National Security and Intelligence Review Agency

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

~~TRÈS SECRET//SI//CEO//SECRET PROFESSIONNEL DE L'AVOCAT~~

EXAMEN DES PRATIQUES D'ÉCHANGE D'INFORMATIONS ENTRE DIVERS VOLETS DU MANDAT DU CST

(EXAMEN DE L'OSSNR N^{O} 2020-07)

Le présent rapport présente une légère modification par rapport à la version finale qui a été soumise au Ministre. En effet, une erreur de formulation s'était glissée dans l'énoncé de la conclusion n^{o} 4, donnant lieu à deux libellés différents dans le rapport et dans le sommaire. Une correction a donc été apportée aux fins de publication. Précisions que le libellé exact a toujours été présent dans le corps du rapport final et qu'en définitive, le libellé erroné a été remplacé par le bon libellé aux fins de publication.

C.P. 2430, Succursale D
Ottawa, Canada K1P 5W5
Tél. : 1-833-890-0293 Téléc. : 613-907-4445

I SOMMAIRE

1. (NC) Le présent examen avait pour objet d'analyser les fondements juridiques suivant lesquels le Centre de la sécurité des télécommunications (CST) est en mesure de communiquer des informations obtenues par l'un des volets de son mandat à un autre des volets du même mandat. L'examen s'est donc concentré sur les pratiques d'échange d'informations à l'intérieur du CST, plus précisément entre, d'une part, le volet axé sur le renseignement étranger (RE) et, d'autre part, le volet axé sur la cybersécurité et l'assurance de l'information (cybersécurité).

2. (NC) L'OSSNR a vérifié si les échanges internes d'informations se rapportant à un Canadien ou à une personne se trouvant au Canada (ICPC) effectués par le CST étaient conformes aux dispositions de la *Loi sur la protection des renseignements personnels*, qui impose aux institutions fédérales des restrictions sur l'utilisation des renseignements personnels obtenus par voie de collecte, mais aussi de la *Loi sur le CST*, qui encadre les ICPC collectées de manière incidente et leur utilisation par le CST. Considérant les descriptions que les articles 16 et 17 de la *Loi sur le CST* fournissent concernant les volets, l'OSSNR constate qu'il peut arriver que des informations collectées par l'un des volets soient utilisées par un autre volet pour des fins semblables ou autrement justifiables. En l'occurrence, il semble bien que les exigences de la *Loi sur la protection des renseignements personnels* en matière d'échange interne soient respectées. Toutefois, il convient de garder une certaine réserve dans la mesure où les volets énoncés dans la *Loi sur le CST* diffèrent les uns des autres. En effet, le CST est tenu de procéder, dans chacun des cas, à une analyse de la conformité visant à étudier l'objet de la collecte et des échanges envisagés.

3. (NC) L'OSSNR estime qu'il est nécessaire que toute demande d'autorisation ministérielle présentée par le chef du CST informe le ministre concernant la façon dont les ICPC pourraient être utilisées par le CST – ce qui comprend l'éventualité d'une communication des ICPC à un autre volet – et les objectifs visés. Hormis une seule exception, les demandes présentées par le chef pendant la période d'examen informaient adéquatement le ministre de la Défense nationale concernant la façon dont les ICPC pourraient être utilisées en guise d'appui à un autre volet. Qui plus est, les demandes en matière de renseignement étranger fournissaient au ministre les informations appropriées quant à la façon dont le CST avait évalué le caractère essentiel (ou l'essentialité) servant à justifier la collecte d'ICPC dans le cadre du volet RE.

4. (NC) La politique du CST indique qu'une évaluation de la pertinence, de l'essentialité ou de la nécessité des ICPC pour chacun des volets est requise avant que des informations puissent être retransmises entre lesdits volets. En outre, la politique du CST fournit des définitions ainsi que des critères d'évaluation et d'application des balises s'appliquant aux informations. Au reste, l'OSSNR est d'avis que le cadre stratégique du CST régissant la communication interne d'informations entre les volets cybersécurité et renseignement étranger du mandat est conforme aux dispositions de la *Loi sur le CST.*

5. (NC) Les informations fournies par le CST n'ont pas été l'objet d'une vérification indépendante de la part de l'OSSNR. Or, des travaux sont en cours dans le but de préparer des politiques opérantes et des pratiques exemplaires devant s'appliquer aux vérifications indépendantes de divers types d'informations selon une approche axée sur la confiance, mais aussi sur la prudence, qui répond à l'engagement de l'OSSNR.

II FONDEMENT LÉGISLATIF

1. (NC) Le présent examen a été réalisé conformément aux dispositions énoncées à 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*).

III INTRODUCTION

2. (NC) Le présent examen avait pour objet d'analyser les fondements juridiques suivant lesquels le Centre de la sécurité des télécommunications (CST) est en mesure de communiquer des informations obtenues par l'un des volets de son mandat à un autre des volets du même mandat. L'examen s'est donc concentré sur les pratiques d'échange d'informations à l'intérieur du CST[1], plus précisément entre, d'une part, le volet axé sur le renseignement étranger (RE) et, d'autre part, le volet axé sur la cybersécurité et l'assurance de l'information (cybersécurité). De plus, le présent examen avait pour objectif de recenser les activités ayant trait à la communication en interne d'informations se rapportant à un Canadien ou à une personne se trouvant au Canada, plus particulièrement entre les volets « cybersécurité » et « renseignement étranger ». En l'occurrence, cette démarche avait pour objet d'alimenter les examens que l'OSSNR serait ultérieurement appelé à réaliser.

3. (~~TS~~) Le Bureau du commissaire du Centre de la sécurité des télécommunications (BCCST) avait déjà étudié les modalités d'échange et d'accès s'appliquant aux informations sur les cybermenaces échangées entre la Direction du SIGINT et la Direction de la Sécurité des TI du CST[2]. L'examen du BCCST avait alors conclu que les activités d'échange d'informations sur les cybermenaces qui avaient eu lieu entre le SIGINT et la Sécurité des TI du CST avaient été conformes aux exigences énoncées dans la *Loi sur la défense nationale* et dans la *Loi sur la protection des renseignements personnels*. L'examen a également indiqué que les informations échangées entre les deux directions n'avaient posé qu'un risque faible pour la vie privée des Canadiens[3].

4. (NC) Avec l'entrée en vigueur de la *Loi sur le CST*, le 1er août 2019, les fondements juridiques sur lesquels s'appuient les activités du CST ont subi des modifications dans la foulée de l'examen du BCCST. En considération des modifications apportées à ces fondements juridiques, l'OSSNR a amorcé une nouvelle évaluation visant à établir si les activités internes d'échange d'informations entre les volets cybersécurité et renseignement étranger du CST étaient toujours conformes aux dispositions de la *Loi sur le CST* et de la *Loi sur la protection des renseignements personnels.*

5. (NC) D'emblée, l'OSSNR s'attend à ce que les échanges internes d'ICPC effectués au sein du CST répondent aux exigences de la *Loi sur le CST* et de la *Loi sur la protection des renseignements personnels*. Le présent examen a donc mis l'accent sur l'analyse des fondements juridiques permettant au CST de procéder à des échanges d'ICPC entre les volets cybersécurité et renseignement étranger.

