser et renforcer les pratiques existantes pour donner suite aux préoccupations éventuelles concernant la protection de la vie privée dans les interactions avec les alliés (depuis l'examen des activités du Bureau de l'anti-terrorisme du CST résumé dans le rapport annuel 2013–2014).

Le CST a donné suite à une recommandation découlant de l'examen de l'assistance qu'il avait fournie au Service canadien du renseignement de sécurité (SCRS) en vertu de l'article 16 de la *Loi sur le Service Canadien du renseignement de sécurité*, résumé dans le rapport annuel 2014–2015, en élaborant une mise en garde à annexer à tout document opérationnel particulier susceptible d'être partagé avec des alliés pour signifier clairement que le document ne doit pas être utilisé sans l'autorisation expresse du CST.

Enfin, le CST a déjà modifié le format de son Dossier relatif aux incidents liés à la vie privée pour donner suite à la recommandation du commissaire formulée dans le rapport de cette année, afin de faire en sorte que les futurs fichiers renferment une information adéquate décrivant et documentant chaque incident de manière approfondie dans le but de faire valoir la conformité et d'indiquer que des mesures appropriées ont été prises pour corriger ou atténuer toute conséquence qui pourrait en découler. Le bureau du commissaire évaluera le format du nouveau fichier dans le cadre de l'examen annuel des incidents liés à la vie privée du prochain exercice.

Le commissaire a encouragé la chef du CST à accélérer le travail pour donner suite à une recommandation importante résumée dans le rapport annuel 2013–2014 demandant que le ministre de la Défense nationale émette une nouvelle directive générale à l'intention du CST qui définit clairement les attentes des Canadiens en matière de protection de la vie privée quand le CST partage des renseignements électromagnétiques étrangers. Comme le partage de l'information avec les alliés constitue un volet essentiel des activités de renseignements électromagnétiques étrangers et d'autres activités du CST, on ne peut nier qu'il pourrait avoir une incidence directe sur la vie privée et la sécurité d'un Canadien lorsqu'une communication privée ou de l'information sur l'identité d'un Canadien est partagée.

APERÇU DES CONSTATATIONS ET DES RECOMMANDATIONS DE 2015–2016

Au cours de l'exercice 2015–2016, le commissaire a présenté au ministre sept rapports classifiés sur ses examens des activités du CST.

Les examens de l'exercice écoulé ont été menés sous l'autorité du commissaire :

- pour s'assurer que les activités du CST sont conformes à la loi — comme il est précisé à l'alinéa 273.63(2)a) de la *Loi sur la défense nationale* (LDN); et
- pour contrôler la conformité des activités du CST menées sous le régime d'une autorisation ministérielle — comme l'établit le paragraphe 273.65(8) de la LDN.

Le premier examen portait sur le soutien assuré par le CST au Service canadien du renseignement de sécurité (SCRS) en vertu de la partie c) de son mandat concernant un certain type de rapport mettant en cause des Canadiens. Le bureau s'est intéressé plus précisément au risque que représentent ces rapports pour la vie privée des Canadiens.

Un examen visait certaines activités relatives aux métadonnées liées aux activités de renseignements électromagnétiques étrangers du CST. Cet examen était le deuxième d'une série d'examens exhaustifs en cours portant sur les activités du CST relatives aux métadonnées.

Un autre examen portait sur une méthode particulière utilisée par le CST pour recueillir des renseignements électromagnétiques étrangers, qui donne régulièrement lieu à un nombre plus élevé d'interceptions non intentionnelles de communications privées.

Comme les années précédentes, le commissaire a effectué des examens annuels des autorisations ministérielles visant la collecte de renseignements électromagnétiques étrangers et la cyberdéfense, y compris des vérifications ponctuelles des communications privées interceptées, utilisées, conservées et détruites par le CST; de la divulgation par le CST d'information sur l'identité de Canadiens; et des incidents et des erreurs de procédure liés à la vie privée.

Les résultats

Chaque année, le commissaire présente une déclaration d'ensemble sur ses constatations concernant la légalité des activités du CST. *Au cours de l'année écoulée, toutes les activités examinées étaient conformes à la loi.*

De même, cette année, le commissaire a formulé cinq recommandations pour promouvoir la conformité à la loi et renforcer la protection de la vie privée, demandant notamment que :

- le CST tienne le ministre au courant de ses activités pour transmettre au SCRS un certain type de rapport mettant en cause des Canadiens;
- le CST harmonise ses pratiques avec les exigences administratives énoncées dans la directive ministérielle préconisant une méthode particulière de collecte de renseignements électromagnétiques étrangers;
- le CST émette des lignes directrices sur le marquage et le dénombrement des communications privées de cybersécurité pour assurer l'exactitude et la cohérence dans les rapports au ministre;
- le CST s'assure que les futurs fichiers du Dossier relatif aux incidents liés à la vie privée renferment une information adéquate pour décrire et documenter chaque incident de manière approfondie; et
- la LDN soit modifiée pour préciser le pouvoir dévolu au CST de recueillir, utiliser, conserver, partager et divulguer des métadonnées.

Vingt années de changement grâce à l'examen

Les examens du commissaire jouent un rôle important dans la promotion d'une culture de la conformité au sein du CST. Nous donnons ci-après quelques exemples de la façon dont les examens des commissaires ont façonné les pratiques du CST et renforcé la protection de la vie privée des Canadiens.

- Les mémoires de demande d'autorisations ministérielles renferment maintenant davantage d'explications et de justifications, de sorte que le ministre puisse mieux comprendre ce que le CST lui demande d'autoriser.

- Le CST a interrompu certaines activités relatives aux métadonnées sur lesquelles le commissaire s'interrogeait afin d'examiner à nouveau la façon dont elles sont menées.
- Le CST a mis en œuvre des systèmes pour mieux documenter et suivre les demandes d'informations sur l'identité de Canadiens présentées par ses clients et partenaires et les renseignements qui leur sont divulgués.
- Le CST a renforcé ses procédures de gestion de l'information, notamment en centralisant son système de gestion des dossiers et en renforçant ses règles de conservation et de destruction des dossiers afin d'être mieux en mesure de documenter et de suivre ses activités, et de fournir la preuve de leur conformité à la loi.
- Le CST a clarifié ses pouvoirs habilitants et révisé les procédures pour fournir une assistance opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité.
- Le CST a cherché à obtenir l'avis du bureau du commissaire lorsqu'il a apporté d'importants changements à son cadre redditionnel ainsi qu'à ses politiques et procédures pour les activités de cyberdéfense menées sous le régime d'autorisations ministérielles.
- Les rapports présentés au ministre par le CST concernant la protection de la vie privée sont désormais plus détaillés, par exemple, concernant les « communications canadiennes » (voir la définition à la page 33) et l'information communiquée aux alliés ou reçue d'eux.
- Le CST a renforcé sa politique afin de faire en sorte que les gestionnaires du CST surveillent activement les activités des employés se rapportant à la conformité et à la protection de la vie privée, et que les employés aient une formation adéquate concernant les exigences en matière de conformité et de protection de la vie privée.
- Une autre histoire de réussite montre l'importance d'enchâsser dans la loi la collaboration et la coopération des organismes d'examen, étant donné que les organismes voués à la sécurité et au renseignement travaillent déjà ensemble. Dans un examen portant sur l'assistance opérationnelle du CST au SCRS sous le régime de certains mandats de la Cour fédérale autorisant la collecte de renseignements sur des Canadiens à l'extérieur du Canada, le commissaire a recommandé que le CST demande au SCRS d'expliquer davantage à la Cour la nature de l'assistance que le CST a fournie

avec la participation de ses alliés. Lors du dépôt du rapport annuel public du commissaire, la Cour a été saisie de cette question et elle a statué qu'elle n'était pas compétente pour approuver l'assistance du CST au SCRS. À son avis, la non-divulgaration de certains renseignements à la Cour était en fait le résultat d'une décision délibérée de la maintenir dans l'ignorance. À cette époque, le SCRS a suspendu ses demandes d'assistance au CST impliquant les alliés.

POINTS SAILLANTS DES RAPPORTS PRÉSENTÉS AU MINISTRE EN 2015-2016

1. Examen du soutien apporté par le CST au Service canadien du renseignement de sécurité en vertu de la partie c) de son mandat concernant un certain type de rapport mettant en cause des Canadiens

Contexte

Les accords de coopération qui existent entre les partenaires de la collectivité des cinq (ou alliés) comportent un engagement à respecter la vie privée des citoyens de chaque pays et à agir d'une manière cohérente relativement aux politiques de chaque nation en matière de respect de la vie privée. Néanmoins, on sait pertinemment que chacun de ces partenaires est un organisme d'un pays souverain qui peut, dans des circonstances exceptionnelles, déroger aux accords s'il y va de l'intérêt national. Dans ces cas exceptionnels, l'un des partenaires du CST peut acquérir de l'information sur un Canadien ou une personne au Canada et faire rapport sur cette information. Un partenaire pourrait faire rapport sur des Canadiens qui se trouvent à l'extérieur du Canada et dont on sait qu'ils sont engagés dans des activités terroristes ou y apportent un soutien. Par exemple, ce rapport pourrait concerner un Canadien connu en tant que « combattant étranger » qui pourrait envisager de rentrer au Canada ou de s'attaquer à des Canadiens. Lorsqu'un partenaire entreprend une activité se rapportant à un Canadien, il peut acquérir des renseignements qui, en plus de répondre à ses propres exigences en matière de sécurité nationale, se rapportent à la sécurité du Canada. En pareil cas, il peut juger utile de les communiquer au Service canadien du

renseignement de sécurité (SCRS), à l'appui de son mandat qui consiste à enquêter sur les menaces pesant sur la sécurité du pays et à en prévenir le gouvernement.

Combattant étranger

On appelle combattant étranger une personne qui quitte son pays d'origine pour se joindre à un mouvement insurrectionnel à l'étranger et dont la principale motivation est idéologique ou religieuse; par exemple les hommes et les femmes ayant quitté le Canada pour se joindre au groupe terroriste qui se fait appeler État islamique.

