

TRÈS SECRET // SI // RAC



**National Security
and Intelligence
Review Agency**

**Office de surveillance des
activités en matière de sécurité
nationale et de renseignement**

Examen de la conservation des données du renseignement électromagnétique par le Centre de la sécurité des télécommunications

OSSNR // Examen 23-14

TRÈS SECRET // SI // RAC

Table des matières

Sigles et acronymes	ii
Glossaire	iii
Sommaire	v
1. Introduction	1
Fondements législatifs	1
Portée de l'examen	1
Méthodologie	1
Énoncés généraux	2
2. Contexte	2
Cadre légal s'appliquant à la conservation des données SIGINT	3
Collecte, conservation et disposition des données SIGINT	4
3. Constatations, analyse et recommandations	6
Gestion de l'information sur un Canadien	6
Information sans valeur sur le plan du renseignement étranger	9
Problèmes relatifs aux politiques et aux pratiques en matière de SIGINT	16
4. Conclusion	24
Annexe A Calendrier de conservation des données SIGINT	25
Annexe B Synthèse des inspections techniques	28
Annexe C Constatations et recommandations	31

Sigles et acronymes

ARE Autorisation de renseignement étranger

CdC Collectivité des cinq

Chef Chef du CST



CR Commissaire au renseignement

CST Centre de la sécurité des télécommunications

EPM-RE Ensemble des politiques relatives à la mission – Renseignement étranger

GC Gouvernement du Canada

ICPC Information se rapportant à un Canadien ou à une personne se trouvant au Canada

MinDN ou le Ministre Ministre de la Défense nationale

OSSNR Office de surveillance des activités en matière de sécurité nationale et de renseignement

RE Renseignement étranger

SIGINT Renseignement électromagnétique (*Signals intelligence*)

Glossaire

Ciblage	Activité que le CST entreprend dans le but de se donner accès à des renseignements ayant trait à une cible.
Cible	Entité (personne, entreprise, organisation ou État étrangers) qui suscite l'intérêt du CST sur le plan du renseignement étranger
Collecte incidente	Acquisition d'une information qui n'était pas délibérément recherchée dans le contexte d'une activité d'acquisition d'information qui ne visait ni des Canadiens ni des personnes se trouvant au Canada.
Collectivité des cinq	Partenariat international d'échange de renseignement regroupant le Canada, l'Australie, la Nouvelle-Zélande, le Royaume-Uni et les États-Unis.
Données SIGINT	Aux fins du présent rapport, le terme « données SIGINT » désigne tous les éléments de communication bruts ou traités en transit (voir plus bas) qui ont été acquis au titre de l'article 16 de la Loi sur le CST et conservés dans des mémoires de collecte consultables et gérées par le CST.
Élément en transit	Unité élémentaire de données SIGINT dans les systèmes du CST. Communication d'une personne ou signal transmis par un canal de communication, qui ont été collectés aux fins du SIGINT. Les éléments en transit peuvent aussi consister en des contenus autres que ceux transmis par les voies de communication, par exemple, des fichiers [REDACTED] [REDACTED]
Ensemble des politiques relatives à la mission – Renseignement étranger (EPM-RE)	Politique opérationnelle SIGINT du CST. L'EPM-RE dont il est question dans le présent rapport a été approuvé au mois d'août 2023.

TRÈS SECRET // SI // RAC

- Renseignement étranger** Information sur les moyens, les intentions ou les activités d'un étranger, d'un État étranger, d'une organisation étrangère ou d'un groupe terroriste étranger, dans la mesure où ces moyens, ces intentions ou ces activités se rapportent aux affaires internationales, à la défense ou à la sécurité.
- Sélecteur** Identifiant unique associé à une entité (p. ex. un numéro de téléphone, une adresse électronique ou un compte de média social).

TRÈS SECRET // SI // RAC

Sommaire

Au sein du gouvernement du Canada, le Centre de la sécurité des télécommunications (CST) est l'organisme national responsable du renseignement électromagnétique (SIGINT pour *Signals intelligence*) lorsqu'il s'agit du renseignement étranger. Pour exploiter le renseignement étranger, le CST élabore, utilise et tient à jour de puissants outils servant à collecter, à traiter et à analyser les communications électroniques.

Certes, le CST est habilité à prendre des mesures extraordinaires pour collecter cette information – pour peu que ces mesures fassent l'objet d'une surveillance exercée en vertu d'autorisations délivrées par le ministre de la Défense nationale et approuvées par le commissaire au renseignement –, mais ce faisant, il doit remplir certaines conditions.

L'une des principales contraintes exercées sur le CST en matière de collecte s'applique à l'information se rapportant à un Canadien ou à une personne se trouvant au Canada (ICPC). La Loi sur le CST interdit au CST de diriger ses activités sur des Canadiens, mais il lui est permis d'acquérir incidemment de l'ICPC pendant le déroulement de ses activités. En outre, le CST peut conserver cette information à condition qu'elle ait une valeur au titre du renseignement étranger et que certaines conditions soient respectées. En revanche, le CST doit supprimer cette information si elle n'a aucune valeur sur le plan du renseignement étranger.

En règle générale, le CST est assujéti à la condition voulant que toute information acquise au titre d'une autorisation ne soit jamais conservée plus longtemps qu'il n'est raisonnablement nécessaire. Pour être en mesure de respecter cette condition, le CST doit établir et respecter des échéances de conservation.

Aux fins du présent examen, l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR, l'Office de surveillance) s'est penché sur l'écosystème technique qui permet au CST de conserver les données SIGINT. L'OSSNR a d'abord cherché à établir si et, le cas échéant, comment le CST remplissait ses obligations juridiques en matière de conservation des données SIGINT. L'OSSNR a également vérifié si le CST retenait les données SIGINT au-delà des échéances inscrites dans son calendrier de conservation et si le calendrier rendait adéquatement compte de tous les types de données collectées par le CST.

Bon nombre des systèmes SIGINT du CST disposent de mécanismes automatisés d'application de la politique, dont certains visent à protéger l'ICPC. Ces mécanismes permettent au CST de supprimer l'ICPC n'ayant aucune valeur sur le plan du renseignement étranger ou toute autre information qu'il aurait collectée par des moyens qui ne se plieraient pas aux contraintes.

TRÈS SECRET // SI // RAC

Néanmoins, l'OSSNR a soulevé une source de préoccupations majeure dans la façon dont le CST traite l'information n'ayant aucune valeur de renseignement étranger. Bien qu'elle ait principalement trait à l'information sur des non-Canadiens, cette source de préoccupation ouvre la possibilité que de l'information soit trop longtemps conservée.

- Le calendrier de conservation que le CST utilise pour le renseignement étranger ne fait aucune distinction entre l'information sur un non-Canadien ayant ou pouvant avoir une valeur sur le plan du renseignement étranger et l'information sur un non-Canadien établie comme n'ayant aucune valeur sur le plan du renseignement étranger. Or, cette situation témoigne d'un écart qui existe entre la façon dont la collecte et la conservation par le CST sont présentées au Ministre et la façon dont elles sont présentées dans les politiques et les pratiques opérationnelles du CST.
- Dans au moins deux cas (sur quatre inspections réalisées), le CST planifiait de conserver de l'information qu'il avait collectée sur un non-Canadien, alors qu'il avait établi que cette information n'avait aucune valeur sur le plan du renseignement étranger. Il pourrait s'agir là d'occurrences de non-conformité aux stipulations de l'*Autorisation de renseignement étranger pour les opérations réseau* délivrée au titre de l'article 26 de la Loi sur le CST.
- Plus généralement, le CST ne dispose d'aucun mécanisme permettant de supprimer, avant la fin de la période de conservation prescrite, certaines informations sur un non-Canadien dont on avait établi qu'elles n'avaient aucune valeur de renseignement étranger.

Outre cette source de préoccupation, l'OSSNR a constaté des faiblesses et des limites dans certains aspects des politiques et des pratiques du CST en matière de SIGINT :

15(1) d)
15(1) f)

- veiller à ce que les analystes cessent de cibler les sélecteurs correspondant à [REDACTED] qui ne sont plus d'intérêt en matière de renseignement étranger;
- demander au Ministre l'autorisation de conserver les informations [REDACTED] malgré le manque de préparation à cet effet, et l'absence d'exigences stratégiques exigeant une évaluation périodique de l'information quant à la valeur qu'elle pourrait avoir sur le plan du renseignement étranger;
- traiter les données SIGINT stockées ailleurs que dans les systèmes centraux de données SIGINT gérés par le CST;
- veiller à ce que les exigences s'appliquant à la conservation des données soient respectées, lorsque de l'information est échangée avec d'autres organismes, notamment avec les partenaires de la Collectivité des cinq.

TRÈS SECRET // SI // RAC

Compte tenu de la diversité des besoins opérationnels en collecte SIGINT – lesquels besoins peuvent être difficiles à prévoir et sont appelés à changer avec le temps –, le CST doit acquérir des données pour être en mesure d'exercer sa mission, mais il doit également se soumettre à des contraintes sur le plan de la conservation des données collectées. L'engagement du CST à respecter ses obligations en matière de conservation des données était manifeste tout au long du présent examen, particulièrement dans la façon dont il traitait et protégeait l'ICPC. Toutefois, en raison des problèmes soulignés précédemment, notamment les potentialités de non-conformité à son *Autorisation de renseignement étranger pour les opérations réseau*, le CST doit continuer de porter une attention particulière à la conservation des données et au respect des échéances de conservation.

TRÈS SECRET // SI // RAC

1. Introduction

Fondements législatifs

1. Le présent examen a été réalisé en application de l'alinéa 8(1)a) de la Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (Loi sur l'OSSNR).

Portée de l'examen

2. L'OSSNR a examiné l'écosystème technique qui permet au CST de conserver les données SIGINT (information acquise au titre de l'article 16 de la Loi sur le CST). L'OSSNR a d'abord cherché à établir si et, le cas échéant, comment le CST remplissait ses obligations juridiques en matière de conservation des données SIGINT. L'OSSNR s'est concentré sur la façon dont le CST conservait les données dans les systèmes opérationnels, à savoir ceux qui servent à collecter, à traiter et à analyser lesdites données.
3. Les mesures prises par le CST pour la conservation des données SIGINT s'appuient sur des échéances établies dans un calendrier de conservation (voir en annexe A). L'OSSNR a donc vérifié si le CST retenait les données SIGINT au-delà des échéances inscrites dans son calendrier de conservation et si le calendrier rendait adéquatement compte de tous les types de données collectées par le CST.
4. L'écosystème technique que le CST emploie pour la conservation des données SIGINT est complexe et compte plusieurs systèmes ainsi que de nombreuses capacités. Après avoir examiné ces systèmes de façon globale, l'OSSNR s'est attardé davantage à un sous-ensemble de systèmes employé pour collecter, traiter, visualiser et conserver les données SIGINT.
5. La période visée par l'examen s'étend d'octobre 2020 à avril 2024.