---

[1] Le CST estime que les données collectées en vertu de l'un des volets, puis communiquées à un autre volet sont réservées à une utilisation interne (la question est discutée plus avant dans la présente, à la section intitulée Conformité aux dispositions de la *Loi sur le CST* et de la *Loi sur la protection des renseignements personnels*). Toutefois, par souci de clarté, le présent examen emploiera le terme « échange interne » pour désigner toute utilisation ou divulgation d'informations ayant lieu entre les volets cybersécurité et renseignement étranger.

[2] BCCST, *Étude de l'accès à l'information sur les cybermenaces et de l'échange entre les programmes de renseignements électromagnétiques et de sécurité des technologies de l'information du CST, 2016-2017.*

[3] BCCST, lettre au ministre de la Défense nationale, 24 février 2017.

6. (NC) La *Loi sur le Centre de la sécurité des télécommunications* (*Loi sur le CST*) divise le mandat du CST en cinq volets distincts[4]. En l'occurrence, la *Loi sur le CST* établit des distinctions entre les volets, notamment, sur le plan des objectifs et des activités. Voici donc un aperçu de ces distinctions :

- Renseignement étranger (RE) (article 16) : acquérir de l'information à partir de l'infrastructure mondiale de l'information (IMI)[5] et utiliser, analyser et diffuser l'information dans le but de fournir des renseignements étrangers.

- Cybersécurité et assurance de l'information (cybersécurité) (article 17) : fournir des avis, des conseils et des services afin d'aider à protéger l'information électronique et les infrastructures de l'information des institutions fédérales ou celles désignées par le paragraphe 21(1) de la *Loi sur le CST*, mais aussi acquérir, utiliser et analyser l'information de sorte à renforcer la protection de cette information électronique et de ces infrastructures.

- Cyberopérations défensives (article 18) : mener, dans l'infrastructure mondiale de l'information, des activités ayant pour but de protéger l'information électronique de même que les infrastructures de l'information des institutions fédérales ou celles désignées au paragraphe 21(1) de la *Loi sur le CST.*

- Cyberopérations actives (article 19) : mener des activités dans l'infrastructure mondiale de l'information visant à réduire, à interrompre, à influencer ou à contrecarrer, selon le cas, les capacités, les intentions ou les activités d'entités étrangères.

- Assistance technique et opérationnelle (article 20) : fournir une assistance technique et opérationnelle aux organismes chargés de l'application de la loi et de la sécurité, aux Forces canadiennes et au ministère de la Défense nationale.

7. (NC) De plus, la *Loi sur le CST* établit des distinctions entre les volets en exigeant aussi l'obtention d'autorisations ministérielles (AM) pour les diverses activités du CST, sauf dans les contextes où celui-ci prête son assistance (art 20)[6]. En outre, exception faite des activités d'assistance, la *Loi sur le CST* stipule que les activités du CST ne peuvent viser des Canadiens ou des personnes se trouvant au Canada et ne peuvent porter atteinte à la *Charte canadienne des droits et libertés*[7]. Les activités menées par le CST dans la réalisation du volet touchant au RE et à la cybersécurité ne doivent pas contrevenir aux autres lois fédérales ni viser l'acquisition d'information à partir de l'infrastructure mondiale de l'information ou par l'entremise de celui-ci qui puisse porter atteinte à une attente raisonnable de protection en matière de vie privée d'un Canadien ou d'une personne se trouvant au Canada, à moins d'être menées au titre d'une autorisation ministérielle[8].

---

[4] Au para 15(2) de la *Loi sur le CST*.
[5] Conformément à l'article 2 de la *Loi sur le CST*, l'infrastructure mondiale de l'information englobe les émissions électromagnétiques et tout équipement produisant de telles émissions; les systèmes de communication; les systèmes et réseaux de technologie de l'information; ainsi que les données ou informations techniques qui ont trait à cet équipement, à ces systèmes ou à ces réseaux, ou que ceux-ci transmettent ou contiennent.
[5] Aux paras 22(3) et 22(4) de la *Loi sur le CST*.
[6] Les termes s'appliquant au volet assistance technique et opérationnelle énoncent ce qui suit : lorsqu'il est appelé à prêter son assistance, le CST dispose d'un pouvoir d'intervention correspondant, selon le cas, à celui qui est exercé par les organismes chargés de l'application de la loi et de la sécurité, par les Forces canadiennes ou par le ministère de la Défense nationale (article 25 de la *Loi sur le CST*).
[7] Au para 22(1) de la *Loi sur le CST*.
[8] Aux paras 22(3) et 22(4) de la *Loi sur le CST*.

8. (NC) Le ministre de la Défense nationale peut délivrer une AM permettant au CST de mener des activités ou des catégories d'activités pouvant contrevenir à une loi fédérale et, dans le cas du RE et de la cybersécurité, de viser l'acquisition d'informations qui porteraient atteinte à l'attente raisonnable de protection en matière de vie privée d'un Canadien ou d'une personne se trouvant au Canada[9]. Les AM de RE et de cybersécurité doivent être approuvées par le commissaire au renseignement (CR), qui est tenu d'examiner si les conclusions que le ministre a rendues avant de délivrer l'autorisation sont raisonnables[10].

9. (NC) Ainsi, le CST est autorisé à acquérir incidemment[11] des informations qui se rapportent à un Canadien ou à une personne se trouvant au Canada au cours d'activités menées au titre d'une autorisation délivrée en vertu d'une AM de RE [art 26(1)], d'une AM de cybersécurité [art 27(1) ou 27(2)] ou encore d'une AM en cas d'urgence (art 40)[12]. Le CST désigne ces informations comme étant des informations se rapportant à un Canadien ou à une personne se trouvant au Canada (ICPC)[13]. Avant de délivrer une autorisation, le ministre doit être convaincu que le CST n'utilisera, n'analysera ou ne conservera les ICPC que si la situation répond aux conditions d'essentialité visées à l'article 34 de la *Loi sur le CST*, conditions qui sont différentes dans le cas des volets RE et cybersécurité. Pour ce qui touche le RE, l'essentialité est établie suivant une évaluation visant à déterminer si l'information est essentielle aux affaires internationales, à la défense ou à la sécurité[14]. Pour ce qui a trait à la cybersécurité, l'essentialité est établie suivant une évaluation visant à déterminer si l'information est nécessaire pour découvrir, isoler, prévenir ou atténuer des dommages (i) aux informations électroniques ou infrastructures de l'information des institutions fédérales ou encore (ii) aux informations électroniques ou infrastructures de l'information visées au paragraphe 21(1) de la *Loi sur le CST*[15].

10. (NC) Étant donné que la *Loi sur le CST* établit des distinctions entre les volets et leurs AM respectives, l'OSSNR a examiné les fondements juridiques encadrant les activités du CST en matière d'échange d'ICPC entre les volets RE et cybersécurité.