Interdiction pour le CST de cibler des Canadiens

En vertu de son *mandat de collecte de renseignements électromagnétiques étrangers*, le CST se voit interdire par la loi, dans le cadre de ses activités de collecte de renseignements électromagnétiques étrangers, de cibler des Canadiens – où qu'ils se trouvent dans le monde – ou toute personne au Canada. Le CST ne peut demander à d'autres d'entreprendre en son nom des activités que lui-même n'est pas autorisé à mener. Par exemple, il serait illégal que celui-ci demande à un partenaire de viser un Canadien et le CST ne devrait pas recevoir en toute connaissance de cause un rapport découlant d'une activité ciblant un Canadien. Toutefois, cette interdiction ne s'applique pas aux activités menées par le CST en vertu de la partie de son mandat qui consiste à *aider les organismes fédéraux chargés de l'application de la loi et de la sécurité*. Lorsqu'il agit dans ce cadre, le CST est plutôt assujéti aux limites imposées par la loi à l'organisme qui a demandé son aide. Le CST est donc habilité, par exemple, à appuyer le SCRS dans l'accomplissement de son mandat qui consiste à faire enquête sur les menaces pour la sécurité du Canada. En pareil cas, si la *Loi sur le Service Canadien du renseignement de sécurité* permet au SCRS de recevoir de l'information sur un Canadien, le CST pourrait en toute légitimité l'aider à recevoir cette information.

Avant février 2015, la méthode utilisée pour fournir ce type de rapport au SCRS était manuelle, sans participation du CST. Afin de combattre la menace terroriste en constante évolution et de faire face à l'augmentation du nombre de combattants étrangers, le SCRS a eu besoin d'un mécanisme plus opportun pour échanger l'information de manière sécuritaire. À cette fin, le SCRS a demandé l'assistance du CST en vertu de la partie c) du mandat de ce

dernier (alinéa 273.64[1]2(c) de la *Loi sur la défense nationale* [LDN]) pour établir un mécanisme lui permettant de recevoir et de traiter ces rapports, par l'intermédiaire des canaux établis du CST.

Cet examen avait pour objectifs : d'acquérir une connaissance précise de l'assistance fournie par le CST au SCRS en ce qui a trait à ces rapports et de documenter cette aide; d'évaluer si les activités sont conformes à la loi et aux instructions ministérielles; et de déterminer la mesure dans laquelle le CST a protégé la vie privée des Canadiens dans l'exercice de ces activités.

Le commissaire a effectué un examen de tous les rapports que le CST a transmis au SCRS du 5 février au 15 mai 2015.

Constatations

Lorsqu'il entreprend des activités en vertu de la partie c) de son mandat, le CST doit respecter les limites imposées par la loi à l'organisme ayant présenté une demande d'assistance (paragraphe 273.64[3] de la LDN). Dans le cas des activités examinées, l'assistance fournie par le CST au SCRS était donc régie par les restrictions prévues par la *Loi sur le Service Canadien du renseignement de sécurité*. En vertu de l'article 12 de la Loi, le SCRS, dans le cadre de son mandat, « recueille, au moyen d'enquêtes ou autrement, dans la mesure strictement nécessaire, et analyse et conserve les informations et renseignements sur les activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada; il en fait rapport au gouvernement du Canada et le conseille à cet égard ».

En outre, toutes les activités du CST, en tant qu'institution gouvernementale, sont assujetties à la *Charte canadienne des droits et libertés*, qui protège les attentes raisonnables d'une personne relativement à la vie privée, et aux instructions ministérielles qui exigent que le CST — lorsqu'il apporte son assistance — gère l'information d'une manière conforme aux principes énoncés dans la *Loi sur la protection des renseignements personnels*.

Le commissaire estime que les activités du CST visant à transmettre ces rapports au SCRS ont été conduites conformément à la loi et aux instructions ministérielles se rapportant à la protection de la vie privée des Canadiens.

Plus précisément, le commissaire a pu établir que :

- les activités consistaient en une assistance technique et opérationnelle qui est autorisée en vertu de la partie c) du mandat du CST;
- il était légitime que le CST approuve la demande d'assistance du SCRS pour élaborer un mécanisme de transmission de ces rapports, puisque le SCRS est autorisé, en vertu de son mandat, à recevoir des rapports ayant trait aux menaces qui pèsent sur la sécurité du pays, comme le prévoit l'article 2 de la Loi sur le SCRS; et
- tous les rapports transmis au SCRS au cours de la période visée par l'examen contenaient de l'information se rapportant à une menace pour la sécurité du pays; le SCRS disposait à la fois du pouvoir et de la justification opérationnelle requis pour obtenir l'information relative à un Canadien.

Le CST a en place des procédures qui fournissent à ses employés des instructions suffisantes pour qu'ils assurent la protection de la vie privée des Canadiens dans le cadre de leurs activités. Un plan opérationnel définit clairement les rôles et responsabilités et restreint l'accès aux rapports à un nombre très limité d'employés. Les gestionnaires du CST ont surveillé systématiquement et étroitement la conduite des activités pour s'assurer que la transmission de ces rapports était conforme aux autorisations pertinentes. Le bureau a vérifié les registres mensuels tenus par la direction du CST où est indiqué le nom des employés ayant examiné ces rapports et il a été satisfait des raisons inscrites justifiant l'accès.

Enfin, le commissaire a noté que la demande du SCRS englobait les menaces envers la sécurité du Canada, au sens de l'article 2 de la Loi sur le SCRS. En outre, même si le CST, en qualité d'agent du SCRS, a fourni une orientation à ses partenaires, il leur a laissé le soin de déterminer en quoi consistent les renseignements se rapportant à une menace pour la sécurité du Canada.

Conclusions et recommandation

Comme les rapports transmis au SCRS au cours de la période visée par l'examen renfermaient de l'information au sujet de Canadiens, ces activités comportent un risque pour la vie privée des Canadiens. Par conséquent, **le commissaire a recommandé** que le CST tienne le ministre informé, sur une base annuelle, en vertu de la partie c) de son mandat, de ses activités de transmission de ce type de rapport au SCRS.

Le bureau du commissaire continuera d'examiner cette assistance au SCRS pour vérifier que le CST se conforme à la loi, c'est-à-dire que l'information au sujet de Canadiens que le CST obtient et transmet au SCRS cadre avec le pouvoir habilitant et la justification opérationnelle du SCRS et que le CST prend des mesures suffisantes pour protéger la vie privée des Canadiens dans la conduite de ses activités.

Après l'achèvement de l'examen, des fonctionnaires du bureau ont rencontré leurs homologues du Comité de surveillance des activités de renseignement de sécurité (CSARS) — lequel amorçait un examen des activités du SCRS sur ce sujet — pour décrire la méthode d'examen employée, fournir un résumé des constatations et définir les domaines d'enquête se rapportant au SCRS qui ne relevaient pas du mandat du commissaire, mais que le CSARS pouvait surveiller de près s'il l'estimait approprié.

2. Examen des activités du CST relatives aux métadonnées liées aux renseignements électromagnétiques étrangers (volet 2)

Contexte

Il y a déjà un certain temps que le bureau du commissaire s'intéresse de très près aux activités du CST relatives aux métadonnées. En fait, presque chaque examen porte sur les métadonnées, qui sont fondamentales tant pour les activités du CST relatives aux renseignements électromagnétiques étrangers que pour les activités de cyberdéfense. Les métadonnées aident le CST à comprendre l'infrastructure mondiale d'information. Le CST utilise également les métadonnées pour cibler des entités étrangères situées à l'extérieur du pays et atténuer le risque d'interception de communications privées de Canadiens. Un premier examen axé sur les métadonnées a été effectué en 2006, et nous avons commencé à planifier un vaste examen des métadonnées en 2012. Le premier volet de cet examen, qui a été résumé dans le rapport annuel de l'an dernier, comportait des renseignements détaillés sur les autorisations applicables aux métadonnées liées aux renseignements électromagnétiques étrangers et sur certaines activités se rapportant à l'utilisation et à la divulgation des métadonnées. Le second volet de l'examen portait sur des activités particulières relatives aux métadonnées liées aux renseignements électromagnétiques étrangers que l'on avait mises de côté dans le cadre du premier volet de l'examen de façon à

explorer plus en profondeur les incidents imputables au fait que le CST n'avait pas minimisé l'information sur l'identité de Canadiens dans certaines métadonnées partagées avec ses alliés. La minimisation est le procédé permettant de rendre non identifiable l'information sur l'identité de Canadiens contenue dans des métadonnées avant de la communiquer.

Métadonnées

En vertu de l'alinéa 273.64(1)a) de la LDN, le CST est habilité à acquérir et à utiliser l'information provenant de l'infrastructure mondiale d'information dans le but de fournir des renseignements étrangers, y compris des métadonnées. Une directive ministérielle de 2011 fournit des instructions supplémentaires et impose des limites aux activités du CST se rapportant aux métadonnées. Le CST décrit les métadonnées comme le contexte d'une communication, mais non le contenu. On entend par métadonnées l'information associée à une communication qui est utilisée pour identifier, décrire, gérer ou acheminer la 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.

Cet examen avait pour objectifs : de passer en revue des activités particulières du CST relatives aux métadonnées liées aux renseignements électromagnétiques; d'évaluer si les activités étaient conformes à la loi, aux instructions ministérielles ainsi qu'aux politiques et procédures opérationnelles du CST; d'évaluer la mesure dans laquelle le CST a protégé la vie privée des Canadiens dans l'exercice des activités; d'assurer le suivi des constatations antérieures des commissaires; et de mettre en évidence tout domaine requérant un examen approfondi par la suite.

Constatations

Le bureau a examiné trois activités distinctes relatives aux métadonnées.

Premièrement, il s'est penché sur certaines activités d'analyse des métadonnées entreprises à des fins de collecte de renseignements étrangers. Même s'il a constaté des progrès encourageants, c'est-à-dire que le CST a mis à jour sa politique opérationnelle pertinente, le commissaire estime que les lignes directrices sur une activité précise touchant les métadonnées comportant de l'information sur l'identité de Canadiens demeurent vagues et doivent être clarifiées.

Le bureau du commissaire continuera d'examiner la conduite de ces activités dans le cadre de ses futurs examens des activités du CST.