Méthodologie

6. L'OSSNR a assisté à des séances d'information ainsi qu'à des démonstrations techniques que des experts du CST ont effectuées sur place. L'OSSNR a également demandé au CST de lui fournir des documents écrits, notamment des réponses à des questions particulières.
7. L'OSSNR a réalisé quatre inspections techniques dans le cadre de sa vérification des politiques et des pratiques du CST ainsi que des mesures techniques prises en matière de conservation des données SIGINT. Ces inspections ont permis à l'OSSNR d'évaluer les affirmations que le CST avait faites au sujet de ses

TRÈS SECRET // SI // RAC

pratiques, grâce à l'inspection de données qui avaient été collectées, puis enregistrées dans les systèmes SIGINT du CST. À l'occasion de chacune de ces inspections, les représentants de l'OSSNR ont rencontré le personnel responsable du ciblage, de l'acquisition et de l'évaluation d'un flux particulier de données SIGINT. L'OSSNR donne de plus amples détails au sujet de ces inspections à l'annexe B.

Énoncés généraux

8. Selon la Loi sur l'OSSNR, l'Office de surveillance doit avoir un accès complet et en temps voulu à tous les renseignements détenus par un ministère ou un organisme (à l'exception des documents confidentiels du Cabinet) et est en droit de recevoir, de la part des ministères ou organismes concernés, tout document et explication que l'OSSNR juge nécessaires. L'OSSNR surveille le degré de coopération affiché en réponse à ses demandes d'accès et prend bonne note de la complétude et de l'exactitude des informations qui lui sont communiquées. C'est notamment à partir de ces facteurs que l'OSSNR évalue la réactivité des ministères et organismes dans le cadre de chacun des examens¹.
9. Dans le contexte du présent examen, le CST a partiellement répondu aux attentes de l'OSSNR pour ce qui a trait à la réactivité. Les représentants du CST ont veillé à ce que l'OSSNR reçoive les documents demandés en temps voulu et ont fourni de l'information de façon proactive lors des réunions et des séances d'information. Toutefois, le CST n'a pas fourni à l'OSSNR un accès direct aux outils de collaboration qu'il exploite. Il n'a plutôt fourni que des copies de l'information demandée, et ce, dans un format qui rendait difficile tout type d'examen. Par ailleurs, l'OSSNR n'a pas été en mesure d'examiner l'utilisation que le CST fait des outils de collaboration de la Collectivité des cinq, au motif que le CST ne pouvait fournir aucun accès à cette information. En somme, même si le CST n'a répondu que partiellement aux attentes de l'OSSNR en matière de réactivité, l'OSSNR n'en demeure pas moins convaincu de la pertinence des constatations et des recommandations qu'il a formulées dans le présent rapport.

2. Contexte

10. En tant qu'organisme SIGINT du gouvernement du Canada (GC), le CST acquiert de l'information concernant les activités qui sont menées par des entités

¹ Les attentes de l'OSSNR en matière de réactivité ont été mises en ligne à l'adresse suivante : <https://nsira-ossnr.gc.ca>.

TRÈS SECRET // SI // RAC

étrangères et qui correspondent aux intérêts et aux priorités du GC en matière de renseignement. Le CST se sert d'outils avancés pour collecter, comprendre et interpréter les divers types de communication électronique, notamment les appels téléphoniques, les messages textes, les communications entre ordinateurs et par Internet, ainsi que les signaux transmis par satellites.

15(1) d)
15(1) f)

11. Cette collecte est vaste. Les communications électroniques sont transmises dans divers formats, à une vitesse considérable et selon des protocoles qui changent ou évoluent constamment. Elles sont également soumises à l'intensification du recours aux protocoles de chiffrement fort. En réaction à ces tendances, les organismes chargés du SIGINT collectent des données passivement, en copiant les flux de communication, ou [REDACTED]

[REDACTED] Dans ce contexte, le CST a élaboré un éventail d'outils et de sources permettant de reconnaître, de récupérer et de stocker en toute sécurité l'information destinée au volet renseignement étranger (RE) de son mandat. Cette information est ensuite traitée, analysée et transmise aux clients du GC.

12. En tant qu'organisme fédéral, le CST doit se soumettre aux lois et aux politiques du GC s'appliquant à la gestion et à l'élimination des renseignements contenus dans ses fonds d'information. En outre, ce cadre juridique et stratégique concerne également l'information que le CST collecte aux fins du renseignement étranger. Ainsi, la conservation constitue un important facteur que le CST doit prendre en compte pour se conformer aux politiques s'appliquant à ses activités de RE.

Cadre légal s'appliquant à la conservation des données SIGINT

13. Les pouvoirs juridiques du CST en matière de conservation des données SIGINT commencent avec le pouvoir de collecter des données SIGINT. L'article 16 de la Loi sur le CST fait état du volet RE du mandat du CST, lequel nécessite l'acquisition, puis l'exploitation d'information SIGINT dans le but de fournir du RE répondant aux priorités du gouvernement en matière de renseignement.
14. En fait, le CST exerce ce volet de son mandat en fonction des pouvoirs énoncés dans les autorisations de renseignement étranger (ARE). Délivrées par le Ministre et approuvées par le commissaire au renseignement (CR), ces ARE font état des moyens et des méthodes permettant au CST d'exploiter ce volet du mandat qu'il exerce. Ce qu'il convient de prendre particulièrement en compte, c'est l'*Autorisation de renseignement étranger pour les opérations réseau*, dont une version est produite pour chacune des années visées par l'examen.
15. Les ARE approuvées ne sont pas un fait isolé. De fait, le Ministre délivre les ARE en se fondant sur une demande que le chef du CST lui a soumise par écrit et dont

TRÈS SECRET // SI // RAC

la teneur a également été transmise au CR. Ainsi, les documents contenus dans le dossier de demande alimentent les décisions prises par le Ministre et le CR dans la mesure où ils établissent les faits devant permettre au Ministre de conclure si l'autorisation est nécessaire et si les conditions préalables à leur délivrance sont réunies.

16. La principale politique suivant laquelle le CST mène ses activités de RE, à savoir l'Ensemble des politiques relatives à la mission – Renseignement étranger (EPM-RE), est jointe au dossier de demande. L'EPM-RE comprend un calendrier de conservation fondé sur le type d'information en cause et les modalités de collecte, mais il indique également si des éléments liés à des intérêts de Canadiens en matière de vie privée ont été reconnus (voir à l'annexe A). Avant qu'une ARE puisse être délivrée, la Loi sur le CST demande que le Ministre ait conclu qu'il y a des motifs raisonnables de croire que toute information acquise ne sera pas conservée plus longtemps que ce qui est raisonnablement nécessaire [alinéa 34(2)a)]. Le calendrier de conservation résulte de l'interprétation que fait le CST quant à ce qui est « raisonnablement nécessaire ».

Collecte, conservation et disposition des données SIGINT

17. Le CST se doit d'établir principalement quelles données il peut conserver et pendant combien de temps cette conservation peut durer. En premier lieu, il convient de souligner que le CST est assujéti à d'imposantes contraintes relativement aux données se rapportant à des Canadiens ou à des personnes se trouvant au Canada. En effet, dès lors que ces données sont collectées, mais qu'elles ne s'avèrent pas essentielles à sa mission, le CST doit être en mesure de les supprimer de ses systèmes, c'est-à-dire d'en abréger le temps de conservation. En second lieu, le CST n'est pas en mesure de collecter et de conserver toutes les données qui *pourraient* être d'intérêt. Le stockage des données est onéreux, et il en va de même pour l'expertise technique nécessaire au développement et à la tenue à jour des systèmes du CST qui servent à collecter, à conserver et à interroger les données SIGINT. Certes, le CST a le pouvoir de conserver les données pendant une certaine période, [REDACTED]

15(1) f)

18. Les données SIGINT ont un cycle de vie. En l'occurrence, les données sont traitées par une série de systèmes conçus pour la collecte, l'enrichissement, le traitement et le stockage, et sont ensuite mises à la disposition des analystes du renseignement du CST. Généralement, les données SIGINT sont traitées par plusieurs systèmes avant qu'un analyste du renseignement puisse les interroger et les analyser. Lorsque l'analyste y trouve de l'information utile, il peut en faire

15(1) f)

TRÈS SECRET // SI // RAC

mention dans un compte rendu de renseignement ou l'utiliser pour élaborer de nouvelles collectes.

19. Toutes les données SIGINT collectées se voient attribuer une série d'identifiants qui permettent aux systèmes du CST de les traiter en fonction de certaines caractéristiques, notamment, le pouvoir au titre duquel elles ont été collectées ainsi que leur date de suppression. Il convient de noter que de cette façon, les systèmes du CST peuvent automatiquement identifier et supprimer les données conformément aux paramètres du calendrier.
20. Les données sont assujetties à diverses périodes de conservation en fonction de ce qui les caractérise. Ces périodes de conservation sont inscrites dans le calendrier de conservation du CST (voir à l'annexe A). Par exemple, lorsqu'elles sont réputées contenir des éléments canadiens qui sont d'intérêt en matière de vie privée, les données sont généralement assorties d'une période de conservation relativement courte, voire d'aucune période de conservation. Pour les autres types de données, les périodes de conservation peuvent varier entre [REDACTED] – pour certaines informations non sélectionnées – et [REDACTED] pour la plupart des communications que le CST collecte. [REDACTED]
[REDACTED]
21. Pendant la période visée par le présent examen, le CST a cherché à obtenir, pour certaines données, des exemptions permettant de prolonger leur temps de conservation au-delà de la période normale, et ce, pour des motifs opérationnels.
22. Lorsque les analystes évaluent les données, le CST peut entamer l'une de trois mesures qui peuvent influencer sur la période de conservation.
 - Premièrement, les données peuvent avoir été « rapportées ». Ce marqueur est employé lorsque les analystes intègrent ces données dans un rapport ou y font référence. En l'occurrence, la période de conservation s'étend à [REDACTED]
 - Deuxièmement, les données peuvent être « annotées ». Ce marqueur est employé pour indiquer le fait qu'on y a reconnu un intérêt concernant la vie privée d'un Canadien. Or, lorsqu'elles ne correspondent pas aux critères autorisant la conservation, ces données sont appelées à être supprimées dans les [REDACTED]
[REDACTED]
 - Troisièmement, les données peuvent être « éliminées ». Ce marqueur est utilisé lorsque les données ont été collectées de façon non conforme. Les données sont alors destinées à être prioritairement supprimées de tous les systèmes du CST (et des systèmes de la Collectivité des cinq si lesdites données ont été communiquées) dans les [REDACTED]

TRÈS SECRET // SI // RAC

Seuls certains analystes responsables de l'assurance des données peuvent créer des demandes d'élimination. L'élimination a généralement lieu en réaction à un incident de non-conformité. Ce type d'élimination doit répondre à des exigences plus élevées que celles s'appliquant aux suppressions conventionnelles : les responsables de systèmes doivent confirmer que les données ont été supprimées; le nombre des éléments en transit touchés est vérifié grâce à un rapport de conformité.