11. (NC) En raison de difficultés opérationnelles et de problèmes liés aux accès, notamment en contexte de pandémie de COVID-19, le présent examen n'a donné lieu ni à une évaluation ni à une vérification indépendantes de la conformité du CST aux lois ou aux contraintes et pouvoirs en vigueur dans les cas d'échanges d'informations en interne, entre divers volets. Au reste, l'OSSNR n'a pas été en mesure de procéder en toute indépendance à des observations, à des enquêtes ou à des validations visant les

---

[9] Aux para 22(3) et 22(4) de la *Loi sur le CST*.
[10] Aux articles 12 à 14 de la *Loi sur commissaire au renseignement.*
[11] Le paragraphe 23(5) de la *Loi sur le CST* définit l'adverbe « incidemment » comme suit : « S'agissant de l'acquisition d'information, s'entend de la manière dont celle-ci est acquise dans le cas où elle n'était pas délibérément recherchée et où le Canadien ou la personne se trouvant au Canada à qui elle se rapporte n'était pas visé par l'acquisition. »
[12] Au paragraphe 23(4) de la *Loi sur le CST*. En vertu de l'article 40 de la *Loi sur le CST*, le ministre peut, en cas d'urgence, délivrer une autorisation d'activités de RE ou de cybersécurité si les conditions – visées à l'article 34 – permettant de délivrer une autorisation de RE ou de cybersécurité sont respectées, alors que le temps requis pour obtenir l'approbation du commissaire au renseignement rendrait inutile la délivrance d'une autorisation.
[13] Par exemple, voir Ensemble des politiques relatives à la mission, Cybersécurité, p. 1 (novembre) [EPM, Cybersécurité].
[14] Pour ce qui concerne le RE, les critères permettant d'établir l'essentialité sont énoncés à l'alinéa 34(2)c) de la *Loi sur le CST* : « […] les mesures visées à l'article 24 permettront d'assurer que l'information acquise au titre de l'autorisation qui est identifiée comme se rapportant à un Canadien ou à une personne se trouvant au Canada sera utilisée, analysée ou conservée uniquement si elle est essentielle aux affaires internationales, à la défense ou à la sécurité. »
[15] Pour ce qui concerne la cybersécurité, les critères permettant d'établir l'essentialité sont énoncés à l'alinéa 34(3)d) de la *Loi sur le CST* : « […] les mesures visées à l'article 24 permettront d'assurer que l'information acquise au titre de l'autorisation qui est identifiée comme se rapportant à un Canadien ou à une personne se trouvant au Canada sera utilisée, analysée ou conservée uniquement si elle est essentielle pour découvrir, isoler, prévenir ou atténuer les dommages (i) aux informations électroniques ou aux infrastructures de l'information des institutions fédérales, dans le cas de l'autorisation visée par le paragraphe 27(1), ou aux informations électroniques ou aux infrastructures de l'information désignées comme étant d'importance pour le gouvernement fédéral en vertu du paragraphe 21(1), dans le cas de l'autorisation visée au paragraphe 27(2). »

systèmes employés aux fins des échanges de données entre divers volets (prière de consulter l'Annexe F pour trouver une description des méthodes et des processus suivis par le CST pour échanger des informations entre deux volets). Or, ces systèmes d'échange de données pourraient ultérieurement être l'objet d'un examen de la part de l'OSSNR.

12. (NC) L'OSSNR avait également l'intention d'examiner les échanges internes d'informations du côté des volets cyberopérations actives (COA) et cyberopérations défensives (COD) du mandat du CST, ce qui comprend également les exigences visées au paragraphe 34(4) de la *Loi sur le CST* concernant l'acquisition d'informations pendant les cyberopérations de type COA ou COD. Entre autres, ce paragraphe stipule qu'aucune information ne sera acquise au titre d'une autorisation de COA ou de COD, sauf conformément à une autorisation de RE [*Loi sur le CST*, paragraphe 26(1)], à une autorisation de cybersécurité [*Loi sur le CST*, paragraphes 27(1) et 27(2)] ou à une autorisation en cas d'urgence [*Loi sur le CST,* paragraphe 40(1)]. Cet aspect de l'examen a plutôt été réalisé à l'occasion d'un autre examen de l'OSSNR intitulé *Cyberopérations actives et cyberopérations défensives du CST – Gouvernance* et sera examiné plus avant à l'occasion d'un prochain examen de l'OSSNR devant se dérouler en 2021.

13. (NC) Il importe d'indiquer que le présent examen ne s'est pas penché sur la communication d'informations nominatives sur un Canadien (INC) à l'extérieur du CST[16].

III CONTEXTE

Que sont les ICPC?

14. (NC) Même si elle est mentionnée à plusieurs reprises dans la *Loi sur le CST*[17], la notion « information se rapportant à un Canadien ou à une personne se trouvant au Canada » (ICPC) n'y est pas précisément définie. De fait, les ICPC sont des informations qui se rapportent à un Canadien ou à une personne se trouvant au Canada et qui pourraient être incidemment collectées par le CST durant des activités de RE ou de cybersécurité menées au titre d'une AM. Selon la politique du CST, s'entend d'une ICPC toute information reconnue comme se rapportant à un Canadien ou à une personne se trouvant au Canada, que cette information puisse ou non servir à identifier ledit Canadien ou ladite personne se trouvant au Canada[18].

---

[16] Précédemment, l'OSSNR avait examiné un échantillonnage des INC divulguées en vertu de la *Loi sur la défense nationale*. Voir l'Examen nº 08-501-3 de l'OSSNR : *Divulgations d'informations identifiant un Canadien*. En vertu de l'article 31 de la *Loi sur l'OSSNR*, l'OSSNR demande actuellement au CST de réaliser une étude au titre de l'article 31 de la *Loi sur l'OSSNR* visant à démontrer que ses divulgations d'INC respectent les dispositions de la *Loi sur le CST*.

[17] Voir l'article 24, le paragraphe 23(4), les alinéas 34(2)c) et 34(3)d) ainsi que le paragraphe 44(1) de la *Loi sur le CST*. À titre d'exemple, l'article 34 propose cette description : « […] l'information acquise au titre [d'une] autorisation qui est identifiée comme se rapportant à un Canadien ou à une personne se trouvant au Canada […]. »

[18] Approuvé le 18 février 2021, l'EPM Renseignement étranger, v.5.0, n'était pas encore en vigueur au moment de l'examen. Mais la politique du CST définit l'ICPC comme suit : [Traduction] « Les ICPC sont des informations qui se rapportent à un Canadien ou à une personne se trouvant au Canada, que cette information puisse ou non être utilisée pour identifier ce Canadien ou cette personne se trouvant au Canada. Or, les ICPC pourraient comprendre ce que l'on appelle les informations nominatives sur un Canadien (INC), lesquelles sont des informations identifiant ou permettant d'identifier un Canadien ou une personne se trouvant au Canada, mais aussi des entités comme les entreprises ou d'autres organisations (p. ex. numéros de téléphone, adresse de courrier électronique, etc.). Les ICPC peuvent également contenir des informations ne permettant pas d'identifier un Canadien ou une personne se trouvant au Canada (pensons aux codes postaux ou à toute autre information ne permettant pas d'identifier un Canadien ou une personne se trouvant au Canada). »

15. (NC) Il faut donc savoir que les ICPC diffèrent de ce que l'on appelle les informations nominatives sur un Canadien (INC). En outre, la *Loi sur le CST* emploie fréquemment les deux termes, ICPC et INC, pour désigner certains types d'informations. De fait, les ICPC comprennent toute information reconnue comme *se rapportant* à un Canadien ou à une personne se trouvant au Canada, tandis que les INC comprennent toute information qui permet *d'identifier* un Canadien ou une personne se trouvant au Canada et qui a été utilisée, analysée ou conservée au titre d'une autorisation de RE ou de situation d'urgence. Pour le CST, les INC sont un sous-ensemble des ICPC[19]. Par ailleurs, l'article 43 de la *Loi sur le CST* indique que les INC peuvent être communiquées par le CST à des personnes désignées en vertu de l'article 45 de cette même Loi.