En ce qui concerne ces activités, nous avons examiné en profondeur un échantillon d'activités comprenant de l'information sur l'identité de Canadiens entreprises sur une période d'un an. Même si un petit nombre d'activités ont soulevé des interrogations concernant les pouvoirs habilitants du CST et que le commissaire a relevé des incohérences dans les pratiques de tenue de dossiers et de documentation du CST, il a constaté que les activités étaient autorisées et menées de façon générale d'une manière conforme aux instructions ministérielles et aux politiques du CST. Bien qu'il ne soit pas entièrement satisfait de l'approche adoptée par le CST, le commissaire n'a pas formulé de recommandations pour s'attaquer aux irrégularités et aux problèmes mis au jour, car après la période visée par l'examen, le CST a suspendu pour une période indéterminée ces activités particulières d'analyse des métadonnées par suite de l'évolution de la jurisprudence (*Loi sur le Service Canadien du renseignement de sécurité [Re]*, 2012 CF 1437, se rapportant à l'application de « vise »). Il est encourageant de voir que le CST a modifié ses pratiques en fonction de la jurisprudence connexe.

Avant de prendre la décision de suspendre ces activités, le CST n'avait pas respecté son engagement de donner suite à la recommandation du commissaire formulée dans un examen des activités du Bureau de l'anti-terrorisme du CST effectué en février 2014 et lui demandant de modifier la politique pertinente pour tenir compte des pratiques actuelles et de renforcer la tenue des dossiers. Toutefois, on peut expliquer la situation par le court laps de temps entre l'examen du Bureau de l'anti-terrorisme et la suspension des activités. Tant que la suspension demeure en vigueur, le commissaire ne s'attend pas à ce que le CST mette en œuvre la recommandation.

Deuxièmement, le commissaire a fait le suivi d'une autre recommandation formulée dans le cadre de l'examen du Bureau de l'anti-terrorisme du CST et demandant que le CST émette des instructions écrites pour officialiser et renforcer les pratiques existantes adoptées pour donner suite aux éventuelles préoccupations quant au respect de la vie privée par les alliés. Le commissaire accepte les réponses du CST aux problèmes mis au jour dans l'examen du Bureau de l'anti-terrorisme et le CST a émis des lignes directrices à l'intention des employés opérationnels pour régler les situations où un risque pourrait peser sur la vie privée de Canadiens.

Troisièmement, le bureau a examiné certaines activités d'analyse des réseaux mettant en cause des métadonnées qui aident le CST, par exemple, à identifier les auteurs de menace étrangers, tels que des groupes terroristes ou des auteurs de cybermenace. Le commissaire n'avait pas de questions concernant les autorisations ou les politiques applicables aux activités et il estime que cette analyse demeure essentielle pour l'exécution du mandat du CST en matière de renseignements électromagnétiques étrangers.

Conclusion

Le vaste examen portant sur l'utilisation par le CST des métadonnées dans un contexte de renseignements électromagnétiques étrangers est maintenant achevé. Dans ce volet de l'examen, le commissaire n'a trouvé aucune preuve de non-conformité et il n'a pas formulé de recommandations. Le bureau du commissaire continuera d'examiner l'utilisation et la divulgation de métadonnées par le CST, qui sont au cœur de toutes les activités de collecte de renseignements électromagnétiques étrangers. Un troisième rapport, qui sera achevé au cours de l'exercice à venir, met l'accent sur l'utilisation des métadonnées par le CST dans un contexte de cyberdéfense.

Mise à jour concernant la non-minimisation d'informations sur l'identité de Canadiens avant leur communication aux alliés

En janvier 2016, le commissaire a décrit l'enquête sur le défaut de minimisation des métadonnées du CST qui l'ont conduit, pour la première fois de l'histoire du bureau, à écrire au ministre et au procureur général du Canada pour les informer qu'il avait découvert que le CST ne se conformait pas à la loi, en particulier aux articles 273.64 et 273.66 de la LDN et, en conséquence, contrevenait à l'article 8 de la *Loi sur la protection des renseignements personnels*. Il a indiqué que même s'il pensait que les actions du CST n'étaient pas délibérées, le CST n'avait toutefois pas agi avec une diligence raisonnable lorsqu'il ne s'était pas assuré que l'information sur l'identité de Canadiens était bien minimisée avant de la communiquer à ses alliés. Par la suite, le ministre et le procureur général ont accepté les recommandations du commissaire se rapportant aux métadonnées, y compris celle demandant la modification de la LDN pour donner un pouvoir exprès et un cadre clair aux activités du CST relatives aux métadonnées.

Le commissaire a discuté de ses constatations avec le commissaire à la protection de la vie privée du Canada, Daniel Therrien, qui a la responsabilité de superviser la *Loi sur la protection des renseignements personnels*. Les hauts fonctionnaires du bureau étaient présents lorsque le CST a expliqué les activités aux représentants de M. Therrien et ces fonctionnaires ont été en mesure de répondre aux questions du commissaire à la protection de la vie privée et du commissariat. Au fur et à mesure que des questions d'intérêt commun se présentent, ce genre de collaboration avec le Commissariat à la protection à la vie privée devrait se poursuivre.

Comme il l'avait fait au cours de l'enquête, le CST a continué d'agir de manière franche et transparente. Non seulement il a suspendu de façon proactive le partage des métadonnées avec ses alliés après la découverte des défauts mais, pour la première fois au cours de ses 69 années d'existence, le CST a organisé une séance d'information technique détaillée à l'intention des médias et mis de l'information sur son site Web concernant ses activités relatives aux métadonnées.

Au moment de la rédaction du présent rapport, le CST n'avait pas encore repris le partage de ce type de métadonnées avec ses alliés. Le ministre et la chef du CST ont fourni des assurances indiquant que le CST ne divulguerait pas ces métadonnées à ses alliés tant que des systèmes ne seraient pas en place pour protéger efficacement la vie privée des Canadiens. Le commissaire s'attend à ce que le CST l'informe avant la reprise de ces activités et le bureau effectuera un examen de suivi pour déterminer si le CST se conforme à la loi et applique efficacement des mesures satisfaisantes de protection de la vie privée.

Le bureau surveillera également les efforts du CST pour mettre en œuvre les deux recommandations formulées dans le premier rapport sur les métadonnées et lui demandant : de mettre à jour la directive ministérielle en vue de fournir des instructions claires concernant la collecte, l'utilisation et la divulgation de métadonnées dans un contexte de renseignements électromagnétiques étrangers; et d'utiliser son système de registre centralisé pour consigner les décisions et les mesures prises concernant les nouveaux systèmes de collecte ou ceux qui ont été mis à jour, de même que les décisions et les mesures prises concernant la minimisation des métadonnées.

3. Examen d'une méthode particulière de collecte de renseignements électromagnétiques étrangers adoptée par le CST sous le régime d'une autorisation ministérielle

Contexte

Cette année, le bureau a achevé un examen des activités du CST se rapportant à une méthode particulière de collecte de renseignements électromagnétiques étrangers sous le régime d'une autorisation ministérielle. Cette méthode fournit de l'information sur : les cibles étrangères relatives aux affaires internationales, à la défense et à la sécurité; les métadonnées à l'appui de la découverte de cibles et de l'analyse des réseaux; et les cybermenaces. Une directive ministérielle de 2004 définit des exigences précises — notamment un cadre d'approbation et les attentes en matière de sécurité et de gestion du risque des activités opérationnelles — applicables à l'échantillon qui a été choisi pour examen. Après la période visée par l'examen, le ministre a émis une directive à jour sur ces activités.

L'examen avait pour objectifs d'évaluer si les activités étaient conformes à la loi, aux instructions ministérielles ainsi qu'aux politiques et procédures opérationnelles du CST, et la mesure dans laquelle le CST a protégé la vie privée des Canadiens dans le cadre des activités en question.

Comparativement aux autres méthodes de collecte de renseignements électromagnétiques étrangers, ces activités donnent lieu à l'interception non intentionnelle d'un nombre plus élevé de communications privées identifiées par le CST. Un des buts spécifiques de l'examen était de mieux comprendre les conséquences possibles de ces activités sur la vie privée des Canadiens.

En 2008, le commissaire Gonthier avait mené un examen exhaustif des activités. Une constatation importante était que le CST n'avait pas agi conformément à toutes les exigences administratives de la directive ministérielle se rapportant à la sécurité et à la gestion du risque. En conséquence, le commissaire recommandait que le CST harmonise ses pratiques avec les exigences administratives énoncées dans la directive ministérielle. Il avait également mis au jour des lacunes se rapportant à des dossiers incomplets et insuffisants. Cet examen faisait le point sur les mesures prises par le CST pour se conformer aux recommandations antérieures et tenir compte des constatations négatives.

Constatations et recommandation

Pour plusieurs raisons — y compris les ressources limitées du bureau et du CST, le roulement de personnel et un incident imprévu hautement prioritaire —, cet examen, qui s'est poursuivi pendant un certain temps, n'a été achevé que lors de cet exercice. En outre, les réponses du CST aux questions du bureau se rapportant à cet examen particulier ont souvent été retardées, incomplètes ou manquaient de cohérence, exigeant de la part des fonctionnaires un suivi régulier. Toutefois, dans ce contexte, d'après l'information examinée et les entretiens qu'il a tenus, le commissaire n'a pas trouvé de preuve de non-conformité à la loi.

Le CST a apporté des améliorations depuis l'examen de 2008. Plusieurs questions demeurent toutefois en attente, et le commissaire a présenté des constatations négatives qui sont similaires à celles de son prédécesseur. Contrairement à ce que prescrivait la directive ministérielle, le CST ne dispose pas de plan à jour, par exemple, pour prévenir et atténuer les répercussions négatives éventuelles d'une divulgation non autorisée. Divers documents sont demeurés sous la forme d'ébauche pendant des années et ne renferment pas suffisamment d'information. Le commissaire est préoccupé par le fait que certains documents importants se rapportant à la sécurité et à la gestion du risque demeurent incomplets. Par conséquent, comme son prédécesseur, **le commissaire a recommandé** que le CST harmonise ses pratiques avec les exigences administratives énoncées dans la directive ministérielle.

Le commissaire a découvert plus d'un cas où, en raison d'un manque de clarté et d'explications des termes clés employés dans le cadre d'approbation de la directive ministérielle, on aurait pu faire valoir que le CST aurait dû chercher à obtenir une approbation expresse avant de mener une activité. La directive ministérielle mise à jour renferme toutefois un nouveau cadre d'approbation et des instructions supplémentaires que le bureau du commissaire évaluera au cours de l'examen de suivi qu'il a prévu.