23. Une fois qu'elles sont arrivées à la fin de leur période de conservation, les données doivent être éliminées, sauf lorsqu'elles ont une valeur archivistique (c.-à-d. qu'elles servent de référence à un compte rendu de renseignement). Le bibliothécaire et archiviste du Canada permet au CST de disposer de [traduction] « [...] tout le "trafic" brut et traité qui est stocké dans des mémoires de données et qui est sous le contrôle du CST » – ce que l'on désigne par le terme « données SIGINT » dans le présent rapport – lorsque le CST détermine qu'il [traduction] « [...] n'est plus opérationnellement ni juridiquement nécessaire » de les conserver.

3. Constatations, analyse et recommandations

Gestion de l'information sur un Canadien

Constatation 1. L'OSSNR constate que le CST a mis en place des mesures de protection de la vie privée des Canadiens et des personnes se trouvant au Canada dans les systèmes de conservation, les fonctions et les outils appelés à traiter les données SIGINT.

24. Le CST acquiert, traite et conserve les données SIGINT en se servant d'un écosystème complexe et évolutif comprenant des bases de données, des applications et des services. Ainsi, en raison de leur nature, les données SIGINT forcent le CST à régulièrement développer et modifier ses systèmes de collecte et de traitement. Il peut même arriver que le CST doive abolir des systèmes pour ensuite en transférer les fonctions à d'autres systèmes en place ou doive tout simplement élaborer de nouveaux systèmes.
25. Outre ses propres systèmes, le CST mise sur des services et des outils fournis [REDACTED] – développés et tenus à jour par [REDACTED] mais aussi par des partenaires de la Collectivité des cinq – ce qui ajoute à la complexité de l'écosystème du CST. Ces outils exigent souvent que le CST s'adapte à des données et à des technologies sur lesquelles il n'a aucun contrôle. Les

15(1) d)

TRÈS SECRET // SI // RAC

répercussions que le recours à des tiers peut avoir sur la conservation sont abordées dans l'énoncé de la constatation 10.

- 15(1) d) 26. Le CST gère ce complexe écosystème technique en mode « distribué », ce qui signifie que la responsabilité à l'égard des composantes n'est pas centralisée. Ainsi, [REDACTED] d'ingénieurs et d'informaticiens développent et tiennent à jour les centres de stockage, les applications et les services qui composent l'écosystème du CST.
27. L'EPM-RE exige le recours à une approche cohérente en matière de développement et de tenue à jour des systèmes. Ainsi, il faut que les systèmes reçoivent et conservent des données qui soient admissibles, que des mesures appropriées de contrôle des accès soient en place et que les systèmes soient adéquatement documentés. L'OSSNR a observé plusieurs pratiques exercées au sein du CST pour veiller à ce que la politique et les systèmes de mise en œuvre de la politique s'harmonisent l'un avec l'autre. Par exemple, le personnel d'un important programme de collecte a décrit son apport annuel au processus d'autorisation ministérielle, à savoir veiller à ce que les détails techniques de la collecte soient présentés avec exactitude, tout en confirmant que sa compréhension des exigences relatives à la conformité découlait de l'autorisation elle-même. Semblablement, le personnel responsable d'un système d'analyse central a décrit la façon dont les équipes stratégiques du CST étaient mobilisées de façon proactive lorsque surviennent de nouvelles exigences stratégiques.
- 15(1) f) 28. La Loi sur le CST interdit au CST de diriger ses activités contre des Canadiens ou des personnes se trouvant au Canada. Or, le CST a mis en place bon nombre de mécanismes et de mesures de contrôle visant à limiter la probabilité d'acquérir ou de conserver de l'information se rapportant à un Canadien ou à une personne se trouvant au Canada (ICPC). Par exemple, l'une des trousse d'outils fonctionne [REDACTED] [REDACTED] pour filtrer le trafic avant qu'il n'entre dans les plateformes du CST qui servent à la conservation des données. Les analystes du CST sont également tenus de procéder à une évaluation de l'extranéité tout au long du cycle de vie SIGINT de sorte à réduire la probabilité que le CST dirige ses activités contre des Canadiens ou des personnes se trouvant au Canada.
29. Malgré ces contrôles, il peut arriver que le CST collecte accidentellement de l'ICPC. Pour parer ce type d'occurrence, le CST a mis en place des processus visant à traiter l'ICPC qui est collectée et reconnue en tant qu'ICPC. Dès lors qu'elle est reconnue, l'ICPC peut être traitée suivant l'une de deux modalités possibles :

15(1) f)

TRÈS SECRET // SI // RAC

- Lorsqu'il juge que les données sont essentielles aux enjeux relevant des affaires étrangères, de la défense ou de la sécurité [voir l'alinéa 34(2)c) de la Loi sur le CST], l'analyste doit les annoter de sorte qu'elles soient désignées comme étant de l'ICPC essentielle, ce qui entraîne leur conservation. Toutefois, leur période de conservation est réduite à [REDACTED]. Pour conserver les données au-delà des [REDACTED], l'analyste doit vérifier si elles sont toujours essentielles. Ainsi, une nouvelle période de conservation de [REDACTED] est ajoutée chaque fois que les données sont jugées comme étant essentielles.
 - Lorsque l'analyste estime que les données ne sont pas essentielles, il doit les annoter de sorte qu'elles soient désignées comme étant de l'ICPC non essentielle, ce qui entraîne leur suppression des systèmes du CST. En l'occurrence, les systèmes doivent supprimer les données dans les [REDACTED] suivant leur annotation.
30. Lorsque des données sont collectées de façon non conforme (p. ex. les données collectées auprès d'une cible pendant que celle-ci se trouvait au Canada), le CST utilise un mécanisme d'élimination qui priorise leur suppression des systèmes.
31. L'une des quatre inspections portait sur des données ayant fait l'objet d'une demande d'élimination. En outre, l'OSSNR a examiné la correspondance faisant état du traitement de ladite demande et a pu confirmer que les éléments en transit qui étaient visés avaient bel et bien été éliminés.
32. Compte tenu de la nature et du volume des communications modernes ainsi que de la portée du volet RE de son mandat, le CST était susceptible de tomber sur de l'ICPC pendant ses activités de collecte de RE. Bien que le CST ne cherche pas à obtenir ce type d'information – rappelons que le CST a mis en place des mesures de précaution visant à éviter de diriger ses activités contre des Canadiens ou des personnes se trouvant au Canada –, il finira par en recueillir. Le CST doit donc disposer de processus rigoureux permettant de traiter l'ICPC dès qu'elle a été reconnue. Les systèmes de traitement SIGINT fournissent aux analystes les outils dont ils ont besoin pour effectuer cette tâche, ce qui permet de contrebalancer l'inévitabilité de la collecte d'ICPC par des mécanismes de suppression ou d'élimination de ladite ICPC.

TRÈS SECRET // SI // RAC

Information sans valeur sur le plan du renseignement étranger

Constatation 2. L'OSSNR constate que le calendrier dont le CST se sert pour la conservation du renseignement étranger ne tient pas compte de l'information sur les non-Canadiens qui n'a aucune valeur sur le plan du renseignement étranger.

Constatation 3. L'OSSNR constate que le CST ne dispose pas de mécanismes aptes à supprimer certaines informations relatives à des non-Canadiens qui n'ont aucune valeur sur le plan du renseignement étranger, ce qui pose le risque que le CST conserve ces informations plus longtemps qu'il n'est raisonnablement nécessaire.

Constatation 4. L'OSSNR constate que le CST a conservé de l'information sur des non-Canadiens, malgré qu'il ait été établi que cette information n'avait aucune valeur sur le plan du renseignement étranger. Cette conservation pourrait ne pas être conforme aux stipulations de l'*Autorisation de renseignement étranger pour les opérations réseau* délivrée au titre de l'article 26 de la Loi sur le CST.

33. La procédure permettant d'établir la « valeur » sur le plan du RE n'est pas si simple. En outre, elle est subjective et se fonde sur les connaissances et l'expertise de personnes qui travaillent sur des ensembles de cibles en constante évolution. Pour illustrer le propos, disons que l'information ayant une valeur de RE serait l'aiguille dans la botte de foin que représenterait l'immense volume d'information collectée par le CST. Or, ce qu'un analyste voit comme une aiguille peut être simplement vu comme du foin par un autre analyste; tout dépend de la valeur relative qu'ils reconnaissent en fonction de leurs domaines respectifs. Semblablement, ce qui ne ressemble en rien à une aiguille aujourd'hui pourrait en être une demain dans la mesure où le domaine du RE change. Par conséquent, le CST tend vers la prudence lorsqu'il traite l'information collectée en préférant conserver le plus d'information possible tout en respectant les limites imposées par son calendrier de conservation – bien souvent, ce qui est supprimé ne peut plus être collecté de nouveau.
34. Malgré tout, il y a des situations où les analystes du renseignement déterminent que l'information collectée n'a aucune valeur de RE, et la présente section traite de ce type de situation. Par ailleurs, il convient de noter que l'OSSNR n'a pas indépendamment estimé la valeur de RE de l'information collectée. Ainsi, les observations formulées ci-après se fondent sur l'estimation des analystes du CST.
35. La demande d'ARE et le processus d'approbation qui s'ensuit comportent plusieurs étapes ainsi qu'un examen de la part du chef, du Ministre et du commissaire au renseignement. L'alinéa 35d) de la Loi sur le CST exige,

TRÈS SECRET //SI // RAC

notamment, que les ARE énoncent « les conditions ou les restrictions que le Ministre estime souhaitables [...] pour assurer que les activités visées par l'autorisation soient raisonnables et proportionnelles ». Dans l'*Autorisation de renseignement étranger pour les opérations réseau*, le Ministre a ajouté une condition ayant trait à l'acquisition et à la conservation de l'information :

[Traduction] « [...] l'information est acquise en fonction des besoins du CST en matière de renseignement étranger. Il s'agit, en l'occurrence, de limiter le volume d'information qui est conservé en tant qu'information dont on estime qu'elle contient du renseignement étranger ou qu'elle s'avère utile aux fins du volet renseignement étranger du mandat du CST ».

Cette condition s'applique à toutes les activités menées au titre de l'ARE et propose un critère d'établissement de la valeur de RE, à savoir que l'information soit considérée comme contenant du RE ou comme étant utile à l'exercice du volet RE du mandat du CST. Lorsqu'il est établi que les données en question ne répondent pas à ce critère, la conservation ne peut plus être autorisée au titre de l'ARE délivrée en vertu de l'article 26 de la Loi sur le CST.