Échanges internes d'ICPC au CST

16. (~~TS~~) Dans certains cas, la politique du CST permet que les ICPC collectées dans le cadre des activités d'un volet soient communiquées aux fins d'utilisation par un autre volet (voir l'Annexe D pour une description des autres types d'informations pouvant être échangées entre les volets RE et cybersécurité). Le CST permet que le RE soit utilisé en interne pour répondre à des besoins liés à la cybersécurité[20]. Les informations conservées au sein du volet cybersécurité peuvent être utilisées par le personnel du CST travaillant au sein du volet RE, à moins que les informations soient assujetties à des conditions particulières imposées par des clients externes ou des entités divulgatrices[21]. Selon le CST, les échanges d'information entre les divers volets du mandat permettent au Centre d'exercer ses fonctions de soutien aux priorités du gouvernement du Canada[22].

17. (~~TS~~) Dans le contexte de la cybersécurité, le CST a indiqué que les ICPC échangées en interne dans le but d'appuyer le volet RE [description des opérations du CST] [23]. [24].

18. (~~TS//SI~~) À titre d'exemple, le CST a abordé [exemple d'opérations du CST] [25]. [26] [27], Le fait de communiquer cette information entre divers volets du mandat a permis au CST de renforcer la protection de l'information électronique et des structures de l'information du GC, mais aussi des systèmes et réseaux d'importance (SRI) en permettant de reconnaître, d'isoler et d'atténuer la menace en question.

---

[19] Commentaires du CST sur l'exactitude des faits, 19 août 2021.
[20] [description des opérations du CST]
[21] EPM, Cybersécurité, section 26.2. Il s'agit là d'entités qui font appel aux services du Centre pour la cybersécurité, notamment les institutions fédérales et les SRI, en vertu d'une entente qu'elles ont conclue en tant que clients. Sont également concernés les consommateurs, les abonnés et ceux qui ont accès aux services du Centre pour la cybersécurité, notamment le service de cyberalerte.
[22] *Sharing information for use across aspects of the CSE Mandate*, CST, présentation à l'OSSNR, 7 février 2020, p. 6.
[23] CST, réponse à la DI-08, 8 octobre 2020, Q5.
[24] CST, réponse à la DI-14, 19 mars 2021, Q5.
[25] *Sharing information for use across aspects of the CSE Mandate*, CST, présentation à l'OSSNR, 7 février 2020, p. 4 et 5.
[26] Par exemple, [exemple d'opérations du CST]
[27] [exemple d'opérations du CST]

Cette communication a également fourni aux décideurs du GC un portrait complet des menaces qui ciblent le Canada.

19. (~~TS~~) Après avoir examiné une série de rapports choisis au hasard[28], reçu des informations de la part du CST et interrogé des analystes expérimentés à la fois en RE et en cybersécurité[29], l'OSSNR a appris que les ICPC échangées[30] entre les volets RE et cybersécurité comprenaient généralement [liste des données opérationnelles utilisées dans le système] La politique du CST permet [31].

20. (NC) Le CST estime que même lorsque des ICPC sont échangées entre les divers volets, les activités ne ciblent aucunement des Canadiens ou des personnes se trouvant au Canada[32]. Comme il a été dit précédemment, les activités du CST ne doivent viser ni les Canadiens ni les personnes se trouvant au Canada.

IV CONCLUSIONS ET RECOMMANDATIONS

Conformité aux dispositions de la *Loi sur le CST* et de la *Loi sur la protection des renseignements personnels*

Quelles sont les lois s'appliquant aux échanges d'informations en interne?

21. (~~S~~) Les lois s'appliquant au CST en matière d'échange d'informations en interne sont les lois habilitantes du CST, à savoir la *Loi sur le CST* et la *Loi sur la protection des renseignements personnels*. La *Loi sur le CST* ne contient pas à proprement parler d'autorisation permettant les échanges d'ICPC entre les divers volets. De même, les dispositions de la *Loi sur le CST* en matière de divulgation des INC, lesquelles sont énoncées aux articles 43 à 45, n'abordent pas directement la question des échanges d'ICPC en interne. De fait, pour que des informations soient divulguées en vertu de ces dispositions, le ministre doit d'abord autoriser le CST à collecter les INC et à les communiquer en interne. De plus, le CST ne constitue pas une entité désignée en vertu de l'article 45 de la *Loi sur le CST* pour ce qui a trait à la réception d'informations divulguées au titre des articles 43 et 44[33].

22. (NC) Les ICPC pourraient constituer des renseignements personnels au sens de l'article 3 de la *Loi sur la protection des renseignements personnels*, à savoir des informations se rapportant à une personne identifiable, qui sont enregistrées sous une forme ou une autre. Par exemple, les adresses IP canadiennes

[28] Les responsables de l'examen de l'OSSNR ont choisi au hasard [nombre] qui, pendant la période d'examen, étaient accessibles à la fois au personnel du RE et à celui de la cybersécurité travaillant respectivement pour les volets RE et cybersécurité du mandat du CST.
[29] CST, réponse à la DI-11, 12 novembre 2020, Q4.
[30] Techniquement, ces rapports sont accessibles pour le personnel travaillant pour les deux volets, évitant ainsi les « échanges » concrets entre les analystes concernés.
[31] EPM, RE, annexe D, (D.xv).
[32] CST, réponse à la DI-06, 17 septembre 2020, Q7. L'OSSNR n'a pas été en mesure de vérifier en toute indépendance l'exactitude de cet énoncé.
[33] Décret ministériel, Centre de la sécurité des télécommunications, *Disclosure of Canadian Identifying Information (Foreign Intelligence)*, signé le 23 juillet 2019; et Décret ministériel, Centre de la sécurité des télécommunications, *Disclosure of Information related to Canadians or Persons in Canada (Cybersecurity and Information Assurance),* signé le 22 juillet 2019.

pourraient constituer à la fois des ICPC au sens de la *Loi sur le CST*, mais aussi des renseignements personnels au sens de la *Loi sur la protection des renseignements personnels*[34]. En vertu de l'article 4 de la *Loi sur la protection des renseignements personnels*, la collecte de renseignements personnels doit être directement liée à une activité ou un programme d'exploitation de l'organisme, ce qui englobe les activités relevant du mandat du CST en vertu de la *Loi sur le CST.*

23. (NC) La *Loi sur la protection des renseignements personnels* exige également que les renseignements personnels soient utilisés ou divulgués conformément aux dispositions des articles 7 et 8 de la *Loi sur la protection des renseignements personnels*. En l'occurrence, l'article 7 énonce ce qui suit :

> À défaut du consentement de l'individu concerné, les renseignements personnels relevant d'une institution fédérale ne peuvent servir à celle-ci :
>
> (a) qu'aux fins auxquelles ils ont été recueillis ou préparés par l'institution de même que pour les usages qui sont compatibles avec ces fins;
>
> (b) qu'aux fins auxquelles ils peuvent lui être communiqués[35] en vertu de du paragraphe 8(2).