En outre, le bureau a cherché à obtenir des statistiques concernant le nombre de communications interceptées par le CST pour le compte de ses alliés ou envoyées à ses alliés en utilisant cette méthode de collecte particulière. Certes, le CST a fourni certains renseignements, mais ses systèmes actuels n'ont pas suivi et enregistré automatiquement cette information et il était difficile et fastidieux pour le CST de donner des réponses. Lors d'un examen des autorisations ministérielles relatives

aux renseignements électromagnétiques étrangers mené en 2013, le CST a indiqué qu'il travaillait à une solution technique pour retracer plus facilement le nombre de communications qu'il avait interceptées et envoyées à ses alliés. Dans un examen subséquent, le bureau du commissaire se penchera sur les efforts déployés par le CST pour mettre en œuvre la solution. En enregistrant et en communiquant régulièrement au ministre un plus large éventail de renseignements statistiques sur le partage d'information avec les alliés, on l'appuiera dans sa reddition de comptes pour le CST.

Conclusion

Compte tenu de la portée et de la nature de cette méthode de collecte de renseignements électromagnétiques étrangers, de la directive ministérielle récente, des constatations négatives continues et du temps qui s'est écoulé depuis le début de cet examen, au moment de la rédaction du présent rapport, le commissaire avait déjà entrepris un autre examen mettant tout particulièrement l'accent sur les activités de ciblage du CST, c'est-à-dire le processus et les pratiques qui conduisent le CST à déterminer que des entités d'intérêt pour le renseignement étranger sont des entités étrangères situées à l'extérieur du Canada. Le commissaire surveillera le délai de réponse du CST.

4. Examen combiné annuel des autorisations ministérielles du CST relatives à la collecte de renseignements électromagnétiques étrangers et à l'interception de communications privées

Contexte

Il s'agit du sixième examen combiné annuel consécutif des autorisations ministérielles relatives à la collecte de renseignements électromagnétiques étrangers. C'est l'une des façons permettant aux commissaires de s'acquitter de leur obligation, en vertu de la LDN, d'examiner les activités menées sous le régime d'une autorisation ministérielle pour s'assurer qu'elles sont dûment autorisées et de faire rapport annuellement de cet examen au ministre.

L'examen a porté sur trois autorisations ministérielles en vigueur du 1^{er} décembre 2014 au 30 juin 2015 et se rapportant à trois méthodes de collecte distinctes. Il s'agissait d'analyser les documents d'autorisation eux-mêmes et les activités décrites dans les autorisations comparativement aux années précédentes pour relever tout changement important touchant chaque méthode de collecte et le programme de collecte de renseignements électromagnétiques étrangers dans son ensemble. Parmi les objectifs de l'examen, mentionnons l'évaluation des répercussions de tout changement sur les risques relatifs à la conformité et à la protection de la vie privée et, en conséquence, la mise en évidence de toute question nécessitant un examen de suivi.

Selon la politique du CST, lorsqu'un analyste ayant directement pour fonction de produire des rapports sur les renseignements étrangers découvre qu'une communication interceptée est une communication privée, une communication émanant d'un Canadien situé à l'extérieur du Canada ou une communication renfermant de l'information sur l'identité de Canadiens et que cette communication n'est pas essentielle aux affaires internationales, à la défense ou à la sécurité, il doit la détruire dès qu'il a relevé ces caractéristiques. Les communications jugées essentielles pour les affaires internationales, la défense ou la sécurité, en revanche, peuvent être utilisées dans un rapport du CST ou conservées.

Pour vérifier la conformité à la loi et déterminer la mesure dans laquelle le CST a protégé la vie privée des Canadiens, le commissaire a examiné ce qu'il était advenu des 13 communications privées identifiées tirées

de renseignements électromagnétiques étrangers que le CST avait utilisées ou conservées à la fin de la période de validité de l'autorisation ministérielle de 2013–2014 et des 342 communications privées que le CST avait utilisées ou conservées à la fin de la période de validité de l'autorisation ministérielle de 2014–2015. L'examen comportait deux vérifications ponctuelles des 262 communications privées utilisées ou conservées par le CST au cours des périodes allant du 1^{er} mars au 30 avril 2015 et du 1^{er} septembre au 31 octobre 2015. Le CST n'avait pas été prévenu que le bureau allait effectuer des vérifications ponctuelles.

Autorisations ministérielles

Les autorisations ministérielles permettent au CST de passer outre l'interdiction d'intercepter des communications privées énoncée à la partie VI du *Code criminel*. Il s'agit d'un document écrit en vertu duquel le ministre de la Défense nationale autorise le CST à entreprendre une activité ou une catégorie d'activités comportant un risque d'interception non intentionnelle de communications privées. Les autorisations ne peuvent demeurer en vigueur pendant une période de plus d'un an. Pour en apprendre davantage sur les autorisations et les limites imposées aux activités du CST, veuillez consulter le site Web du bureau à : www.ocsec-bccst.gc.ca.

Constatations

Le commissaire a constaté que les autorisations ministérielles de 2014–2015 relatives aux renseignements électromagnétiques étrangers remplissaient les conditions d'autorisation définies dans la LDN, à savoir :

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

Le commissaire n'a pas observé de changements importants dans les autorisations ministérielles de 2014–2015 ni dans les mémoires de demande connexes adressés au ministre.

On observe une amélioration de la reddition de comptes concernant les communications entre un avocat et son client, protégées par le secret professionnel, puisque des mesures sont prévues pour informer le ministre des cas où des communications interceptées non intentionnellement entre un avocat et son client et renfermant des renseignements étrangers ont été conservées, utilisées ou divulguées. Toutefois, il n'y a pas une cohérence parfaite entre la politique opérationnelle du CST et la nouvelle façon de procéder, et des révisions s'imposent. Au cours de la période visée par l'examen, aucune communication entre un avocat et son client n'a été utilisée ou conservée par le CST. En fait, le CST n'a pas utilisé ni conservé de communications de ce genre au cours des cinq dernières années. Le bureau continuera de surveiller et d'examiner la conservation ou l'utilisation par le CST de communications privées, y compris d'éventuelles communications entre un avocat et son client.

Il est encourageant de voir que des précisions ont été ajoutées dans les autorisations ministérielles et les mémoires concernant ce qu'on entend par communication privée « essentielle » ainsi que pour clarifier les situations dans lesquelles le CST pourrait intercepter de manière non intentionnelle une communication privée.

Le CST a mis en œuvre une recommandation du commissaire résumée dans le rapport annuel 2013–2014 en modifiant sa politique opérationnelle pour préciser qui est la personne chargée d'approuver certaines activités de collecte de renseignements électromagnétiques étrangers. Le CST travaille également à la mise à jour d'une politique applicable à certaines autres activités que le bureau examinera lorsqu'elle sera publiée.

Le CST a apporté des changements à la technologie qu'il utilise pour certaines de ses activités de collecte de renseignements électromagnétiques étrangers qui continuent d'être contestées dans la foulée des révélations non autorisées faites par Edward Snowden en 2013. Les révélations ont abouti à l'utilisation croissante du cryptage et d'autres contre-mesures par les cibles du renseignement étranger qui espèrent échapper ainsi aux efforts de collecte du CST et de ses alliés.

Protection de la vie privée des Canadiens

Le CST se voit interdire, dans le cadre de ses activités de collecte de renseignements électromagnétiques étrangers et de cyberdéfense, de cibler des Canadiens – où qu'ils se trouvent dans le monde – ou toute personne au Canada. Le fait que le travail du CST vise des cibles étrangères signifie que, à la différence des autres organismes de renseignement et de sécurité du Canada, le CST a des interactions limitées avec les Canadiens. Lorsque le CST acquiert fortuitement de l'information se rapportant à un Canadien, il est tenu par la loi de prendre des mesures pour protéger la vie privée de ce Canadien. Dans le cadre de son examen des activités du CST, le commissaire vérifie entre autres si le CST ne cible pas des Canadiens et s'il applique efficacement des mesures satisfaisantes pour protéger la vie privée des Canadiens dans toutes les activités opérationnelles qu'il entreprend.

En ce qui concerne les communications privées, d'après les renseignements examinés et les entretiens qu'il a menés, le commissaire estime que :

- toutes les communications privées identifiées par le CST ont été interceptées de manière non intentionnelle et traitées conformément aux politiques et procédures du CST — rien ne portait à croire que les communications privées qui avaient été identifiées comme telles par le CST au cours de cette période avaient été interceptées intentionnellement, ce qui aurait été illégal;
- toutes les communications privées utilisées et conservées par le CST étaient essentielles aux affaires internationales, à la défense ou à la sécurité, comme l'exige la LDN; et
- les communications privées qui n'étaient pas essentielles ont été détruites. Le CST n'a pas conservé de communications privées au-delà des périodes de conservation et de destruction prescrites par sa politique.

Le commissaire a observé que, au cours de la période visée par l'examen, le nombre de communications privées identifiées par le CST avait augmenté comparativement aux périodes de validité des autorisations ministérielles précédentes. Il s'agit d'une conséquence des caractéristiques techniques de technologies de communication

particulières et de la manière dont on dénombre les communications privées.

Il est encourageant de voir, comme le commissaire l'avait recommandé, le rapport de fin d'année sur les autorisations ministérielles présenté au ministre par la chef pour 2014–2015 renfermait davantage d'information détaillée concernant le nombre de communications privées conservées tout au long de la période visée, y compris une explication de leur augmentation au cours de la période allant de mars à avril 2015.

Conclusion

Le CST prend des mesures pour mettre en œuvre les recommandations des examens précédents se rapportant aux autorisations ministérielles et aux communications privées. L'examen dont il est question dans le présent rapport ne donne lieu à aucune recommandation. Le bureau du commissaire continuera d'effectuer des examens annuels pour vérifier que les autorisations ministérielles sont conformes et de procéder à des vérifications ponctuelles des « communications canadiennes » acquises et identifiées par le CST pour vérifier que le CST ne cible pas des Canadiens et protège leur vie privée. Au cours du prochain exercice, en vue d'apporter des garanties supplémentaires, les vérifications ponctuelles seront élargies pour englober un échantillon d'autres « communications canadiennes » acquises par le CST, y compris celles émanant d'alliés.