36. Les dossiers de demandes d'ARE analysés pendant la période visée par le présent examen en disent un peu plus au sujet du respect de ce critère en indiquant que [traduction] « le CST ne conserve que l'information qui fera avancer le volet renseignement étranger du mandat du CST conformément à l'EPM-RE ». Compte tenu de cet énoncé, il est raisonnable de s'attendre à ce que le CST établisse une distinction entre, d'une part, l'information dont la valeur de RE est avérée ou potentielle (information qui fera avancer le volet RE du mandat) et, d'autre part, l'information qui n'a pas cette valeur (information qui *ne fera pas* avancer le volet RE du mandat). Toutefois, le calendrier de conservation établi par l'EPM ne fait pas cette distinction, sauf pour l'ICPC. L'EPM ne contient rien qui corresponde à l'énoncé fait au Ministre – il n'y a aucune exigence selon laquelle le CST « conserve seulement » ce type d'information ni rien qui prescrive la suppression des données n'ayant aucune valeur de RE avant la fin de sa période de conservation.

37. Au cours du présent examen, l'OSSNR a réalisé quatre inspections de données que le CST avait collectées [REDACTED] (voir l'annexe B). Dans l'une de ces inspections (inspection 3), les données collectées ont permis d'exercer d'autres activités de RE. Pour les trois autres inspections, les analystes du CST ont trouvé que l'information [REDACTED] n'avait aucune valeur de RE :

15(1) d)
15(1) f)

- Au cours de l'inspection 1, les représentants du CST avaient choisi une cible particulière et croyaient que [REDACTED] par la cible. Or,

15(1) d)
15(1) f)

TRÈS SECRET // SI // RAC

l'information collectée a révélé [REDACTED] la cible, mais qu'il appartenait plutôt à une personne non apparentée, qui ne présentait aucun intérêt sur le plan du RE.

- Au cours des inspections 2 et 4, le CST n'avait pas déterminé de cible désignée ou connue. Il [REDACTED] en fonction [REDACTED]

[REDACTED] L'information collectée a montré que [REDACTED]
[REDACTED] ne correspondaient pas [REDACTED] et que [REDACTED]
[REDACTED] ne présentaient aucun intérêt sur le plan du RE.

38. Au cours de l'inspection 2, l'analyste a décelé un faible indice établissant un lien potentiel avec le Canada et a supprimé les données. Cette intervention a eu lieu par l'intermédiaire du processus d'élimination, et [REDACTED] a été inscrit à la liste des entités protégées de sorte à prévenir tout ciblage ultérieur. Cette inspection a confirmé que le processus du CST s'appliquant à la suppression d'information ayant un rapport avec l'intérêt d'un Canadien en matière de vie privée fonctionnait comme prévu.
39. Au cours des inspections 1 et 4, les analystes ont marqué les données collectées de sorte à indiquer qu'elles n'avaient aucune valeur de RE, en s'attendant à ce que ce marquage empêche tout nouveau ciblage [REDACTED]. Cette démarche n'a pas fonctionné comme l'analyste s'y attendait et fait l'objet de la constatation 6 énoncée dans le présent rapport. Néanmoins, il s'agissait là d'une évaluation indiquant clairement, selon les experts travaillant sur ces cibles, que l'information collectée n'avait aucune valeur de RE.
40. Même s'il a été établi que les données n'avaient aucune valeur de RE, on ne s'est pas attendu pour autant à ce que les analystes les suppriment des systèmes du CST, si ce n'est qu'à leur connaissance, il n'existait aucun mécanisme leur permettant de procéder à cette suppression. Questionnés à ce sujet, les représentants du CST ont fini par indiquer que [traduction] « une procédure ponctuelle de suppression manuelle peut être engagée par une demande adressée à nos administrateurs de systèmes depuis notre application de gestion des demandes ». Toutefois, le CST n'a pas montré à l'OSSNR qu'il aurait fait part de cette procédure aux analystes. Par ailleurs, s'il y avait eu un indice signalant un lien avec le Canada, comme c'était le cas pour l'inspection 2, l'analyste aurait pu engager la procédure d'élimination prévue par le CST.
41. Le CST s'est fié au calendrier de conservation des données RE présenté dans l'EPM pour conserver les données provenant [REDACTED] examinés lors des inspections 1 et 4. Toutefois, il semble y avoir des écarts entre la Loi sur le CST, les ARE et l'EPM pour ce qui a trait à la conservation des données qui n'ont

TRÈS SECRET // SI // RAC

aucune valeur de RE. Rappelons que même si l'EPM ne reconnaît aucune distinction entre l'information ayant une valeur de RE et celle qui n'en a aucune, l'ARE et les applications connexes, pour leur part, établissent une norme de conservation axée sur la valeur de l'information. Le CST a déterminé que cette information n'avait aucune valeur de RE. Ainsi, le fait de continuer la conservation de cette information pourrait déroger aux conditions de conservation énoncées dans l'ARE.

42. Le pouvoir que le CST exerce en matière d'acquisition et de conservation de l'information n'est pas arbitraire. Bien que la Loi sur le CST et les ARE autorisent l'acquisition initiale d'information répondant aux priorités du GC en matière de renseignement, des évaluations subséquentes de cette information pourraient révéler qu'en fait, elle ne répond pas auxdites priorités en matière de renseignement. Sans une politique qui établisse une distinction entre les données qui ont une valeur de RE et celles qui n'ont pas cette valeur, le CST risque de continuer de conserver de l'information en contravention aux conditions énoncées plus haut.
43. La valeur des données collectées n'est pas évidente dès le départ. En effet, il se peut que les données n'aient aucune valeur pour une équipe, mais une valeur potentielle pour une autre équipe. Il existe donc des situations où la décision de conserver ces données n'irait pas à l'encontre des conditions. Une politique peut servir à préciser ce type de nuance. Or, il n'est pas raisonnablement nécessaire de conserver des données pendant [REDACTED] lorsqu'elles ont été jugées comme n'ayant aucune valeur de RE. C'est ce qui ressort des données examinées pendant les inspections : dans l'une d'entre elles, les données ne correspondaient pas à la cible connue et visée; dans deux autres, les données ont révélé que les personnes ciblées ne correspondaient pas [REDACTED] attendu et qu'elles n'étaient d'aucun intérêt pour ce qui est du RE.

15(1) f)

Recommandation 1. L'OSSNR recommande que le CST supprime immédiatement les données qui ont été jugées comme n'ayant aucune valeur sur le plan du renseignement étranger dans le contexte des inspections 1 et 4 dans la mesure où la conservation de ces données n'est pas raisonnablement nécessaire.

Recommandation 2. L'OSSNR recommande que le CST modifie son Ensemble de politiques relatives à la mission en créant une catégorie pour l'information sur un non-Canadien reconnue comme n'ayant aucune valeur sur le plan du renseignement étranger, et qu'il fixe une échéance pour sa suppression de sorte qu'elle ne soit pas conservée plus longtemps qu'il n'est raisonnablement nécessaire.

Constatation 5. L'OSSNR constate que l'approche choisie par le CST consistant à traiter certains types de données SIGINT en tant « qu'éléments en transit » – alors que plusieurs communications distinctes peuvent parfois être groupées dans un seul élément – pourrait donner lieu à la conservation d'information n'ayant aucune valeur sur le plan du renseignement étranger.

44. Lorsque le CST collecte des données SIGINT, il les traite de sorte à produire et à conserver des « éléments en transit » discrets, l'élément en transit constituant l'unité élémentaire à partir duquel les mécanismes de conservation du CST fonctionnent. Ce qui constitue un élément en transit peut varier en fonction de la méthode de collecte ou de la façon dont le CST choisit de traiter cet élément.
45. [REDACTED] du CST permet d'accéder [REDACTED]
[REDACTED] L'acquisition d'information provenant directement [REDACTED] constitue l'une des méthodes employées par le CST [REDACTED]
[REDACTED] réseaux d'information par lesquels les communications sont transmises.
46. Dans le contexte de [REDACTED] les éléments en transit ne correspondent pas nécessairement aux communications individuelles. Par exemple, lorsqu'il collecte [REDACTED] le CST choisit d'intervenir sur un seul élément en transit : [REDACTED]
[REDACTED]
[REDACTED] puis une fois traitée, elle est stockée en tant qu'élément en transit unique. En l'occurrence, un seul élément en transit peut contenir plusieurs, [REDACTED] de communications individuelles. Dans d'autres cas, la collecte et le traitement effectués par le CST pourraient ne produire qu'un seul [REDACTED] lequel ne contiendrait qu'une seule [REDACTED]
[REDACTED] se trouvant dans [REDACTED]
47. Compte tenu de l'importante diversité des technologies de communication sur lesquelles le CST mène [REDACTED]
[REDACTED] peuvent être difficiles à examiner selon les analystes. Pour faciliter le travail de ces analystes, le CST a conçu des systèmes de traitement secondaire [REDACTED]
[REDACTED]
[REDACTED] Ces systèmes de traitement secondaire peuvent être perfectionnés avec le temps, notamment, lorsque [REDACTED]
[REDACTED]
[REDACTED]

15(1) d)
15(1) f)

TRÈS SECRET // SI // RAC

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED] De cette façon, les analystes n'ont pas autant besoin

[REDACTED]

[REDACTED] ce qui leur permet de se concentrer davantage sur l'évaluation du RE et l'établissement de rapports connexes.