24. (NC) L'OSSNR a vérifié si les échanges d'ICPC effectués par le CST en interne répondaient aux exigences de la *Loi sur la protection des renseignements personnels*, laquelle impose des contraintes sur la façon dont les renseignements personnels collectés peuvent être utilisés par les institutions fédérales. L'OSSNR a conclu que dans certaines circonstances, comme il est décrit plus loin dans le présent rapport, les échanges d'ICPC constituant des renseignements personnels entre les volets RE et cybersécurité pourraient répondre aux exigences de la *Loi sur la protection des renseignements personnels*. Or, cette évaluation de la conformité nécessite l'analyse de chacun des cas.

Analyse juridique de la Direction des services juridiques (DSJ) du CST

25. (~~Protégé B//Secret professionnel de l'avocat~~) L'OSSNR s'est penché sur l'analyse juridique de la DSJ du CST[36], laquelle a été réalisée par les avocats du ministère de la Justice (MJ), [redacted]

[redacted] [avis ou conseil juridique] [redacted]

[redacted][37].

[34] La Cour suprême du Canada a déclaré qu'en certaines circonstances, l'utilisation d'une adresse IP pouvait créer une attente raisonnable de protection de la vie privée. « À mon avis, il faut reconnaître que l'identité d'une personne liée à son utilisation d'Internet donne naissance à un intérêt en matière de vie privée qui a une portée plus grande que celui inhérent à son nom, à son adresse et à son numéro de téléphone […]. » R c Spencer, 2014 CSC 43, au para 47. De la même façon, une adresse IP peut être considérée comme un renseignement personnel si elle peut être associée à un individu identifiable. Voir le document *Ce qu'une adresse IP peut révéler à votre sujet*, un rapport préparé par la Direction de l'analyse de la technologie du Commissariat à la protection de la vie privée du Canada, mai 2013.

[35] Il convient de noter que dans la traduction française de la *Loi sur la protection des renseignements personnels*, plus précisément aux articles 7 et 8, les termes anglais *disclosed* et *disclosure* sont rendus respectivement par les équivalents « communiqués » et « communication ». Or, il faut savoir que les versions anglaise et française d'une loi bilingue constituent des documents officiels et que les deux font autorité. *Voir le Renvoi relatif aux droits linguistiques du Manitoba* [1985] CSC nº 36.

[36] Il convient de noter que les conseils juridiques que le CST reçoit de la part de la DSJ proviennent du ministère de la Justice.

[37] [nom du document] Services juridiques du CST à destination du directeur général, Divulgation, politiques et examen, 17 décembre 2019, p. 2 [nom du document]

[redacted][38].

[redacted][39]. »

26. (~~Protégé B//Secret professionnel de l'avocat~~) Selon le MJ, [avis ou conseil juridique] [redacted]

[38] [lié à un avis ou conseil juridique] [redacted]

[39] [lié à un avis ou conseil juridique] [redacted]

[40] [lié à un avis ou conseil juridique] [redacted]

[redacted]

27. (~~Protégé B//Secret professionnel de l'avocat~~) Selon le MJ, [avis ou counseil juridique] [redacted][1]. [redacted]

[redacted][42]. »

Conformité à la Loi sur la protection des renseignements personnels

28. (NC) Suivant son évaluation de la conformité à l'article 7 de la *Loi sur la protection des renseignements personnels*, l'OSSNR note que le CST met davantage l'accent sur la conformité aux dispositions des alinéas 34(2)c) et 34(3)d) de la *Loi sur le CST*, lorsqu'il s'agit de soutenir les échanges internes de renseignements personnels entre divers volets du mandat.

29. (NC) Comme il a été indiqué, l'article 7 de la *Loi sur la protection des renseignements personnels* déclare qu'à défaut du consentement de l'individu concerné, les renseignements personnels relevant d'une institution fédérale ne peuvent servir à celle-ci : 1) qu'aux fins auxquelles ils ont été recueillis ou préparés par l'institution de même que pour les usages qui sont compatibles avec ces fins; ou 2) qu'aux fins auxquelles ils peuvent lui être communiqués en vertu du paragraphe 8(2) de la Loi. Il importe de souligner

[41] DSJ du CST, réponse à la DI-6, 16 septembre 2020, [lié à un avis ou conseil juridique] [redacted]

[42] DSJ du CST, courriel de suivi envoyé après la réunion du 20 octobre 2020 avec l'OSSNR.

que les fins de l'utilisation des informations ne doivent pas forcément être identiques à celles auxquelles les informations ont été obtenues; il suffit que cette utilisation soit *compatible* avec les fins[43].

30. (NC) Le fait de s'appuyer sur l'article 34 de la *Loi sur le CST* pose une difficulté sur le plan de la conformité à la *Loi sur la protection des renseignements personnels*, car l'article 34 ne cite pas à proprement parler les fins de la collecte incidente d'ICPC ni n'énonce d'autorisation visant les échanges en interne. Il établit plutôt les préalables qu'il faut respecter avant que le ministre exerce son pouvoir de délivrer une AM. Les alinéas 34(2)c) et 34(3)d) de la *Loi sur le CST* précisent que le ministre doit être convaincu que les mesures de protection de la vie privée visées à l'article 24 de la Loi garantiront que les ICPC seront utilisées, analysées, et conservées uniquement si ces ICPC sont conformes aux exigences en matière d'essentialité qui s'appliquent, selon le cas, au RE ou à la cybersécurité. En outre, ces conditions établissent un seuil obligatoire s'appliquant à l'utilisation, à l'analyse et à la conservation des ICPC collectées en vertu d'une AM, et non une autorisation visant les échanges d'ICPC en interne.

31. (NC) Tout dépend des circonstances de fait suivant lesquelles les ICPC sont échangées. En effet, tout échange d'ICPC contenant des renseignements personnels entre les volets RE et cybersécurité du CST pourrait être permis en vertu de la *Loi sur le CST* et de la *Loi sur la protection des renseignements personnels*, pour peu que les informations soient échangées pour les mêmes motifs que ceux pour lesquels elles avaient été obtenues ou pour une utilisation qui soit compatible avec ces motifs. En l'occurrence, il conviendrait de procéder à une évaluation de chacun des cas pour s'assurer que les ICPC sont *de facto* échangées en interne pour les mêmes motifs que ceux invoqués pour justifier la collecte, pour des motifs compatibles avec ceux ayant justifié la collecte ou encore pour les motifs visés à l'alinéa 7b) en vertu desquels les échanges sont permis à condition de répondre à l'un des critères énoncés par le Parlement au paragraphe 8(2) de la *Loi sur la protection des renseignements personnels*. Tel qu'il a été dit précédemment, le CST ne considère pas les échanges internes comme étant des divulgations d'informations. Or, l'OSSNR note que la question de savoir si les échanges internes constituent à proprement parler une « utilisation » ou une « divulgation » au titre de la *Loi sur la protection des renseignements personnels* demeure nébuleuse[44]. Néanmoins, l'OSSNR souligne qu'en se basant uniquement sur le critère « d'essentialité » visé à l'article 34, le CST ne se permet pas de conclure indubitablement qu'il dispose des pouvoirs requis pour procéder auxdits échanges en interne.