« Communication canadienne »

On entend par Canadien un citoyen canadien, un résident permanent au sens du paragraphe 2(1) de la *Loi sur l'immigration et la protection des réfugiés* ou une personne morale constituée ou prorogée sous le régime d'une loi fédérale ou provinciale.

Une « communication canadienne » désigne une communication entre deux interlocuteurs dont l'un se trouve physiquement au Canada (c'est-à-dire une communication privée) ou est un Canadien qui se trouve physiquement à l'extérieur du Canada.

5. Examen annuel des activités de cyberdéfense du CST menées sous le régime d'une autorisation ministérielle

Contexte

Pour détecter les cybermenaces sophistiquées — y compris celles émanant d'un État étranger, d'auteurs de menaces criminelles ou terroristes —, et s'en protéger, le CST peut, sur réception d'une demande écrite provenant d'une institution du gouvernement du Canada, mener des activités de cyberdéfense et mettre en place des mesures pour recueillir et analyser les données tirées de systèmes ou de réseaux informatiques d'un client. Du fait que les activités de cyberdéfense du CST comportent un risque d'interception de communications privées, il est tenu de les mener sous le régime d'une autorisation ministérielle.

Protection de la vie privée des Canadiens

Dans le cadre des activités de cyberdéfense, les données interceptées par le CST, y compris les communications privées, ne peuvent être utilisées ou conservées que si elles sont pertinentes et essentielles pour identifier, isoler ou prévenir les activités dommageables visant les systèmes ou les réseaux informatiques du gouvernement du Canada.

L'examen annuel portait sur deux autorisations ministérielles de cyberdéfense en vigueur du 1^{er} décembre 2013 au 30 novembre 2014 et du 1^{er} décembre 2014 au 30 juin 2015.

Il comprenait l'étude des documents relatifs aux autorisations ministérielles de cyberdéfense et des activités qu'ils décrivent, le but étant de s'assurer que les conditions applicables à l'autorisation précisées par la LDN avaient été respectées. Nous avons comparé les autorisations et les activités avec celles des années antérieures, pour repérer les changements importants. Un des objectifs de l'examen était d'évaluer l'incidence de tout changement sur les risques relatifs à la conformité et à la vie privée et, en conséquence, de mettre en évidence toute question nécessitant un examen de suivi.

Pour vérifier la conformité à la loi et évaluer la mesure dans laquelle le CST a protégé la vie privée des Canadiens, le bureau a examiné un échantillon de données et de communications identifiées comme privées

qui ont été interceptées en vertu des autorisations ministérielles, et utilisées ou conservées du fait qu'elles étaient essentielles pour identifier, isoler ou prévenir les activités dommageables visant les systèmes ou les réseaux informatiques du gouvernement du Canada.

Le bureau a sélectionné et examiné un échantillon de données interceptées se rapportant à environ 20 pourcent du nombre total de cyberincidents recensés au cours de la période de validité des autorisations ministérielles de 2013–2014 et 2014–2015. Un incident cybernétique peut comporter un ou plusieurs cyberévénements et une ou plusieurs communications privées. Environ 70 pourcent de l'échantillon renfermait une ou plusieurs communications privées identifiées. Il n'est pas possible de révéler le nombre de communications privées utilisées et conservées par le CST en lien avec les activités de cyberdéfense, car cela permettrait à l'adversaire d'évaluer les capacités du CST.

Le bureau a examiné :

- les cyberévénements qui ont été à l'origine des incidents;
- le maliciel, qui est le logiciel utilisé par les auteurs de la menace, par exemple pour essayer de voler l'information d'un système informatique ou de saboter le réseau;
- les rapports internes et externes du CST relatifs aux cybermenaces;
- les courriels;
- les notes des analystes; et
- les détails contenus dans les outils et les bases de données connexes, comme la justification de la conservation d'une communication privée particulière, et l'information sur l'auteur de la menace.

Un autre objectif était d'assurer le suivi des constatations et recommandations antérieures des commissaires, y compris celles découlant de l'examen approfondi de l'an dernier portant sur les activités de cyberdéfense menées au cours de la période de validité des autorisations ministérielles allant de 2009–2010 à 2011–2012.

Constatations et recommandation

Le commissaire considère que les autorisations ministérielles de cyberdéfense visant les périodes de 2013–2014 et 2014–2015 remplissent les conditions d'autorisation établies dans la LDN, à savoir que :

- l'interception était nécessaire pour identifier, isoler ou prévenir les activités dommageables visant les systèmes ou les réseaux informatiques du gouvernement du Canada;
- les renseignements à obtenir ne pouvaient raisonnablement être obtenus d'une autre manière;
- le consentement des personnes dont les communications peuvent être interceptées ne pouvait raisonnablement être obtenu;
- des mesures satisfaisantes étaient en place pour faire en sorte que seuls les renseignements qui sont essentiels pour identifier, isoler ou prévenir les activités dommageables visant les systèmes ou les réseaux informatiques du gouvernement du Canada soient utilisés ou conservés; et
- des mesures satisfaisantes étaient en place pour protéger la vie privée des Canadiens en ce qui touche l'utilisation et la conservation de ces renseignements.

D'après l'information examinée et les entretiens qu'il a tenus, le commissaire n'a trouvé aucune preuve de non-conformité à la loi au sens où l'entend le ministère de la Justice du Canada. Le cadre de validation de la conformité du CST pour les activités de cyberdéfense — qui prévoit la tenue de registres de vérification étoffés et la surveillance de la conformité aux politiques et procédures opérationnelles — fournit la preuve que le CST s'est conformé aux obligations légales.

Il n'y avait aucun changement important dans les autorisations ministérielles et les mémoires de demande connexes adressés au ministre ou dans la conduite des activités de cyberdéfense qui aurait eu une incidence sur le risque pour la conformité ou la protection de la vie privée.

Les autorisations ministérielles de cyberdéfense renfermaient des changements similaires à ceux apportés aux autorisations de collecte de renseignements électromagnétiques étrangers en vue de renforcer la

reddition de comptes concernant les communications entre l’avocat et son client. La politique opérationnelle en matière de cyberdéfense devrait également être modifiée pour prendre en compte les nouvelles exigences.

Le commissaire a constaté un autre changement positif introduit en 2014–2015 par le CST, qui consiste à en aviser le ministre quand il accepte de mener des activités de cyberdéfense sous le régime d’une autorisation ministérielle à la demande d’une institution du gouvernement du Canada. Cela rationalisera l’assistance fournie aux clients par le CST et facilitera une réponse rapide aux cyberincidents (les autorisations de 2013–2014 et antérieures à cette date exigeaient que le CST informe le ministre avant de pouvoir accepter de mener ce genre d’activités).

Récemment, le CST a commencé à faire usage d’une nouvelle technologie défensive spécialisée pour détecter et atténuer la cyberactivité malveillante ou anormale visant les systèmes et réseaux clients du gouvernement du Canada. La technologie semblait généralement bien convenir aux activités de cyberdéfense actuelles du CST et ce dernier applique aux nouvelles activités les politiques et procédures opérationnelles en place, le cadre de validation de la conformité ainsi que des mesures de protection de la vie privée. Toutefois, puisqu’il s’agit d’une technologie déployée depuis peu, les nouvelles activités justifient une analyse minutieuse dans le cadre d’un examen exhaustif futur.

En ce qui concerne les communications privées, d’après l’information examinée et les entretiens tenus, le commissaire a pu établir que :

- toutes les communications privées identifiées par le CST avaient été interceptées de manière non intentionnelle et traitées conformément aux politiques et procédures du CST — rien ne portait à croire que le CST ait visé des Canadiens ou toute autre personne au Canada dans le cadre de ses activités de cyberdéfense;
- toutes les communications privées utilisées et conservées par le CST étaient essentielles pour identifier, isoler ou prévenir les activités dommageables visant les systèmes ou les réseaux informatiques du gouvernement du Canada, comme l’exige la LDN; et
- les communications privées qui n’étaient pas essentielles ont été détruites; le CST n’a pas conservé de communications privées au-delà des périodes de conservation et de destruction prescrites par sa politique.

Toutefois, on a observé que les analystes avaient recours à deux méthodes différentes pour marquer et dénombrer les communications privées de cyberdéfense. Par souci d'exactitude et de cohérence dans les rapports au ministre, **le commissaire a recommandé** que le CST émette des lignes directrices à ce sujet.

Toutes les communications privées de cyberdéfense utilisées ou conservées par le CST qui ont été examinées cette année ne renfermaient rien de plus que le maliciel ou l'activité anormale touchant les systèmes et les réseaux.

Comme c'était généralement le cas par le passé, dans les communications privées examinées, il n'y avait pas d'échange d'information personnelle ou d'autre information importante entre l'auteur de la cybermenace et un employé du gouvernement du Canada ou un autre Canadien. Le commissaire continue de mettre en doute la pratique du CST qui consiste à traiter tous les courriels interceptés non intentionnellement à destination ou en provenance du Canada et se rapportant à des activités de cyberdéfense comme des communications privées et se demande si cette pratique reflète avec exactitude le risque pour la vie privée et la façon dont ce risque est décrit au ministre. Le commissaire a noté que des progrès avaient été réalisés du fait que les rapports du CST présentés au ministre concernant les communications privées mettent désormais en lumière les différences importantes — y compris sur le plan des attentes relatives à la vie privée — entre les communications privées interceptées dans le cadre des activités de collecte de renseignements électromagnétiques étrangers et des activités de cyberdéfense. Il n'en demeure pas moins qu'à ses yeux, une communication ne renfermant rien de plus qu'un code malveillant 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 commissaire a observé une augmentation de la proportion d'incidents ne renfermant pas de communications privées. Selon le CST, cette augmentation est attribuable à une utilisation accrue de certaines techniques destinées à réduire le risque d'intercepter non intentionnellement des communications privées.

Il est encourageant de voir que le rapport de fin d'exercice sur les autorisations ministérielles, présenté au ministre pour 2014–2015 par le chef du CST, renfermait davantage d'information détaillée concernant le nombre de communications privées identifiées et acquises par le CST dans le cadre d'activités de cyberdéfense particulières.