48. Vu l'architecture actuelle des systèmes SIGINT du CST, les éléments en transit [REDACTED] constituent le fondement des processus d'établissement de rapport et de conservation. Par exemple, lorsqu'il s'agit de produire des rapports concernant [REDACTED] le CST ajuste la période de conservation de l'élément en transit original, qui se trouve à être la base de données de [REDACTED]. Comme l'ajustement de la période de conservation a lieu au niveau de l'élément en transit, ce sont tous [REDACTED] de la base de données qui en viennent à être conservés pendant la période prolongée et non [REDACTED] [REDACTED] ayant fait l'objet du rapport.
49. Ces facteurs limitent les options dont disposent les analystes, lorsque ceux-ci ont affaire à de l'ICPC ou à de l'information collectée d'une façon qui est non conforme. Par exemple, lorsqu'une cible étrangère tient un échange [REDACTED] avec un Canadien, [REDACTED] de ce Canadien présentent un intérêt relatif à la vie privée de Canadiens, ce qui n'est pas le cas pour les communications avec un non-Canadien. Dans ce cas, le CST ne pourrait supprimer [REDACTED] présentant un intérêt pour la vie privée de Canadiens qu'en supprimant l'intégralité de la base de données [REDACTED] collectée sur [REDACTED] ciblé.
50. Cette situation pose clairement un dilemme pour le CST lorsqu'un même [REDACTED] peut contenir [REDACTED] [REDACTED] ayant une valeur de RE parallèlement à d'autres [REDACTED] qui présentent un intérêt relatif à la vie privée de Canadiens, mais qui n'ont aucune valeur de RE. Compte tenu des moyens dont il dispose actuellement, un analyste du CST ne pourrait conserver ces [REDACTED] ayant une valeur de RE qu'en conservant [REDACTED] présentant un intérêt relatif à la vie privée de Canadiens, mais n'ayant aucune valeur de RE.
51. Ce dilemme n'est pas qu'une simple hypothèse. En 2023, une équipe du renseignement du CST a fourni quelques informations concernant un incident qui pourrait avoir eu lieu au sein de l'équipe de conformité interne, laquelle est responsable de garantir l'observation des prescriptions de l'EPM. Ce qui est en cause, ce sont certains [REDACTED] collectés sur [REDACTED] dans le contexte d'une collecte [REDACTED] qui semblaient contenir de l'ICPC. Bien qu'en

15(1) d)

15(1) f)

TRÈS SECRET // SI // RAC

définitive, le CST ait jugé que la collecte était conforme, l'équipe du renseignement a soulevé ce même problème lors de discussions concernant de possibles solutions : lorsqu'elle a été avisée par l'équipe de la conformité que [REDACTED] contenant de l'ICPC avaient été annotés en vue d'être supprimés, l'équipe du renseignement a répondu que la seule façon de procéder serait de supprimer l'intégralité de la base de données contenant [REDACTED] collectés. Toutefois, ce faisant, on supprimerait d'autres [REDACTED] qui manifestement avaient une valeur de RE et qui n'auraient pas nécessité d'annotation s'ils avaient été collectés séparément.

52. Des représentants du CST ont invoqué des limites techniques lorsqu'on leur a demandé s'ils avaient envisagé des solutions concernant ce problème. Par exemple, le caractère fluctuant [REDACTED] peut poser problème lorsqu'il s'agit de convenablement diviser en ses parties une base de données remplie de [REDACTED] dans leur état actuel, les outils mis en place par le CST conservent l'intégralité de la base de données résultant de ce type de collecte en tant qu'élément en transit brut sur lequel se fondent ultérieurement toutes les mesures de traitement et d'analyse. Or, la décision de procéder ainsi n'est pas sans conséquences pour le CST. Rappelons que le CST a des responsabilités en matière de conservation, en particulier lorsque la conservation risque de poser problème (notamment l'intérêt d'un Canadien sur le plan de la vie privée de Canadiens). Ainsi, par cette approche, le CST pourrait conserver de l'information n'ayant aucune valeur de RE qui, en plus, pourrait présenter un intérêt relatif à la vie privée de Canadiens.
53. Bien qu'il fût immédiatement apparent dans [REDACTED] du CST, ce problème pourrait également se poser à ses autres programmes de collecte. Par exemple, le programme [REDACTED] du CST permet à celui-ci de collecter des transmissions passant par l'infrastructure [REDACTED]. Dans plusieurs cas, ces transmissions correspondent directement à des communications [REDACTED] notamment, [REDACTED]. Lorsque ces transmissions sont traitées en tant qu'éléments en transit, le CST est en mesure d'appliquer ses méthodes de conservation et de suppression avec une précision accrue. Ainsi, lorsqu'un message constitue en soi un élément en transit, le dilemme soulevé précédemment risque moins de se poser. Or, le programme [REDACTED] du CST n'est pas infaillible à cet égard; il pourrait donner lieu à [REDACTED]
[REDACTED]
[REDACTED]
- Ce type de situation susciterait le même genre de préoccupation.
54. Cette façon de traiter l'information n'est pas la seule option dont le CST dispose. Par exemple, le CST pourrait maintenir son approche actuelle quant au traitement

15(1) d)
15(1) f)

TRÈS SECRET // SI // RAC

des données collectées en tant qu'éléments en transit, mais il pourrait également incorporer un processus exceptionnel pouvant convertir l'information dérivée en éléments en transit, dans les situations où certains contenus ont une valeur, alors que d'autres contenus soulèvent des préoccupations sur le plan de la conformité. Ces éléments dérivés pourraient remplacer l'élément en transit original. Ainsi, lorsqu'il s'agit d'opter pour la conservation ou pour la suppression, la décision pourrait s'appuyer sur une information plus précise.

Recommandation 3. L'OSSNR recommande que le CST établisse un processus s'appliquant à la gestion des éléments en transit qui contiennent à la fois de l'information ayant une valeur sur le plan du renseignement étranger et de l'information qui doit être supprimée.

Problèmes relatifs aux politiques et aux pratiques en matière de SIGINT

Analystes du renseignement et décisions relatives au ciblage

Constatation 6. L'OSSNR constate qu'au CST, les analystes du renseignement ne cessent pas systématiquement de cibler [REDACTED] qui ne présentent plus d'intérêt en matière de renseignement étranger.

55. Les analystes du renseignement tiennent un rôle fondamental pour ce qui concerne la conservation des données SIGINT : ils reconnaissent les sélecteurs en vue de la collecte, évaluent les données collectées et prennent des décisions qui influent sur la conservation. À titre d'exemple, les analystes du renseignement sont chargés d'apposer les annotations et de signaler les incidents de non-conformité ayant trait à l'ICPC, ce qui a une incidence sur la conservation. Les besoins opérationnels en matière de renseignement ont aussi une influence sur les décisions stratégiques que le CST prend quant à la conservation. Il en va de même pour les priorités propres à chacune des équipes techniques qui conçoivent les outils devant servir à la conservation.
56. Les analystes du renseignement utilisent plusieurs outils et interagissent avec divers systèmes SIGINT de l'écosystème du CST, lesquels sont tous mis à jour régulièrement. Or, les fonctions de ces outils ne sont pas toujours documentées, et il peut arriver que la formation donnée soit plutôt informelle.
57. Lors de deux inspections, deux analystes du renseignement ont tenu pour acquis que le fait de marquer [REDACTED] comme ne présentant aucun intérêt sur le plan du RE serait suffisant pour empêcher toute collecte et tout stockage d'information

15(1) d)

15(1) f)

TRÈS SECRET // SI // RAC

provenant [REDACTED]. Toutefois, ce ne fut pas le cas, et [REDACTED] sont demeurés activement ciblés selon les paramètres des outils de ciblage du CST. Les deux incidents ont eu lieu à environ 18 mois d'intervalle. Ces interventions contrevenaient aux politiques de ciblage du CST, mais des mesures de protection techniques et procédurales ont empêché le CST de collecter de nouveaux contenus sur [REDACTED]. Aucun des sélecteurs ne semblait être lié à un Canadien ou à une personne se trouvant au Canada.

58. Lorsqu'on leur a demandé si leur organisation avait apporté quelques ajustements à son programme de formation destiné aux analystes, des représentants du CST ont indiqué qu'ils ne pouvaient pas témoigner des pratiques exercées dans chacune des équipes. En revanche, ils avaient modifié certains produits de communication pour rappeler aux analystes qu'après avoir utilisé la fonction permettant de marquer [REDACTED] comme ne présentant aucun intérêt sur le plan du RE, ils devaient également mettre à jour l'outil de ciblage de sorte à ne plus cibler [REDACTED] en question.

Recommandation 4. L'OSSNR recommande que le CST élabore des formations destinées au personnel ainsi que des mécanismes qui auront pour effet de stopper le ciblage [REDACTED] que les analystes du renseignement ont marqués comme ne présentant plus aucun intérêt sur le plan du renseignement étranger.

Conservation [REDACTED] des renseignements [REDACTED] [REDACTED]

Constatation 7. L'OSSNR constate que le CST a demandé et reçu une autorisation du Ministre lui permettant de conserver [REDACTED] l'information [REDACTED] [REDACTED] malgré le fait qu'il ne disposait d'aucun plan pour la mise en œuvre d'une capacité apte à conserver [REDACTED] ladite information.

Constatation 8. L'OSSNR constate que la politique du CST sur la conservation [REDACTED] de l'information [REDACTED] ne comportait aucune disposition exigeant que l'information soit périodiquement évaluée quant à sa valeur sur le plan du renseignement étranger.

59. La notion d'information [REDACTED] englobe un large éventail d'informations nominatives qui pourraient être associées à une cible du CST. Pensons, par exemple, [REDACTED]
[REDACTED]
[REDACTED] D'après le CST, cette information peut révéler des indices sur une cible légitime qui pourrait s'avérer déterminante pour l'accomplissement de son mandat.

15(1) d)

15(1) f)

TRÈS SECRET // SI // RAC

60. C'est en 2020 que le CST a introduit l'information [REDACTED] dans son calendrier de conservation en tant qu'information distincte. Il a été initialement établi que l'information [REDACTED] nécessitait une période de conservation de [REDACTED]
61. L'année suivante, le CST a assujéti l'information [REDACTED] à une période de conservation [REDACTED]
62. Ce changement a été autorisé en fonction du libellé qui a été introduit dans les demandes d'ARE que le CST a présentées en 2021, lequel fait valoir qu'au fil du temps, l'information [REDACTED] s'avérait particulièrement précieuse pour le CST. En l'occurrence, la requête visait à demander au Ministre [traduction] « l'autorisation de faire passer de [REDACTED] l'échéance de la période de conservation de cette information, tant que celle-ci a une valeur sur le plan du renseignement étranger ». D'ailleurs, cette dernière phrase a été répétée dans les demandes ultérieures sous la forme suivante : [traduction] « Pour ces raisons, le CST pourrait conserver cette information [REDACTED] tant que celle-ci est évaluée comme ayant une valeur sur le plan du renseignement étranger ». En outre, ce libellé est repris dans les autorisations du Ministre. Or, le recours à la formule [traduction] « tant que celle-ci est évaluée comme ayant [...] » invoque la nécessité de procéder à une réévaluation périodique de la valeur de renseignement étranger que ladite information peut avoir.
63. Toutefois, en réponse aux demandes d'information de l'OSSNR, le CST a indiqué, au sujet de la conservation [REDACTED] de cette information [traduction] « qu'il n'était pas nécessaire de vérifier [...] si les données étaient encore utiles ». Ainsi, dès lors qu'on juge qu'elle pourrait avoir une valeur de RE, l'information [REDACTED] pourrait même être conservée [REDACTED] [REDACTED] Outre le contenu du calendrier de conservation, la demande d'ARE ne contenait aucune information pouvant indiquer que le Ministre aurait été informé de l'interprétation selon laquelle aucun examen n'était requis. Le défaut d'ajouter cette exigence dans le calendrier de conservation est contraire au libellé [traduction] « tant que celle-ci est évaluée comme ayant [...] » qui fait partie de l'ARE.
64. Certes, cette conservation [REDACTED] est autorisée depuis 2021, mais le CST a indiqué à l'OSSNR qu'il ne se servait pas de cette autorisation. Lorsqu'on leur a demandé comment ils exerçaient concrètement la conservation [REDACTED] de l'information [REDACTED] des représentants du CST ont indiqué [traduction] « qu'ils n'avaient pas recours à des moyens automatisés de reconnaître ce type d'information [et que] les analystes du renseignement pouvaient repérer ce type d'information manuellement ». Ils ont également indiqué,

toutefois, que le CST ne disposait d'aucune politique ni d'aucun moyen technique pouvant permettre aux analystes de reconnaître l'information comme étant [REDACTED] et, par conséquent, d'en modifier la période de conservation. Vers la fin de 2024, les efforts devant aboutir à la mise en place de tels moyens techniques n'en étaient toujours qu'aux premières étapes, et ce, quelques années après que cette autorisation ait d'abord été demandée.