32. (NC) Une justification au titre de l'alinéa 7a) ou de l'alinéa 8(2)a) de la *Loi sur la protection des renseignements personnels* exige que le CST révèle l'objet de la collecte incidente et de l'échange en interne, qui est énoncé dans le volet correspondant du mandat du CST. Les motifs de collecte – de même que l'autorisation de procéder à la collecte – de renseignements personnels sont énoncés dans la *Loi sur le CST*. Les articles 16 et 17 de la Loi décrivent le RE et la cybersécurité comme étant les programmes et

---

[43] *R c Bernard*, 2014 CSC 13, au para 31. Autrement dit, il suffit qu'il y ait un lien direct entre les motifs et l'utilisation envisagée, à savoir un lien permettant de s'attendre à ce que les informations soient utilisées de la façon proposée.

[44] *Gauthier c Canada (ministre de la Consommation et des Affaires commerciales)* [1992] ACF nº 1040. Cet arrêté indique que l'utilisation de renseignements personnels par une autre section d'un même ministère constitue une divulgation. Il indique également que les échanges de renseignements personnels entre des sections d'un même ministère constituent des utilisations compatibles desdits renseignements. En outre, dans le dossier *Gauthier*, la Cour a conclu que la divulgation de renseignements personnels à une autre section d'un même ministère en guise de réponse à une autre personne respectait les dispositions du paragraphe 8(2) de la *Loi sur la protection des renseignements personnels* : [Traduction] « les articles 7 et 8 de la *Loi sur la protection des renseignements personnels* prévoient que les renseignements personnels ne peuvent être ni utilisés ni divulgués sans le consentement de l'individu concerné. Il y a bien quelques exceptions à cette règle générale. Toutefois, le paragraphe 8(2) stipule que les renseignements se rapportant à un individu peuvent être divulgués sans son consentement, si lesdits renseignements sont utilisés pour des motifs compatibles avec ceux pour lesquels ils ont été obtenus. » Par conséquent, les échanges internes d'ICPC entre les divers volets pourraient être vus comme des divulgations au titre de l'alinéa 7b) et du paragraphe 8(2) de la *Loi sur la protection des renseignements personnels*. Or, si l'utilisation en interne est considérée comme une divulgation, les dispositions énoncées aux articles 43 à 45 de la *Loi sur le CST* encadrant la divulgation d'informations par le CST s'appliqueraient aux activités d'échange en interne. Le ministre serait alors tenu de désigner des personnes ou des catégories de personnes au sein du CST pour l'application de l'article 43 et du paragraphe 44(1).

les activités opérationnelles de l'organisme, et les autorisent à collecter des informations dans l'exercice de leurs mandats respectifs. Rappelons que les AM doivent autoriser la collecte dès lors que les activités pourraient contrevenir aux dispositions d'une loi du Parlement ou prévoir l'acquisition – à partir de/par l'entremise de l'IMI – d'informations qui pourraient porter atteinte à une attente raisonnable en matière de protection de la vie privée d'un Canadien ou d'une personne se trouvant au Canada. Suivant la description des volets aux articles 16 et 17 de la *Loi sur le CST*, il peut y avoir des cas où les informations acquises en vertu de l'un des volets puissent être utilisées pour les mêmes motifs ou pour des motifs compatibles avec ceux d'un autre volet, ce qui répond aux exigences de la *Loi sur la protection des renseignements personnels* en matière d'échange interne des informations. Toutefois, on ne peut pas tenir ce principe pour acquis dans la mesure où les objectifs des divers volets sont décrits différemment dans la Loi.

33. (NC) L'article 16 de la *Loi sur le CST* autorise le Centre à acquérir des informations à partir/par l'entremise de l'IMI et d'utiliser, d'analyser et de communiquer ces informations aux fins de production de renseignement étranger conformément aux priorités du gouvernement du Canada (GC)[45]. Or, l'article 17 de la *Loi sur le CST* autorise le Centre à fournir des avis, des conseils et des services dans le but d'aider à protéger l'information électronique et les infrastructures de l'information des institutions fédérales, mais aussi les systèmes désignés comme étant importants pour le gouvernement fédéral, ainsi qu'à acquérir, à utiliser et à analyser les informations issues de l'IMI ou d'autres sources afin de fournir lesdits avis, conseils et services[46].

34. (~~TS//SI~~) Lorsqu'il s'agit d'échanger des ICPC acquises par le volet RE dans le but d'appuyer le volet cybersécurité du mandat du CST, il y a tout lieu de croire que les motifs demeurent les mêmes si la cybersécurité fait partie des motifs pour lesquels le RE a été obtenu, utilisé, analysé ou communiqué. Or, il convient de mentionner que pendant la période couverte par le présent examen, [redacted] [lié aux priorités du GC] [redacted][47]. Les échanges d'informations qui visent à répondre aux objectifs du CST consistant, selon l'article 17, à fournir des avis, des conseils et des services afin d'aider à protéger l'information électronique et les infrastructures de l'information des institutions fédérales ou désignées pourraient être considérés comme constituant des usages semblables (sinon compatibles) à l'usage pour lequel les ICPC ont initialement été obtenues. Dès lors que du RE est utilisé dans le cadre du volet prévu à l'article 17 afin de protéger l'information électronique et les infrastructures de l'information fédérales ou désignées, les motifs de la collecte et l'utilisation corollaire des informations collectées pourraient demeurer les mêmes.

35. (NC) Pour ce qui concerne les ICPC acquises par le volet cybersécurité, les communications d'informations vers le volet RE pourraient être autorisées pour peu que l'usage du RE repose sur des motifs semblables (sinon compatibles) à ceux qui justifient l'acquisition initiale des informations, c.-à-d. de fournir des avis, des conseils et des services afin d'aider à protéger l'information électronique ou les infrastructures de l'information fédérales ou désignées. Ainsi, la communication d'ICPC obtenues par le

---

[45] L'article 16 de *la Loi sur le CST* énonce ce qui suit : « En ce qui a trait au volet de son mandat touchant le renseignement étranger, le Centre acquiert, secrètement ou d'une autre manière, de l'information à partir de l'infrastructure mondiale de l'information ou par son entremise, notamment en engageant des entités étrangères situées à l'extérieur du Canada ou en interagissant avec celles-ci ou en utilisant tout autre moyen d'acquérir de l'information, et utilise, analyse et diffuse l'information dans le but de fournir des renseignements étrangers, en conformité avec les priorités du gouvernement fédéral en matière de renseignement. »

[46] Le volet ayant trait à la cybersécurité et à l'assurance de l'information est décrit à l'article 17 : « En ce qui a trait au volet touchant la cybersécurité et l'assurance de l'information, le Centre a) fournit des avis, des conseils et des services afin d'aider à protéger (i) l'information électronique et les infrastructures de l'information des institutions fédérales, et (ii) l'information électronique et les infrastructures de l'information d'importance pour le gouvernement fédéral désignées comme telles en vertu du paragraphe 21(1); acquiert, utilise et analyse de l'information provenant de l'infrastructure mondiale de l'information ou d'autres sources afin de fournir de tels avis, conseils et services. »

[47] *Liste des priorités SIGINT nationales, version nº 2020.02.01.*

volet cybersécurité vers le volet RE serait permissible en vertu de la *Loi sur la protection des renseignements personnels* pour peu que les échanges internes servent l'objectif consistant à aider à protéger l'information électronique et les infrastructures de l'information fédérales ou désignées.