Dans le rapport de l'an dernier, le commissaire avait indiqué que le CST pourrait améliorer certaines politiques et procédures se rapportant à la conservation de certaines communications privées. Toutefois, compte tenu des explications fournies dans le contexte de cet examen, la suggestion a été retirée; le commissaire ne s'attend à aucune intervention du CST à ce sujet.

Le CST prend des mesures pour donner suite aux constatations négatives et mettre en œuvre les recommandations antérieures, y compris :

- l'émission de nouvelles lignes directrices et de communications régulières à l'intention de la direction et des employés opérationnels sur les changements touchant la politique;
- la mise en place d'un nouveau cours obligatoire sur la politique pour aider les analystes à mieux comprendre ses exigences;
- l'amélioration de la tenue des dossiers grâce au déploiement prévu d'une nouvelle base de données pour la cyberdéfense; et
- l'adoption d'un marquage et d'un mode de consignation des communications privées plus détaillés et plus précis — notamment des explications plus complètes sur les raisons de la conservation d'une communication privée — ce qui a fourni au commissaire des preuves plus solides de la conformité et a facilité la conduite de l'examen.

Conclusion

Le commissaire a formulé une recommandation pour améliorer la politique se rapportant à la cohérence dans le marquage et le dénombrement des communications privées. Le bureau continuera d'effectuer des examens annuels des autorisations ministérielles de cyberdéfense et des communications privées pour vérifier que les activités sont conformes et que le CST ne cible pas des Canadiens et protège leur vie privée. Il surveillera les mesures prises par le CST pour régler les problèmes mis en évidence dans l'examen. Cette année, le commissaire achèvera une étude portant sur la coopération et le partage d'information entre les employés du CST chargés de la sécurité des TI et ceux des renseignements électromagnétiques étrangers pour contrer les cybermenaces, qui sera résumée dans le rapport annuel 2016–2017.

6. Examen annuel de la divulgation d'information sur l'identité de Canadiens, 2014-2015

Contexte

Il s'agit du septième examen annuel consécutif d'un échantillon d'information sur l'identité de Canadiens divulguée par le CST — qui inclut tout renseignement se rapportant uniquement à un Canadien et susceptible de permettre son identification. Le but de l'examen était de vérifier que le CST, dans ses divulgations d'information concernant l'identité de Canadiens, s'est conformé à la loi, aux instructions ministérielles ainsi qu'à ses politiques et procédures, tout en évaluant la mesure dans laquelle il a protégé la vie privée des Canadiens.

Dans le cadre de l'examen de cette année, le bureau du commissaire a sélectionné et examiné un échantillon d'environ 20 pourcent (225 demandes) des 1 126 demandes de divulgation d'information sur l'identité de Canadiens contenue dans les rapports du CST et adressées au CST par des clients du gouvernement du Canada. Les demandes ont été reçues entre le 1^{er} juillet 2014 et le 30 juin 2015. L'échantillon incluait toutes les institutions gouvernementales qui avaient présenté une demande au cours de cette période. Le bureau a aussi examiné les 111 demandes des alliés et les six demandes de divulgation à des entités n'appartenant pas à la collectivité des cinq; un client du gouvernement du Canada a fait cinq demandes et un allié a fait une demande de partage d'information précise sur l'identité de Canadiens avec des entités n'appartenant pas à la collectivité des cinq — qui a été refusée. Il est important de signaler que le nombre de demandes représente le nombre de cas où des institutions ou des partenaires ont présenté des demandes distinctes de divulgation d'information sur l'identité qui avait été supprimée des rapports, en fournissant dans chaque cas une justification opérationnelle particulière. Une demande peut concerner l'identité de plusieurs Canadiens et l'identité d'un Canadien peut être divulguée plusieurs fois à différents partenaires ou institutions. Différents types d'information sur l'identité de Canadiens peuvent renvoyer à différents niveaux de risque en ce qui a trait à la vie privée.

Information sur l'identité de Canadiens

L'information qui peut identifier un Canadien est généralement supprimée, c'est-à-dire remplacée par une mention générale telle que « un Canadien », pour protéger l'identité de cette personne. Les clients du gouvernement du Canada ainsi que les alliés du CST peuvent demander et recevoir cette information supprimée, pourvu qu'ils aient une justification opérationnelle à cet égard et qu'ils y soient autorisés. La divulgation d'information sur l'identité de Canadiens doit être effectuée en conformité avec la *Loi sur la protection des renseignements personnels* et avec le cadre de politique opérationnelle du CST. Pour en savoir davantage sur les pouvoirs et les limites se rapportant aux activités du CST, veuillez consulter le site Web du bureau à : www.ocsec-bccst.gc.ca.

Constatations

Le commissaire a pu établir ce qui suit :

- les divulgations par le CST d'information sur l'identité de Canadiens étaient conformes à la loi;
- le client du gouvernement du Canada ou l'allié qui a présenté la demande avait à la fois l'autorisation et la justification opérationnelle requises pour obtenir l'information;
- le CST avait appliqué efficacement les mesures de protection de la vie privée mentionnées dans les instructions ministérielles ainsi que dans ses politiques et procédures opérationnelles;
- le CST avait agi en conformité avec le cadre établi par le Cabinet concernant les risques inhérents au partage d'information avec des entités étrangères susceptible d'entraîner des mauvais traitements; et
- aucun incident relatif à la vie privée n'a été recensé en plus de ceux qui avaient déjà été consignés par le CST dans son Dossier relatif aux incidents liés à la vie privée.

Le CST est chargé d'effectuer une évaluation du risque de mauvais traitements lorsque c'est à lui qu'il incombe d'autoriser la communication de l'information. Toutefois, d'autres institutions du gouvernement du Canada assument aussi cette responsabilité lorsque des renseignements

sont diffusés par leurs propres canaux. Il est encourageant de constater que, dans les renseignements qu'il divulgue à des destinataires ne faisant pas partie de la collectivité des cinq, le CST a inclus une mise en garde précise pour rappeler aux clients du gouvernement du Canada à l'origine de ces demandes qu'il leur incombe d'effectuer une évaluation du risque inhérent au partage d'information avec une entité étrangère, lorsque cela pourrait entraîner des mauvais traitements.

Au cours de l'examen, le commissaire a communiqué des renseignements mettant en cause le SCRS au président du CSARS pour tout suivi que ce dernier pourrait juger pertinent.

Le système de gestion automatisée de l'information et des dossiers visant les demandes émanant de clients du gouvernement demeure efficace. Pour un certain nombre de raisons valables, le travail sur un système similaire de traitement des demandes émanant des alliés a été retardé. Le bureau surveillera les changements touchant les systèmes et les processus de divulgation d'information sur l'identité de Canadiens.

Conclusion

L'examen n'a donné lieu à aucune recommandation. Le bureau continuera d'effectuer des examens annuels des divulgations par le CST d'information sur l'identité de Canadiens à des clients et partenaires pour vérifier que le CST se conforme à la loi et protège la vie privée des Canadiens.

7. Examen annuel du Dossier relatif aux incidents liés à la vie privée et du Dossier des erreurs de procédure mineures tenus par le CST, 2015

Contexte

Depuis 2011, les commissaires effectuent un examen annuel de tous les incidents consignés par le CST qui ont fait peser un risque sur la vie privée d'un Canadien d'une manière qui va à l'encontre de ses politiques opérationnelles ou qui n'était pas prévue par ces politiques. En cas d'atteinte à la vie privée, le CST consigne l'incident dans le Dossier relatif aux incidents liés à la vie privée. Le CST utilise ce dossier pour surveiller les incidents comportant un risque pour la vie privée et y remédier, ainsi que pour améliorer les méthodes et politiques au besoin. Le Dossier des erreurs de procédure mineures fait état des erreurs opérationnelles survenues en rapport avec de l'information liée à la vie privée mais sans entraîner une perte de contrôle des renseignements de la part du CST ou leur divulgation à des destinataires externes qui n'auraient pas dû recevoir ces renseignements.

Le commissaire peut faire enquête en cas d'atteinte substantielle à la vie privée. Selon la politique pangouvernementale, une atteinte substantielle à la vie privée est une atteinte touchant des renseignements personnels sensibles, dont on peut raisonnablement penser qu'elle risque de causer un préjudice ou un dommage sérieux à la personne ou implique un nombre élevé de personnes touchées. Au cours des examens portant sur des activités particulières, le commissaire fait également enquête de manière approfondie sur les incidents liés à la vie privée.

Les objectifs de cet examen étaient :

- d'en apprendre davantage sur les incidents liés à la vie privée, les erreurs de procédure et les mesures prises par la suite par le CST pour corriger la situation ou atténuer les répercussions;
- d'en apprendre davantage sur les atteintes substantielles à la vie privée imputables aux opérations du CST et sur les mesures correctives connexes;
- de déterminer quels sont les incidents, le cas échéant, susceptibles de donner lieu à des interrogations quant à la conformité à la loi ou à la protection de la vie privée des Canadiens;

- de relever toutes les tendances ou lacunes systémiques qui pourraient donner à penser que des mesures correctives supplémentaires doivent être prises par le CST, que des changements doivent être apportés à ses méthodes ou à ses politiques ou qu'un examen approfondi d'un incident particulier ou d'une activité particulière doit être effectué par le commissaire; et
- d'évaluer le cadre de validation de la conformité à la politique et les activités de surveillance du CST.

Le commissaire a examiné tous les incidents liés à la vie privée et les mesures prises par la suite par le CST pour y remédier. Les incidents concernaient, par exemple, le partage ou l'intégration non intentionnel dans un rapport destiné à des clients ou dans un échange de courriels avec eux d'information non minimisée sur l'identité de Canadiens; le ciblage involontaire d'un Canadien ou d'une personne au Canada; et une recherche d'information se rapportant sans le savoir à un Canadien ou à une personne au Canada. Nous examinerons l'an prochain certains de ces incidents étant donné que le CST continuait de prendre des mesures pour y remédier au moment de l'examen. Certains autres incidents qui se rapportent à la transmission au SCRS d'information en provenance des partenaires du CST seront également analysés l'an prochain dans le cadre de l'examen de suivi planifié portant sur l'assistance fournie par le CST au SCRS en vertu de la partie c) de son mandat concernant un certain type de rapport mettant en cause des Canadiens.