65. Cela remet en question la nécessité de l'inclure dans l'ARE. Or, les demandes d'ARE constituent le principal moyen par lequel le CST annonce au Ministre la nature des activités qu'il compte mener. En fait, les demandes donnent lieu aux documents dont le Ministre se sert pour déterminer s'il convient de délivrer une ARE et si ses conditions sont respectées. En l'absence de précisions dans les demandes d'ARE, il est difficile de savoir si ce que le Ministre autorise sera assurément mis en œuvre. Le CST pourrait renforcer la reddition de comptes à l'égard du Ministre en veillant à ce que ses demandes d'obtention de ce type d'autorisation correspondent exactement aux pratiques qu'il exerce. Le CST risque d'affaiblir sa reddition de compte en demandant répétitivement l'autorisation de mener des activités qu'il n'a pas l'intention d'exercer.
66. L'un des critères à respecter pour l'obtention d'une autorisation visée à l'article 33 est que le Ministre ait des motifs raisonnables de croire que l'information à acquérir au titre de l'autorisation ne sera pas conservée plus longtemps que ce qui est raisonnablement nécessaire. L'OSSNR considère que pour remplir cette condition, le CST doit disposer de moyens permettant de montrer régulièrement la nécessité de poursuivre la conservation de certaines informations [REDACTED]
[REDACTED]

Recommandation 5. L'OSSNR recommande que le CST veille à ce que les indications qu'il fournit dans ses demandes d'autorisation de renseignement étranger quant à la conservation de l'information [REDACTED] fassent précisément état des pratiques qu'il applique en matière de conservation. Lorsque le CST choisit de conserver [REDACTED] ce type d'information, il doit mettre en place un mécanisme garantissant que la conservation ne sera pas plus longue que raisonnablement nécessaire.

Données SIGINT stockées dans des systèmes périphériques

Constatation 9. L'OSSNR constate que le CST stocke des données SIGINT dans des systèmes et des outils qui ne sont pas soumis aux processus de suppression automatisés. En l'occurrence, c'est manuellement que les données sont supprimées, ce qui pose un risque de non-conformité.

TRÈS SECRET // SI // RAC

67. L'EPM-RE exige que les systèmes SIGINT suivent des principes d'intendance des données. Ces principes ont pour objet de veiller à ce que les mêmes exigences en matière de gouvernance continuent de s'appliquer aux données, lorsque celles-ci sont transférées entre les systèmes et entre les divers analystes.
68. La majeure partie des principaux systèmes SIGINT du CST disposent de fonctions automatisées grâce auxquelles les données sont traitées conformément à ces principes. Bien qu'il ait montré de rigoureuses pratiques de suppression dans ses systèmes de collecte, de traitement et d'analyse, le CST a tout de même reconnu le risque que les données supprimées des systèmes par les analystes ne soient pas automatiquement assujetties à des mesures de surveillance.
69. Par exemple, les analystes peuvent télécharger sur leur poste de travail les données SIGINT résultant d'une recherche pour en faire une analyse approfondie. Or, cette pratique donne lieu assez régulièrement à des incidents de non-conformité, dans la mesure où les analystes ou les équipes finissent par découvrir des copies locales de données qui sont arrivées au-delà de leur date limite de conservation. Bien que les données soient supprimées des systèmes centraux automatisés, il n'existe aucun mécanisme qui puisse automatiquement supprimer les copies enregistrées localement une fois qu'elles ont atteint leur date limite de conservation; pour les reconnaître et les supprimer, il faut avoir recours à des interventions manuelles.
70. De façon plus générale, les données SIGINT sont parfois traitées ou stockées dans des systèmes qui ne sont pas conçus pour répondre au cadre de gouvernance des données du CST. Ces systèmes périphériques comprennent des outils que le CST utilise pour gérer les projets et les processus, pour communiquer en interne ainsi qu'avec les organismes partenaires, et pour échanger des connaissances dans une optique de collaboration ou de mise en commun de pratiques exemplaires relatives aux projets, aux opérations, aux outils et aux processus.
71. Cette situation est compréhensible jusqu'à un certain point : dans l'exercice de leurs fonctions, les analystes peuvent très bien avoir besoin de copier localement des données à partir desquelles ils souhaitent développer et appliquer des outils ou pratiques novatrices en matière d'analyse. Ainsi, ils stimulent l'innovation, ce qui rend le SIGINT possible. Néanmoins, le CST, mais aussi chacun des analystes sont responsables des données qu'ils traitent et ils doivent veiller à ce que celles-ci soient gérées conformément aux principes d'intendance des données du CST.
72. Cela dit, le CST a mis en place certaines pratiques visant à atténuer le risque que des données soient stockées en dehors des systèmes dotés de mécanismes de suppression automatisés (« systèmes gérés ») :

TRÈS SECRET // SI // RAC

- Le CST continue de développer une trousse d'outils d'analyse plus complète pour ses systèmes gérés, de sorte à permettre aux analystes d'exécuter un nombre accru de leurs tâches sans avoir à recourir aux données copiées localement.
 - Lorsqu'ils en viennent à télécharger des données se trouvant dans les systèmes gérés, les analystes constatent que certains systèmes leur rappellent leur responsabilité quant à la gestion adéquate et à la suppression en temps opportun des copies qu'ils téléchargent localement.
73. Toutefois, l'EPM-RE du CST n'en dit que très peu sur les exigences particulières ou les pratiques de gestion des données que les analystes doivent observer lorsqu'ils traitent des données SIGINT en dehors des systèmes gérés. Il indique notamment que [traduction] « le calendrier de conservation doit s'appliquer à toutes les données SIGINT sans égard au support ou au lieu dans lequel ces données se trouvent ». Or, cette exigence est abordée dans une section consacrée aux « Systèmes SIGINT », ce qui crée de l'ambiguïté quant à savoir quelles exigences il convient de respecter lorsque les analystes travaillent en dehors des systèmes SIGINT.
74. Tout au long du présent examen, l'OSSNR a cherché à comprendre ce que le personnel du CST considérait comme étant des données SIGINT, et à savoir si les principes étaient bien communiqués et compris au sein des diverses équipes prenant part à la production du SIGINT.
75. L'OSSNR a vu que des sélecteurs et des identifiants étaient échangés par courriels avec des homologues du CST et que des données SIGINT étaient utilisées dans la plateforme de gestion de projets du CST. Dans tous les cas observés, il y avait des motifs valables pour justifier que les données soient traitées dans ces systèmes périphériques. Toutefois, ces activités contrevenaient au cadre de gouvernance des données du CST et ne faisaient pas appel à des moyens automatisés de traitement des données, alors que le personnel du CST – en raison des ambiguïtés soulevées précédemment – pourrait ne pas avoir toujours été au fait des exigences permettant de veiller à ce que les données stockées dans ces systèmes soient supprimées au terme de la période de conservation applicable.
76. Cette pratique pourrait s'étendre à l'utilisation, par le CST, des outils de collaboration de la Collectivité des cinq. Or, le CST ne semblait pas avoir une connaissance étendue de la façon dont son personnel utilise ces outils. Lorsqu'on les a interrogés au sujet des pratiques d'audit que le CST avait mis en place pour ces outils, des représentants du CST ont indiqué qu'ils [traduction] « n'étaient pas en mesure de les auditer », mais croyaient que ces outils étaient audités par le

TRÈS SECRET // SI // RAC

partenaire de la Collectivité des cinq. Ils s'attendaient donc à collaborer avec leur partenaire de la Collectivité des cinq lorsqu'il s'agirait d'auditer un incident, le cas échéant.

77. Ces systèmes périphériques remplissent une fonction importante : compte tenu de la vitesse à laquelle les technologies et les pratiques SIGINT évoluent, le personnel du CST doit demeurer souple dans la façon dont il utilise les données collectées et dans ses initiatives de collaboration en interne et à l'externe. Toutefois, la conservation de données dans des systèmes périphériques peut poser et pose effectivement des risques de non-conformité. Le CST devrait donc veiller à ce que ses politiques prennent en compte la gestion et la conservation des données SIGINT dans tous les environnements.

Recommandation 6. L'OSSNR recommande que le CST mette à jour son Ensemble de politiques relatives à la mission de sorte à éliminer les ambiguïtés concernant les données SIGINT stockées dans des systèmes périphériques et fournisse des directives permettant de garantir la conformité aux exigences en matière de conservation.

Outils et données SIGINT mis à la disposition des partenaires de la Collectivité des cinq

Constatation 10. L'OSSNR constate qu'en communiquant des données SIGINT à d'autres organismes, notamment les partenaires de la Collectivité des cinq, le CST limite sa capacité de veiller à ce que la conservation de ces données réponde aux stipulations de ses propres politiques.

78. Le partenariat avec la Collectivité des cinq a permis de réaliser d'importants progrès dans le développement des technologies qui sont essentielles à la production du SIGINT. Il convient de rappeler que les systèmes du CST sont complexes et répartis au sein de plusieurs équipes responsables de la production du SIGINT. Certains des systèmes que le CST utilise – de la collecte des données jusqu'à l'étape de la conservation – proviennent de partenaires de la Collectivité des cinq ou résultent de la collaboration entre le CST et certains de ces partenaires.
79. L'intégration soutenue qui se réalise entre les membres de la Collectivité des cinq a permis au CST d'utiliser des outils qu'il lui serait difficile, voire impossible de créer lui-même. Ainsi, le CST tire certainement avantage de cet accès aux experts techniques et aux développeurs de logiciels de la Collectivité des cinq. Toutefois, cette intégration a un effet direct sur la capacité du CST à remplir les obligations stipulées dans les politiques relativement à la conservation des données SIGINT. Le CST a indiqué qu'il devait lui-même développer et tenir à jour certaines

15(1) d)

15(1) f)

TRÈS SECRET // SI // RAC

[REDACTED] par un partenaire de la collectivité des cinq, de sorte à garantir leur conformité aux exigences canadiennes en matière de conservation.