36. (NC) Somme toute, si le CST acquiert des renseignements personnels afin d'alimenter les activités des volets RE ou cybersécurité ou de servir des usages compatibles avec ces activités, ses échanges internes d'ICPC peuvent être conformes aux dispositions de l'alinéa 7a) ou du paragraphe 8(2) de la *Loi sur la protection des renseignements personnels*, pour peu que les fins poursuivies par les activités de collecte et d'échange soient énoncées et justifiées. De plus, le CST doit toujours répondre aux conditions stipulées dans la *Loi sur le CST* et ayant trait aux AM relativement à la collecte et à l'utilisation des ICPC. Pour justifier les échanges internes de renseignements personnels entre divers volets, il faut réaliser une analyse approfondie axée sur les circonstances de fait de chacun des cas.

(NC) Conclusion nº 1 : Les échanges internes d'informations entre les volets RE et cybersécurité du mandat du CST n'ont pas été suffisamment examinés quant à leur conformité aux dispositions de la *Loi sur la protection des renseignements personnels.*

(NC) Recommandation nº 1 : L'OSSNR recommande que le CST obtienne de plus amples conseils juridiques concernant ses échanges d'informations entre les volets touchant la cybersécurité et le renseignement étranger de son mandat, plus précisément pour ce qui a trait à leur conformité aux dispositions de la *Loi sur la protection des renseignements personnels*, lesquelles traitent en profondeur des deux questions suivantes :

1) établir si les échanges internes d'informations entre les volets touchant la cybersécurité et le renseignement étranger de son mandat constituent des utilisations ou des divulgations d'informations au titre de la *Loi sur la protection des renseignements personnels*;

2) établir si les utilisations et les divulgations sont réalisées en conformité avec les dispositions des articles 7 et 8 de la *Loi sur la protection des renseignements personnels.*

Autorisations ministérielles

37. (NC) La *Loi sur le CST* ne permet pas au ministre d'autoriser les échanges d'ICPC en interne. En effet, seules les AM peuvent accorder une autorisation visant, dans le cas du RE, les activités ou catégories d'activités énumérées au paragraphe 26(2) ou encore, dans le cas de la cybersécurité, les activités d'accès ou d'acquisition visant les informations visées aux paragraphes 27(1) et 27(2). Tout échange interne d'ICPC contenant des renseignements personnels doit être réalisé en conformité aux dispositions de la *Loi sur la protection des renseignements personnels.*

38. (NC) Comme il a été dit précédemment, l'article 24 de la *Loi sur le CST* exige que le Centre mette en place des mesures pour protéger la vie privée des Canadiens et des personnes se trouvant au Canada en ce qui a trait à l'utilisation, à l'analyse, à la conservation et à la divulgation d'ICPC. Ainsi, lorsqu'il délivre une AM, le ministre doit avoir conclu que ces mesures garantiront que les ICPC acquises ne seront utilisées, analysées ou conservées que si elles répondent aux critères d'essentialité énoncés aux alinéas 34(2)c) ou 34(3)d). Le ministre peut délivrer les autorisations s'il conclut que les activités en cause sont « raisonnables et proportionnelles compte tenu de la nature de l'objectif à atteindre et des activités[48]. » Alors que le ministre soupèse le caractère raisonnable des activités proposées aux fins du RE ou de la cybersécurité, on peut imaginer que certaines activités puissent être raisonnables et proportionnelles dans un contexte, mais pas dans l'autre. Certes, les activités autorisées au titre du paragraphe 26(2) peuvent acquérir un éventail d'informations plus large que celui qui est visé aux paragraphes 27(1) et 27(2). Or, les communications d'informations allant du RE à la cybersécurité pourraient permettre au CST d'utiliser, aux fins de la cybersécurité, plus d'informations que ce qui est permis par les autorisations de cybersécurité en soi et pourraient nécessiter de nouvelles mesures de protection de la vie privée lorsque lesdites informations sont utilisées.

39. (NC) Pour délivrer une AM, le chef du CST doit, dans une demande, faire état des faits de telle sorte que le ministre puisse conclure qu'il y a des motifs raisonnables de croire que l'autorisation est nécessaire et que les critères justifiant la délivrance sont respectés[49]. L'OSSNR estime nécessaire que la demande présentée par le chef donne au ministre toutes les informations requises sur la façon dont les ICPC pourraient être utilisées et analysées par le CST, ce qui comprend les modalités d'échange des ICPC avec d'autres volets ainsi que les fins poursuivies. Ces informations devraient également permettre au ministre de déterminer, en application de l'article 35, si d'autres critères, conditions ou contraintes pourraient être recommandés afin de protéger la vie privée des Canadiens dès lors qu'il est question de délivrer une autorisation de RE ou de cybersécurité.

40. (~~TS//SI~~) Pour ce qui concerne les autorisations délivrées en 2020, la plupart des demandes présentées par le chef du CST indiquaient que les informations collectées et conservées pourraient possiblement être utilisées par d'autres volets, alors que le texte de la plupart des AM correspondantes ne faisait aucune mention de possibles utilisations par d'autres volets[50]. Dans un cas particulier, c'est la situation inverse qui s'est produite : [exemple d'opérations du CST] [redacted][51].

41. (~~TS//SI~~) De plus, en 2020, les demandes et les autorisations de RE indiquent que pour répondre au critère d'essentialité s'appliquant à la conservation des ICPC au titre de l'alinéa 34(2)c) de la *Loi sur le CST*, les ICPC seront conservées pour peu qu'elles soient jugées essentielles pour la cybersécurité[52]. En l'occurrence, la cybersécurité fait partie de ces éléments qui sont « essentiels pour la sécurité », ce qui

[48] Au paragraphe 34(1) de la *Loi sur le CST*.
[49] Au paragraphe 33(2) de la *Loi sur le CST*.
[50] Les demandes suivantes indiquent que des ICPC seront utilisées par un volet différent, mais ne font aucune mention de cette utilisation dans l'AM : Demande d'activités de cybersécurité – fédéral (26 juin 220), au para 58; [nom du document] (25 août 2020), au para 96; [nom du document] (25 août 2020), au para 68.
[51] Au paragraphe 19.
[52] Les AM de RE suivantes indiquent que des ICPC seront conservées si elles sont jugées essentielles aux affaires internationales, à la défense ou à la sécurité : [nom du document] aux paras 77 et 137; [nom du document] aux paras 6(d), 94, 103, 165, 166 et 168; [nom du document] aux paras 41 à 44 et 54d) et g); [nom du document] aux paras 65 et 144; et [nom du document] aux paras 40, 41 et 57d).

donne au ministre des éléments contextuels additionnels sur la façon dont les conditions de l'essentialité sont évaluées, mais aussi respectées par le CST[53]. L'OSSNR estime que ces informations sont nécessaires dans la mesure où elles permettent au ministre d'établir si les conditions énumérées à l'article 34 de la *Loi sur le CST* ont été respectées préalablement à la délivrance de l'AM.

(NC) Conclusion nº 2 : À l'exception d'une seule, les demandes d'autorisations ministérielles présentées par le chef du CST en 2020 informaient adéquatement le ministre de la Défense nationale que des informations conservées pourraient être utilisées en soutien à un volet distinct.

(NC) Conclusion nº 3 : Les demandes d'autorisation de renseignement étranger que le chef du CST a présentées pendant la période visée par le présent examen informaient adéquatement le ministre de la Défense nationale de la façon dont les conditions visées à l'alinéa 34(2)c) avaient été respectées pour ce qui concerne les ICPC collectées en vertu du volet RE du mandat du CST.