Le commissaire a également examiné toutes les erreurs de procédure mineures consignées par le CST en 2015. Il s'agissait, par exemple : de la conservation d'information sur l'identité de Canadiens plus longtemps que ne l'autorise la politique; de la divulgation d'information concernant un Canadien au mauvais destinataire au sein du CST; et de l'envoi d'information concernant l'identité de Canadiens à des destinataires externes même si, dans ce cas, l'erreur a été corrigée avant que les destinataires en question aient accès à l'information.

Constatations et recommandation

D'après l'examen du Dossier relatif aux incidents liés à la vie privée et du Dossier des erreurs de procédure mineures, les réponses aux questions et la vérification de l'information contenue dans les bases de données du CST, le commissaire a conclu que le CST avait pris des mesures correctives pertinentes en réponse aux incidents liés à la vie privée et aux erreurs de procédure mineures qu'il a recensés en 2015.

Le commissaire n'a pas mis en doute l'évaluation du CST indiquant que les incidents liés à la vie privée recensés en 2015 ne représentaient pas des atteintes substantielles à la vie privée et il était d'accord avec l'évaluation du CST indiquant que les erreurs de procédure qu'il avait consignées étaient réellement mineures et n'avaient pas entraîné d'incidents liés à la vie privée.

Le CST a ajouté de l'information au Dossier relatif aux incidents liés à la vie privée pour indiquer si les incidents représentaient une atteinte substantielle à la vie privée et s'ils devaient être portés à l'attention de la direction et faire l'objet de mesures de sa part. Toutefois, globalement, le Dossier renfermait moins de détails qu'au cours des années précédentes. Bien que le CST ait répondu aux questions du bureau à propos des incidents, il est important de donner suffisamment d'explications dans le Dossier pour faire la preuve de la conformité et pour indiquer que des mesures appropriées ont été prises pour corriger ou atténuer toute répercussion possible d'un incident. Par conséquent, **le commissaire a recommandé** que le CST s'assure que son Dossier relatif aux incidents liés à la vie privée renferme une information adéquate pour décrire et documenter chaque incident de manière approfondie.

Au cours de notre examen des rapports dont il était question dans un incident lié à la vie privée, nous avons découvert qu'un petit nombre de rapports n'avaient pas été annulés ou republiés comme le recommandait le CST et comme il l'avait indiqué. Le CST a corrigé le problème et le bureau a vérifié que les rapports avaient été annulés.

Le CST a mis en œuvre une recommandation formulée au cours de l'examen des incidents liés à la vie privée mené en 2013 en révisant sa politique opérationnelle pour clarifier les questions relatives aux conventions d'appellation et à la suppression d'information sur l'identité de Canadiens dans les rapports de renseignements électromagnétiques étrangers. Le bureau examinera l'application de la nouvelle politique au cours des futurs examens des activités du CST.

Conclusion

La consignation et la déclaration des incidents liés à la vie privée demeurent une mesure efficace utilisée par le CST pour promouvoir la conformité aux obligations légales et aux exigences ministérielles ainsi qu'aux politiques et procédures opérationnelles et pour améliorer la protection de la vie privée des Canadiens. L'examen n'a révélé aucune atteinte substantielle à la vie privée, aucune lacune systémique ni aucune question nécessitant un examen de suivi. D'après le CST, il n'a pas été avisé de répercussions négatives sur les Canadiens concernés par les incidents liés à la vie privée. Les commissaires continueront de faire enquête sur ces incidents et les erreurs de procédure du CST. Le bureau continuera de surveiller les progrès relatifs aux constatations et à la recommandation formulées dans cet examen. Il collaborera également au besoin avec le Commissariat à la protection de la vie privée relativement aux atteintes substantielles à la vie privée.

Un thème récurrent : Modifications apportées à la *Loi sur la défense nationale*

Le 24 décembre 2001, la *Loi antiterroriste*, issue du projet de loi C-36, est entrée en vigueur. Ce projet de loi omnibus — adopté rapidement dans la foulée des événements du 11 septembre — renfermait de nombreux éléments ayant une incidence sur de nombreuses institutions et activités gouvernementales. L'ajout de la partie V.1 à la *Loi sur la défense nationale* (LDN) et les modifications apportées à la *Loi sur les secrets officiels* ont été fort appréciés puisqu'ils ont donné une assise législative aux activités du CST de même qu'aux activités du commissaire du CST, établissant les mandats, les pouvoirs et les relations des deux organismes avec le Parlement et le ministre de la Défense nationale.

Peu après l'adoption de la loi, toutefois, les commissaires qui se sont succédé ont commencé à formuler des préoccupations quant à l'application et à l'interprétation de la LDN. Au fil des années, ils ont recommandé que l'on supprime les ambiguïtés dans la législation et que l'on renforce la reddition de comptes du CST. Plus de 10 ans se sont écoulés depuis qu'un commissaire a demandé pour la première fois des modifications qui n'ont jamais été apportées.

- Les termes « activités » et « activité ou catégorie d'activités » sont employés dans la loi dans des contextes différents — se rapportant à la fois au CST et au commissaire — et il a été recommandé qu'ils

soient définis. Fait notable, les autorisations ministérielles visant la collecte de renseignements électromagnétiques étrangers permettent au CST d'intercepter non intentionnellement des communications privées en lien avec une « activité ou catégorie d'activités » qui y est précisée en tant que méthode d'acquisition de renseignements étrangers – le comment. Toutefois, les autorisations pourraient être interprétées comme se rapportant à une personne ou à un sujet en particulier – le qui ou le quoi.

- En ce qui concerne les conditions à remplir, le seuil requis pour que le ministre puisse délivrer une autorisation n'est pas clair. Il faudrait modifier la LDN de façon à préciser que l'autorisation repose sur « un motif raisonnable de croire » ou « un motif raisonnable de soupçonner ».
- Lorsqu'il entreprend les activités d'acquisition d'information prévues par son mandat, le CST peut intercepter de façon non intentionnelle une communication privée – au sens du *Code criminel* – mais il a besoin d'une autorisation ministérielle pour le faire. Le terme « acquérir » n'est pas défini dans la LDN, ni les termes « intercepter » et « interception », qui ne renvoient pas au *Code criminel*. En conséquence, le moment précis où le CST « acquiert » ou « intercepte » l'information dans le cadre de ses activités de collecte de renseignements électromagnétiques étrangers est ambigu. Or, ces termes sont d'une importance opérationnelle pour les activités de collecte de renseignements électromagnétiques étrangers et de cyberdéfense du CST et ils ont également leur importance pour le mandat du commissaire, lequel détermine si le CST se conforme à la loi.
- Le pouvoir de donner une autorisation ministérielle de cyberdéfense au CST renvoie à des circonstances précisées dans le *Code criminel* s'appliquant à une personne qui fournit au public un service de communications téléphoniques, télégraphiques ou autres et qui intercepte une communication privée en fournissant le service. Si l'on modifiait la LDN pour effectuer un renvoi à une partie différente du *Code criminel* – adoptée depuis que la partie V.1 de la LDN est entrée en vigueur – on lèverait toutes les ambiguïtés se rapportant au pouvoir accordé au CST de mener des activités de cyberdéfense comportant le risque d'interception non intentionnelle de communications privées.
- Le commissaire a recommandé que l'on modifie la LDN pour accorder explicitement au CST le pouvoir de recueillir, d'utiliser, de conserver et de divulguer des métadonnées. En prévoyant dans la loi des mesures de protection particulières de la vie privée dans le cadre des activités du

CST relatives aux métadonnées, comme celles que l'on trouve dans des instructions ou des politiques ministérielles, on améliorerait la reddition de comptes et la transparence.

- Enfin, on pourrait modifier la LDN afin de confier au commissaire de nouvelles fonctions pour appuyer le ministre dans sa reddition de comptes et le contrôle du CST. Par exemple, le commissaire pourrait effectuer une évaluation experte indépendante des autorisations ministérielles proposées, des conditions d'autorisation définies dans la Loi pour vérifier qu'elles sont remplies et prévoir des mesures de protection de la vie privée connexes. Comme le commissaire s'acquitte déjà de cette tâche, cela ne changerait que le moment où il l'effectue. Il pourrait ainsi mener à bien son évaluation et la remettre au ministre avant que les autorisations soient signées, ce qui renforcerait la reddition de comptes. Des réformes en ce sens sont en cours au Royaume-Uni.

L'adoption de mesures pour clarifier la loi irait dans le sens des engagements pris par le gouvernement, à savoir renforcer la reddition de comptes et la transparence de la législation et des activités du CST. Le commissaire affirme d'ailleurs que les modifications recommandées ne suscitent pas de controverse.

PLAINTES CONCERNANT LES ACTIVITÉS DU CST

En 2015–2016, le bureau a été contacté par plusieurs personnes en quête d'information ou exprimant des préoccupations concernant les activités du CST. Toutefois, il a été déterminé que les demandes de renseignements ne relevaient pas du mandat du commissaire, ne se rapportaient pas aux activités opérationnelles du CST ou manquaient de sérieux. Aucune plainte concernant les activités du CST ne justifiaient une enquête.

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

Le commissaire est 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 CST en faisant valoir la primauté de l'intérêt public. Aucune affaire de ce genre n'a été signalée au commissaire en 2015–2016.

ACTIVITÉS DU BUREAU DU COMMISSAIRE

Le travail du bureau axé sur les examens requiert une assise solide, non seulement en ce qui a trait à ses pouvoirs en vertu de la loi et à l'étendue des connaissances et des compétences techniques des agents chargés de l'examen, mais également en ce qui concerne la compréhension de son rôle par le gouvernement et de ses constatations par le public. Les activités de relations publiques, de réseautage et d'apprentissage du bureau renforcent sa capacité de mener à bien le mandat du commissaire.