80. Le partenariat compte sur de solides mécanismes d'échange d'information et d'intégration opérationnelle. Le CST peut [REDACTED] [REDACTED] directement d'organismes partenaires de la Collectivité des cinq, demandes qui sont pourtant assujetties aux mêmes critères que ceux imposés aux analystes du renseignement du CST. Certaines données SIGINT [REDACTED] peuvent également être communiquées [REDACTED] et dès leur collecte avec les partenaires du CST faisant partie de la Collectivité des cinq. Or, le présent examen n'a pas prévu d'évaluer en profondeur ces pratiques [REDACTED] et d'échange. Par contre, il a été l'occasion d'examiner certains des effets que les échanges de données SIGINT peuvent avoir sur la conservation.
81. Selon le CST, lorsqu'elles sont traitées par des fonctions automatisées, les données SIGINT qu'il collecte s'accompagnent d'identifiants créés par le CST, mais conformes au format utilisé par les partenaires de la Collectivité des cinq, lequel comprend la date à laquelle les données devront être supprimées. Toujours d'après le CST, lorsque les partenaires reçoivent les données du CST, c'est la plus courte des périodes de conservation – celle prévue par le CST ou celle prévue par le partenaire – qui est appliquée aux données une fois qu'elles se trouvent dans les systèmes dudit partenaire. Certes, ces identifiants permettent aux partenaires de supprimer les données communiquées conformément au calendrier de conservation du CST, mais la création de plusieurs copies de données en dehors des systèmes appartenant au CST donne lieu, en soi, à une diminution du contrôle que le CST est en mesure d'exercer sur la conservation des données.
82. Cet échange automatisé rend plus difficile l'élimination des éléments en transit qui sont non conformes, notamment les données acquises après avoir accidentellement ciblé un Canadien, puisqu'ainsi, le CST doit également demander à l'homologue qui a reçu l'information de procéder, à son tour, à l'élimination des données enregistrées dans ses systèmes. Le CST pourrait très bien recevoir, de la part du partenaire, un avis confirmant que l'élimination a eu lieu – et l'OSSNR a vu des preuves de l'envoi de ce type d'avis pendant son examen –, mais il n'aura jamais la certitude que l'information a été complètement détruite, puisqu'il n'est pas en mesure de voir le contenu des systèmes du partenaire en question.
83. Le CST a récemment mis en place un nouveau mécanisme s'appliquant aux échanges de certaines des données qu'il a collectées (« requêtes en place »). Ce mécanisme permet aux analystes de la Collectivité des cinq d'obtenir des données se trouvant dans les fonds d'information du CST moyennant une raison valable. Il permet également au CST de savoir qui consulte et recueille les données, veillant

TRÈS SECRET // SI // RAC

ainsi à ce que les accès à l'information soient conformes aux politiques du CST. Ce mécanisme n'élimine pas entièrement les problèmes cités précédemment : si le CST jugeait que certaines données dussent être éliminées, il devrait tout de même demander que l'organisme partenaire élimine lui-même lesdites données. Comparativement à la communication automatisée, que le CST continue d'utiliser pour certaines données, cette mesure réduit le volume de données communiquées, ce qui pourrait diminuer la probabilité que des problèmes surviennent.

4. Conclusion

84. Compte tenu des divers besoins opérationnels en matière de collecte SIGINT – lesquels changent constamment et peuvent être difficiles à anticiper –, le CST doit miser sur les données pour accomplir sa mission, mais doit composer avec d'importantes contraintes s'appliquant à la conservation des données collectées. L'engagement du CST à respecter les exigences applicables à la conservation des données était manifeste, particulièrement dans la gestion et la protection de l'ICPC.
85. Bien que cet engagement soit notable et authentique, le CST a affiché des lacunes pour ce qui a trait à sa conservation des données SIGINT, comme en témoigne le présent rapport. Mais ce qu'il faut noter, c'est que le CST ne dispose pas de mécanismes permettant de supprimer certaines informations qui se rapportent à des non-Canadiens, mais qui n'ont aucune valeur de RE. Lors de ses inspections, l'OSSNR a constaté que le CST avait conservé de l'information collectée se rapportant à des non-Canadiens, dont on avait pourtant établi qu'elle n'avait aucune valeur de RE. En agissant de la sorte, le CST pourrait ne s'être pas conformé aux stipulations de l'*Autorisation de renseignement étranger pour les opérations réseau*. D'un point de vue plus général, l'absence de tels mécanismes pourrait amener le CST à conserver ce type d'information plus longtemps qu'il n'est raisonnablement nécessaire.
86. Le CST doit continuer de prioriser la conservation des données, lorsqu'il conçoit et met en œuvre ses politiques, ses processus, ses systèmes et la formation de son personnel. La loi sur le CST exige que les données SIGINT ne soient pas conservées plus qu'il n'est raisonnablement nécessaire. Cette prescription soit se refléter dans les principes et pratiques qui sous-tendent les opérations du CST.

15(1) d)
15(1) f)

TRÈS SECRET // SI // RAC

Annexe A. Calendrier de conservation des données SIGINT

L'EPM-RE propose le calendrier de conservation des données suivant.

Type	Conservation	Commentaire
Si le contenu de l'information sélectionnée présente un intérêt relatif à la vie privée d'un Canadien et est jugé essentiel aux affaires internationales, à la sécurité et à la cybersécurité, alors :		
██████████ ██████████ ██████████ ██████████	██████████ ██████████ ██████████ ██████████	Une fois l'information repérée, les analystes doivent appliquer, tel qu'il est exigé, les annotations relatives à la vie privée et conserver dans des contenants sécurisés tout matériel ayant été utilisé dans des produits finis. La conservation des communications protégées par le secret professionnel de l'avocat nécessite l'approbation du Ministre.
Si le contenu de l'information sélectionnée présente un intérêt relatif à la vie privée d'un Canadien et est jugé non essentiel aux affaires internationales, à la sécurité et à la cybersécurité, alors :		
██████████ ██████████	██████████ ██████████	Une fois l'information repérée dans les bases de données de contenus, les analystes doivent appliquer, tel qu'il est exigé, les annotations relatives à la suppression du matériel; le contenu sera automatiquement supprimé des bases de données de contenus après ██████████
Si le contenu de l'information sélectionnée est reconnu comme étant canadien aux ██████████ alors :		
██████████ ██████████	Aucune conservation permise	Une fois l'information repérée, les analystes doivent marquer ces communications en vue de leur suppression, et l'équipe de l'assurance des données doit être avisée pour qu'elle puisse procéder à un examen des sélecteurs concernés, puis à l'élimination des données.
Pour toutes les autres données et pour les communications ne présentant aucun intérêt relatif à la vie privée d'un Canadien :		
██████████ ██████████ ██████████ ██████████ ██████████	██████████	S.O.

15(1) d)
15(1) f)

TRÈS SECRET // SI // RAC

Type	Conservation	Commentaire
[REDACTED] [REDACTED] [REDACTED] [REDACTED]		
[REDACTED] [REDACTED] [REDACTED] [REDACTED]	[REDACTED]	S.O.
[REDACTED] [REDACTED] [REDACTED] [REDACTED]	[REDACTED]	S.O.
[REDACTED] [REDACTED] [REDACTED] [REDACTED]	[REDACTED]	
Chiffrement Déchiffrement	[REDACTED]	Une fois qu'elle est accessible, l'information est assujettie aux normes de conservation énoncées dans le calendrier.
[REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]	[REDACTED]	L'information peut être conservée [REDACTED] [REDACTED] Le responsable de cette information devrait mener périodiquement une revalidation du besoin de conserver. Si l'information est [REDACTED] période de conservation [REDACTED] [REDACTED] les mesures suivantes s'appliquent : • évaluée comme étant du RE selon les priorités en vigueur et marquée aux fins d'utilisation et de conservation; • évaluée comme n'ayant aucune valeur de RE et marquée aux fins de suppression, sauf si une autorisation prévoit d'autres mesures.
[REDACTED] [REDACTED]	[REDACTED]	L'information [REDACTED] [REDACTED] peut être conservée [REDACTED].

15(1) d)
15(1) f)

TRÈS SECRET // SI // RAC

Type	Conservation	Commentaire
[REDACTED] [REDACTED]	[REDACTED]	[REDACTED] [REDACTED] [REDACTED] peuvent être conservées [REDACTED] Ces données comprennent l'information [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]
[REDACTED] [REDACTED] [REDACTED]	[REDACTED] [REDACTED]	L'information sera conservée pendant une période d'au plus [REDACTED] débutant le jour où l'information a d'abord été acquise. Après cette période de [REDACTED] l'information sera automatiquement supprimée, à moins qu'il soit établi que [REDACTED] [REDACTED] présente un intérêt sur le plan du renseignement étranger.
[REDACTED] [REDACTED] [REDACTED] [REDACTED]	[REDACTED]	Il s'agit d'information non sélectionnée acquise [REDACTED] [REDACTED] L'information sera conservée pendant une période d'au plus [REDACTED] débutant le jour où l'information a d'abord été acquise. Une autorisation ministérielle est requise pour conserver l'information au-delà de [REDACTED]

15(1) d)
15(1) f)

TRÈS SECRET // SI // RAC

Annexe B.Synthèse des inspections techniques

L'OSSNR a sélectionné les quatre ensembles de données devant subir une inspection en procédant ainsi.

- Demande d'une liste [REDACTED] les ensembles de données [REDACTED] collectés au moyen [REDACTED] activé par une capacité [REDACTED] particulière.
- Réception d'une liste de 321 ensembles de données. Pour chacun des ensembles de données, la liste fournissait divers renseignements : [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
- Filtrage de la liste des ensembles de données suivant l'application d'un certain nombre de critères, notamment la probabilité de trouver de l'ICPC et la récence des données. Pour vérifier la description fournie par le CST quant au processus d'élimination, l'OSSNR a inclus, dans cette liste filtrée, un ensemble de données éliminé.

Chacune des quatre inspections a permis à l'OSSNR d'observer les aspects propres à la collecte du SIGINT et à la chaîne de conservation.

1. L'inspection 1 avait pour objet d'examiner l'ensemble de données [REDACTED] qu'un analyste [REDACTED] avait ciblé et évalué [REDACTED]. La cible a été trouvée par [REDACTED] effectuée au moyen d'outils du CST et de la Collectivité des cinq. On a évalué les données SIGINT collectées, et il a été établi que [REDACTED] n'appartenait pas à la cible recherchée. En conséquence, l'information n'avait aucune valeur de renseignement étranger (RE). Ainsi, dans l'outil [REDACTED] du CST, l'analyste lui a appliqué la mention indiquant qu'elle n'était d'aucun intérêt sur le plan du RE, de sorte à empêcher d'autres analystes de la cibler. Collectées en [REDACTED] les données étaient toujours dans les fonds d'information du CST au moment de l'inspection réalisée en septembre 2024, et leur suppression n'était pas prévue avant leur date de péremption fixée en [REDACTED].
2. L'inspection 2 avait pour objet d'examiner l'ensemble de données [REDACTED] qu'un analyste [REDACTED] du CST avait ciblé et évalué [REDACTED]. L'analyste a identifié la cible à partir [REDACTED]. Il a évalué les données SIGINT collectées et a indiqué que [REDACTED].

15(1) d)
15(1) f)

TRÈS SECRET // SI // RAC

[REDACTED] mais n'a trouvé aucun autre indicateur de lien avec un Canadien. Pendant la recherche de ces indicateurs, il a également estimé que l'information n'avait aucune valeur de RE. Ainsi, après consultation auprès de l'équipe de la conformité du CST, l'analyste a attribué [REDACTED] une marque signifiant qu'il présentait un intérêt relativement à la vie privée d'un Canadien [traduction] « par mesure d'extrême prudence ». Cette situation a donné lieu à une procédure d'élimination. Collectées en [REDACTED] les données ont été éliminées du système quelques jours plus tard, pendant le même mois, ce qui a été confirmé pendant l'inspection menée en septembre 2024.

3. L'inspection 3 avait pour objet d'examiner l'ensemble de données [REDACTED] qu'un analyste [REDACTED] du CST avait ciblé et évalué

[REDACTED] L'analyste avait identifié la cible à partir [REDACTED] Il a évalué les données SIGINT collectées, puis il a confirmé qu'elles correspondaient à l'ensemble de cibles désiré et que l'information avait une valeur sur le plan du RE. L'analyste a ciblé de nouveau [REDACTED] à plusieurs reprises pour collecter de plus amples informations ayant une valeur de RE. Collectées de [REDACTED] [REDACTED] les données étaient toujours dans le fonds d'information du CST au moment de l'inspection réalisée en octobre 2024, et leur suppression n'était pas prévue avant leur date de péremption fixée en [REDACTED]. [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

4. L'inspection 4 avait pour objet d'examiner l'ensemble de données [REDACTED] que le même analyste [REDACTED] (voir inspection 2) avait ciblé et évalué [REDACTED] La cible a été identifiée à partir des mêmes critères que ceux employés pour la cible dont il est question dans le cas de l'inspection 2. On a évalué les données SIGINT collectées, et il a été établi que [REDACTED] n'appartenait pas à la cible recherchée. Ainsi, l'information n'avait aucune valeur sur le plan du RE, comme il a été noté lors de l'inspection 2. Toutefois, contrairement à ce qui a été constaté lors de cette inspection 2, il n'y avait rien qui puisse établir un lien avec un Canadien. Par conséquent, l'analyste ne pouvait ni supprimer ni éliminer lesdites données. Ainsi, dans [REDACTED] de données du CST, l'analyste a plutôt appliqué la mention indiquant que l'information ne présentait aucun intérêt sur le plan du RE, de sorte à empêcher d'autres analystes de la cibler, semblablement à ce qui a été constaté lors de l'inspection 1. Collectées en [REDACTED] les données étaient toujours dans le fonds d'information du CST lors de l'inspection réalisée en

15(1) d)
15(1) f)

TRÈS SECRET // SI // RAC

octobre 2024, et leur suppression n'était pas prévue avant leur date de péremption fixée en [REDACTED]

Pendant sa préparation en vue des premières inspections, le CST a identifié un incident de non-conformité pour chacun des deux cas visés.

1. Lors de l'inspection 1, l'analyste tenait pour acquis que le fait de marquer [REDACTED] [REDACTED] comme ne présentant aucun intérêt sur le plan du RE dans un système désactiverait automatiquement le ciblage dans tous les autres systèmes. Or, tel ne fut pas le cas, et [REDACTED] a continué d'apparaître comme étant ciblé dans l'outil de ciblage du CST. Bien qu'il s'agisse là d'une atteinte aux politiques de ciblage du CST, un certain nombre de mesures de protection de nature technique et procédurale ont empêché que le CST prélève de nouvelles informations [REDACTED] – comme pour [REDACTED] [REDACTED] portant la même marque. Pour résoudre ce problème, le CST a retiré [REDACTED] du répertoire des cibles, et ce, dans tous les systèmes.
2. Lors de l'inspection 2, un faible nombre de transmissions ont été reçues de la part [REDACTED] après que la demande d'élimination a été présentée. Or, ces transmissions provenaient [REDACTED] [REDACTED]. Ainsi, comme elles ne contenaient aucune information, ces transmissions ne contenaient aucune donnée [REDACTED]. En raison d'une erreur administrative involontaire, les analystes de l'assurance des données du CST n'ont éliminé que les données recueillies jusqu'à la dernière date de collecte connue. Or, comme elles ont été reçues après cette date, ces transmissions n'ont pas été éliminées. Ces données sont demeurées dans le système jusqu'à ce que le CST se prépare en vue de l'inspection. C'est à ce moment que le CST a enregistré l'incident, pour ensuite éliminer lesdites données en [REDACTED].

Pendant les inspections, le CST a communiqué de plus amples informations sur l'incident, notamment sur la façon dont les intervenants du CST ont résolu le problème et sur les mesures qu'ils avaient appliquées ou envisageaient d'appliquer dans le but de prévenir toute récurrence du problème.

TRÈS SECRET // SI // RAC

Annexe C. Constatations et recommandations

Dans le cadre du présent examen, l'OSSNR a formulé les constatations et les recommandations suivantes.

Gestion de l'information canadienne

Constatation 1. L'OSSNR constate que le CST a mis en place des mesures de protection de la vie privée des Canadiens et des personnes se trouvant au Canada dans les systèmes de conservation, les fonctions et les outils appelés à traiter les données SIGINT.

Information sans valeur sur le plan du renseignement étranger

Constatation 2. L'OSSNR constate que le calendrier dont le CST se sert pour la conservation du renseignement étranger ne tient pas compte de l'information sur les non-Canadiens qui n'a aucune valeur sur le plan du renseignement étranger.

Constatation 3. L'OSSNR constate que le CST ne dispose pas de mécanismes aptes à supprimer certaines informations relatives à des non-Canadiens qui n'ont aucune valeur sur le plan du renseignement étranger, ce qui pose le risque que le CST conserve ces informations plus longtemps qu'il n'est raisonnablement nécessaire.

Constatation 4. L'OSSNR constate que le CST a conservé de l'information sur des non-Canadiens, malgré qu'il ait été établi que cette information n'avait aucune valeur sur le plan du renseignement étranger. Cette conservation pourrait ne pas être conforme aux stipulations de l'*Autorisation de renseignement étranger pour les opérations réseau* délivrée au titre de l'article 26 de la Loi sur le CST.

Recommandation 1. L'OSSNR recommande que le CST supprime immédiatement les données qui ont été jugées comme n'ayant aucune valeur sur le plan du renseignement étranger dans le contexte des inspections 1 et 4 dans la mesure où la conservation de ces données n'est pas raisonnablement nécessaire.

Recommandation 2. L'OSSNR recommande que le CST modifie son Ensemble de politiques relatives à la mission en créant une catégorie pour l'information sur un non-Canadien reconnue comme n'ayant aucune valeur sur le plan du renseignement étranger, et qu'il fixe une échéance pour sa suppression de sorte qu'elle ne soit pas conservée plus longtemps qu'il n'est raisonnablement nécessaire.

15(1) d)

15(1) f)

TRÈS SECRET // SI // RAC

Constatation 5. L'OSSNR constate que l'approche choisie par le CST consistant à traiter certains types de données SIGINT en tant « qu'éléments en transit » – alors que plusieurs communications distinctes peuvent parfois être groupées dans un seul élément – pourrait donner lieu à la conservation d'information n'ayant aucune valeur sur le plan du renseignement étranger.

Recommandation 3. L'OSSNR recommande que le CST établisse un processus s'appliquant à la gestion des éléments en transit qui contiennent à la fois de l'information ayant une valeur sur le plan du renseignement étranger et de l'information qui doit être supprimée.

Problèmes relatifs aux politiques et aux pratiques en matière de SIGINT

Analystes du renseignement et décisions relatives au ciblage

Constatation 6. L'OSSNR constate qu'au CST, les analystes du renseignement ne cessent pas systématiquement de cibler [REDACTED] qui ne présentent plus d'intérêt en matière de renseignement étranger.

Recommandation 4. L'OSSNR recommande que le CST élabore des formations destinées au personnel ainsi que des mécanismes qui auront pour effet de stopper le ciblage [REDACTED] que les analystes du renseignement ont marqués comme ne présentant plus aucun intérêt sur le plan du renseignement étranger.

Conservation [REDACTED] des renseignements [REDACTED] [REDACTED]

Constatation 7. L'OSSNR constate que le CST a demandé et reçu une autorisation du Ministre lui permettant de conserver [REDACTED] l'information [REDACTED] [REDACTED] malgré le fait qu'il ne disposait d'aucun plan pour la mise en œuvre d'une capacité apte à conserver [REDACTED] ladite information.

Constatation 8. L'OSSNR constate que la politique du CST sur la conservation [REDACTED] de l'information [REDACTED] ne comportait aucune disposition exigeant que l'information soit périodiquement évaluée quant à sa valeur sur le plan du renseignement étranger.

Recommandation 5. L'OSSNR recommande que le CST veille à ce que les indications qu'il fournit dans ses demandes d'autorisation de renseignement étranger quant à la conservation de l'information [REDACTED] fassent précisément état des pratiques qu'il applique en matière de conservation. Lorsque le CST choisit de conserver [REDACTED] ce type d'information, il doit mettre en place un mécanisme

TRÈS SECRET // SI // RAC

garantissant que la conservation ne sera pas plus longue que raisonnablement nécessaire.

Données SIGINT stockées dans des systèmes périphériques

Constatation 9. L'OSSNR constate que le CST stocke des données SIGINT dans des systèmes et des outils qui ne sont pas soumis aux processus de suppression automatisés. En l'occurrence, c'est manuellement que les données sont supprimées, ce qui pose un risque de non-conformité.

Recommandation 6. L'OSSNR recommande que le CST mette à jour son Ensemble de politiques relatives à la mission de sorte à éliminer les ambiguïtés concernant les données SIGINT stockées dans des systèmes périphériques et fournisse des directives permettant de garantir la conformité aux exigences en matière de conservation.

Outils et données SIGINT mis à la disposition des partenaires de la Collectivité des cinq

Constatation 10. L'OSSNR constate qu'en communiquant des données SIGINT à d'autres organismes, notamment les partenaires de la Collectivité des cinq, le CST limite sa capacité de veiller à ce que la conservation de ces données réponde aux stipulations de ses propres politiques.