Comité sénatorial permanent de la sécurité nationale et de la défense

Cette année, le commissaire a comparu à deux reprises devant le Comité sénatorial permanent de la sécurité nationale et de la défense. Lors de sa première comparution, en avril 2015, il devait s'exprimer dans le cadre des audiences en cours concernant la *Loi antiterroriste* de 2015 (projet de loi C-51), adoptée le 9 juin 2015 par le Parlement sous le gouvernement précédent. La partie 1 du projet de loi, *Loi sur la communication d'information ayant trait à la sécurité du Canada*, autorise le partage de renseignements avec 17 institutions désignées du gouvernement du Canada. Le commissaire a avisé le Comité qu'il avait écrit au président du Comité de la Chambre des communes examinant le projet de loi pour lui demander pourquoi les organismes d'examen actuels ne bénéficiaient pas également du pouvoir explicite de partager entre eux l'information. En réitérant la position qu'il avait adoptée dans la lettre, le commissaire a souligné l'importance, si l'on élargit les pouvoirs régissant le partage d'information entre les organismes d'application de la loi ou voués à la sécurité et au renseignement, d'accroître également la capacité des organismes d'examen correspondants à partager leurs renseignements et à coopérer entre eux. Il avait indiqué au Comité que la loi devrait explicitement autoriser la coopération entre le bureau, le Comité de surveillance des activités de renseignement de sécurité (CSARS) et la Commission civile d'examen et de traitement des plaintes relatives à la GRC (CCETP).

La partie 4 du projet de loi C-51 a ajouté des mesures propres à atténuer la menace pesant sur la sécurité du Canada qui ont été proposées pour le Service canadien du renseignement de sécurité (SCRS). Ces mesures ont une incidence directe sur le CSARS, qui examinera le rendement du SCRS à cet égard. Le commissaire a prévenu le Comité que ces mesures pourraient avoir une incidence sur le bureau, car il est possible que le

SCRS demande l'aide du CST pour intervenir en vue de réduire la menace pour la sécurité du pays et que le CST fournisse une assistance technique et opérationnelle au SCRS. L'incidence sur le bureau des mesures prévues par la partie 4 demeure inconnue. Toutefois, si le SCRS et le CST coopèrent en vertu de ces dispositions, le commissaire vérifiera s'il convient d'accroître les ressources du bureau en conséquence.

Lors de sa seconde comparution devant le Comité, en février 2016, le commissaire a répondu aux questions de ce dernier concernant le rapport annuel public de 2014–2015. (En raison du déclenchement des élections fédérales à la fin de l'été, le rapport n'a été déposé devant le Parlement qu'en janvier dernier.) Les observations formulées par le commissaire devant le Comité portaient sur les enjeux importants soulevés dans le cadre des examens menés au cours de l'exercice 2014–2015. On peut trouver le résumé non classifié de ces examens dans le Rapport annuel 2014–2015 sur le site Web du bureau.

Sensibilisation, apprentissage et réseautage

En avril 2015 et en mars 2016, le commissaire s'est adressé aux étudiants en droit de l'Université d'Ottawa, auxquels il a exposé le mandat et le rôle du bureau. Tout au long de l'année, il a également rencontré plusieurs de ses homologues au Canada et d'autres hauts fonctionnaires.

Cette année encore, le bureau a donné des présentations sur son travail devant les employés du CST nouvellement recrutés dans le cadre du programme d'apprentissage général du CST. Parallèlement, plusieurs employés du bureau ont assisté à des cours au CST, qui leur ont donné les mêmes informations de base qu'aux employés du CST.

Les avocates internes du bureau ont pris la parole devant les étudiants des cycles supérieurs de l'Université de Sherbrooke sur les pouvoirs et les activités du commissaire. En novembre et février, l'avocate interne du bureau et le directeur exécutif ont assisté à des conférences sur la protection de la vie privée et la sécurité à Vancouver et à Victoria, en Colombie-Britannique.

Tout au long de l'année, le personnel du bureau a également assisté à des conférences portant sur les affaires internationales, la sécurité de la technologie de l'information, la sécurité nationale, la protection de la vie privée et la cybersécurité. Ces conférences étaient organisées notamment par l'Association des industries canadiennes de défense et de sécurité, l'Association internationale des professionnels de la protection de la vie

privée, l'Association du Service du renseignement des Forces canadiennes et l'Association canadienne pour les études de renseignement et de sécurité. Des activités de ce genre aident les employés à se tenir au courant des problématiques liées à la sécurité, au renseignement et à la protection de la vie privée.

Le bureau a continué d'offrir son appui au « Canadian Network for Research on Terrorism, Security and Society » (TSAS), mis sur pied par plusieurs universitaires.

Consultation avec les organismes d'examen canadiens

Le Forum des organismes d'examen réunit des représentants du bureau, du CSARS, de la CCETP et du Commissariat à la protection de la vie privée du Canada. Il offre la possibilité de comparer les pratiques exemplaires en matière d'examen et de discuter des questions d'intérêt et de préoccupation mutuels. Le forum s'est réuni en septembre et en mars. En mars, il a invité des hauts fonctionnaires appartenant au Bureau du Conseil privé et à Sécurité publique Canada qui ont discuté d'idées et d'approches pour assurer la reddition de comptes et la coopération.

Comme par le passé, le commissaire a rencontré le président du CSARS pour des discussions générales concernant la coopération entre les deux organisations, et les directeurs exécutifs respectifs discutent régulièrement de la coordination des éléments de base des examens concernant à la fois le CST et le SCRS qui les intéressent mutuellement. Comme nous l'avons noté dans la section sur l'examen, plusieurs questions concernant le SCRS ont été soulevées au cours de l'examen des activités conjointes menées par le CST et le SCRS et ont été renvoyées au CSARS pour qu'il assure tout suivi qu'il juge opportun. Les hauts fonctionnaires du bureau, du CSARS et de la CCETP se sont également rencontrés pour discuter d'autres possibilités de coopération et d'échange sur les questions se rapportant à l'examen des organismes de renseignement et de sécurité.

Le commissaire a rencontré à plusieurs reprises au cours de l'exercice écoulé le nouveau commissaire à la protection de la vie privée du Canada, Daniel Therrien. M. Therrien et ses homologues provinciaux ont un domaine de responsabilité beaucoup plus vaste qui s'étend à toutes les institutions des secteurs public et privé relevant de leur compétence respective, alors que le mandat du commissaire du CST porte exclusivement sur la conformité du CST et la protection de la vie privée.

Consultation avec les organismes d'examen étrangers

En novembre, le directeur exécutif a rencontré le conseiller en chef en visite du comité parlementaire norvégien de surveillance du renseignement pour discuter de l'examen en général, y compris de la portée et des méthodes. Le bureau est également entré en contact et a eu des échanges avec plusieurs organismes d'examen d'autres pays.

PLAN DE TRAVAIL – EXAMENS EN COURS ET PRÉVUS

Le commissaire procède à partir d'un plan de travail triennal mis à jour deux fois par an et dont l'élaboration repose sur de nombreuses sources, notamment les séances d'information régulière du CST sur les nouvelles activités et les changements touchant les activités en place. Le rapport annuel classifié présenté par le chef du CST au ministre de la Défense nationale et faisant état des priorités du CST et des questions importantes sur le plan juridique, politique ou en matière de gestion constitue un autre document source important. Afin d'en apprendre davantage sur l'approche préventive axée sur le risque adoptée par le commissaire pour effectuer ses examens, veuillez consulter le site Web du bureau à : www.ocsec-bccst.gc.ca.

Trois examens et une étude amorcés en 2015–2016 seront achevés en 2016–2017 : un examen ciblé des activités relatives aux métadonnées menées par la section de la Sécurité des TI du CST; un examen portant sur une méthode particulière de collecte de renseignements électromagnétiques étrangers menée sous le régime d'une autorisation ministérielle et d'une directive ministérielle; un examen du partage des renseignements électromagnétiques étrangers avec des clients n'appartenant pas à la collectivité des cinq, notamment une évaluation du risque de mauvais traitement; et une étude portant sur la coopération et le partage d'information entre les employés du CST chargés de la sécurité des TI et ceux des renseignements électromagnétiques étrangers afin de contrer les cybermenaces.

Les autres examens censés débiter en 2016–2017 sont les suivants : un examen de suivi d'une méthode particulière de collecte par le CST de renseignements électromagnétiques étrangers menée sous le régime d'une autorisation ministérielle, qui sera axé sur les activités de ciblage du CST; un examen d'autres activités de ciblage du CST menées dans des circonstances exceptionnelles; un examen de suivi d'un certain

type de rapport concernant des Canadiens; et un examen de suivi portant sur l'aide fournie par le CST au Service canadien du renseignement de sécurité (SCRS) en vertu de la partie c) de son mandat et des articles 12 et 21 de la *Loi sur le Service canadien du renseignement de sécurité* se rapportant à l'interception des télécommunications de Canadiens désignés situés à l'extérieur du Canada (appelées originalement « Mandats d'interception au Canada de télécommunications étrangères »).

En outre, le commissaire continuera d'effectuer des examens annuels portant sur :

- les autorisations ministérielles de collecte de renseignements électromagnétiques étrangers et de cyberdéfense, y compris les vérifications ponctuelles de « communications canadiennes » acquises et identifiées par le CST;
- les divulgations par le CST d'information sur l'identité de Canadiens; et
- les incidents liés à la vie privée et les erreurs de procédure mises au jour par le CST et les mesures qu'il a prises par la suite pour y remédier.

ANNEXE A : BIOGRAPHIE DE L'HONORABLE JEAN-PIERRE PLOUFFE, CD

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 des Forces armées canadiennes. Il a pris sa retraite en 1976, alors qu'il était lieutenant-colonel. Par la suite, il a été avocat en pratique privée au sein du cabinet Séguin, Ouellette, Plouffe et associés, à Gatineau, au Québec, où il s'est spécialisé en droit criminel, a agi en tant que président du tribunal disciplinaire des pénitenciers fédéraux, ainsi qu'en tant qu'avocat de la défense en cour martiale. Par la suite, M. Plouffe a travaillé pour le bureau d'aide juridique en qualité de directeur de la section de droit criminel.

M. Plouffe a été nommé juge militaire en 1980 (Force de réserve), puis juge à la Cour du Québec en 1982. Pendant plusieurs années, il a été chargé de cours en procédure pénale à la Section de droit civil de l'Université d'Ottawa. 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.

Au cours de sa carrière, M. Plouffe a participé à la fois à des activités professionnelles et communautaires. Il a reçu des distinctions honorifiques civiles et militaires.

ANNEXE B : 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.

Loi sur les enquêtes

- (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.

Loi sur la protection de l'information

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.