(NC) Recommandation nº 2 : Toutes les demandes touchant le renseignement étranger et la cybersécurité présentées par le chef du CST devraient informer adéquatement le ministre de la Défense nationale que des informations conservées pourraient être utilisées en soutien à un volet distinct.

Évaluation de l'essentialité, de la nécessité et de la pertinence

42. (NC) En vertu de la politique du CST, il faut procéder à une évaluation de la pertinence, de l'essentialité ou de la nécessité des ICPC pour chacun des volets avant d'être en mesure d'établir s'il convient d'échanger les informations entre divers volets (voir l'Annexe G pour connaître les balises et les définitions employées pour l'évaluation des ICPC que l'on envisage de communiquer entre divers volets). Ces termes sont tirés de la *Loi sur le CST*, mais n'y sont pas définis. La politique du CST fournit des définitions et des critères sur lesquels reposent l'évaluation et l'application de ces balises aux informations. Or, l'OSSNR n'a évalué ni le caractère licite de ces balises stratégiques ni la façon dont les exigences sont respectées par le CST lorsque ce dernier procède à des échanges d'ICPC en interne. Ces aspects pourraient être examinés à l'occasion d'examens ultérieurs.

43. (~~TS~~) La politique du CST établit également les critères suivant lesquels il convient d'autoriser les échanges d'ICPC entre divers volets (voir l'Annexe E pour connaître les processus d'approbation que le CST applique aux échanges d'informations). Avant que les ICPC puissent être échangées entre divers volets, leur caractère essentiel doit être évalué en fonction du volet qui en a fait l'acquisition. Dès lors qu'elles ne respectent pas les balises permettant d'établir leur caractère essentiel, les informations doivent être supprimées[54].

44. (~~Protégé B//Secret professionnel de l'avocat~~) Selon le CST, [avis ou conseil juridique] [redacted]

[53] CST, réponse à la DI-09, 27 octobre 2020, Q5.
[54] CST, réponse à la DI-06, 16 septembre 2020, Q6.

[redacted][55].

45. (NC) L'OSSNR admet que la *Loi sur le CST* n'exige pas que les ICPC échangées en interne entre les volets RE et cybersécurité respectent les deux conditions de l'essentialité visées aux alinéas 34(2)c) et 34(3)d) de la Loi. Or, les paragraphes 22(3) et 22(4) de la *Loi sur le CST* exigent la délivrance d'une AM de RE ou de cybersécurité, lorsque les activités à mener en soutien à l'un ou l'autre de ces volets impliquent l'acquisition, à partir de l'IMI, d'informations pouvant porter atteinte à une attente raisonnable de protection de la vie privée ou lorsque les activités pourraient contrevenir à une loi fédérale. Les AM ne peuvent autoriser que les activités ou catégories d'activités énumérées au paragraphe 26(2) pour le RE, ou pour accéder aux infrastructures de l'information et acquérir les informations énoncées aux paragraphes 27(1) et 27(2). Comme il a été dit précédemment, les balises s'appliquant à « l'essentialité » (cf. l'article 34) établissent l'autorité du ministre en matière d'approbation d'une AM en fonction des préalables énoncés au paragraphe 24 concernant la protection de la vie privée. On pourrait donc comprendre que cette exigence s'applique à l'utilisation, à l'analyse et à la conservation des ICPC collectées par le CST en vertu d'une AM, et ce, dans un seul volet. Par conséquent, la *Loi sur le CST* n'exige d'aucune façon que le CST respecte les balises encadrant la notion d'essentialité dans le cas d'un volet dont les ICPC font l'objet d'un échange en interne. Les ICPC doivent uniquement respecter les conditions initiales d'essentialité énoncées à l'alinéa 34(2)c) ou à l'alinéa 34(3)d) lorsque des ICPC sont acquises conformément à l'AM qui autorise la collecte incidente desdites ICPC.

(NC) Conclusion nº 4 : La position du CST voulant que le Centre ne soit pas tenu d'évaluer « l'essentialité » en deux occasions lorsque des informations sont échangées entre le volet renseignement étranger et le volet cybersécurité de son mandat est compatible avec les dispositions des alinéas 34(2)c) et 34(3)d) de la *Loi sur le CST*.

V CONCLUSION

46. (NC) Comme la *Loi sur le CST* établit des distinctions entre les divers volets et les AM correspondantes, l'OSSNR a décidé d'examiner les fondements juridiques régissant les échanges d'ICPC entre le volet RE et le volet cybersécurité du mandat du CST. L'OSSNR a conclu que dans certaines circonstances, les échanges en interne pourraient être compatibles avec les dispositions de la *Loi sur la protection des renseignements personnels*. Toutefois, le CST doit accorder une attention accrue aux motifs de la collecte d'ICPC lorsqu'il s'agit de justifier les échanges d'ICPC en interne.

47. (NC) Le présent examen a également permis d'acquérir une connaissance de base des processus, des systèmes et des mesures de conformité en vigueur au CST relativement aux échanges d'ICPC entre divers volets du mandat. Même s'il n'a pas été en mesure de vérifier ces informations en toute indépendance, l'OSSNR envisage de s'en inspirer pour réaliser les examens ultérieurs.

[55] DSJ du CST, réponse à la DI-06, 17 septembre 2020, Q2. [avis ou conseil juridique] [redacted] voir CST, réponse à la DI-11, 19 mars 2021, Q14.

ANNEXE A : OBJECTIFS, PORTÉE ET MÉTHODOLOGIE

1. (NC) Initialement, l'OSSNR se proposait d'examiner les échanges internes d'ICPC entre divers volets du mandat du CST suivant une approche thématique devant se concentrer sur plusieurs secteurs opérationnels et plusieurs volets. En outre, l'examen prévoyait d'examiner les échanges d'informations ayant eu lieu entre divers volets, du 1er août 2019 au 1er août 2020, de sorte à évaluer en toute indépendance :

- la conformité aux exigences juridiques, ministérielles et stratégiques, notamment la gestion adéquate des risques liés à la conformité pendant la conduite d'activités d'échange d'informations entre divers volets du mandat du CST;

- les politiques, les procédures et les pratiques du CST s'appliquant aux échanges internes d'informations entre divers volets du mandat du CST.

2. (NC) Compte tenu de la conjoncture défavorable au déroulement des opérations, pensons notamment aux perturbations et aux difficultés d'accès liées à la pandémie de COVID-19, il a fallu réviser à la baisse les objectifs, la portée et la méthodologie qui avaient été fixés pour le mandat du présent examen (envoyé au CST le 28 août 2020). Par conséquent, l'examen n'a porté que sur les fondements juridiques sur lesquels s'appuient les échanges d'informations entre le volet RE et le volet cybersécurité.

3. (NC) L'OSSNR a donc examiné des documents et des dossiers ayant trait aux échanges d'informations entre divers volets du mandat du CST, et ce, pour la période s'étendant du 1er août 2019, date d'entrée en vigueur de la *Loi sur le CST*, au 1er août 2020.

4. (NC) Deux entrevues ont été réalisées avec des employés du CST ayant pris part à des échanges d'informations entre divers volets du mandat du CST. De plus, une entrevue a été réalisée avec un avocat du ministère de la Justice qui connaît bien le cadre juridique qui régit ce type d'activités.

5. (NC) L'OSSNR a également produit une description élémentaire de certains des processus, des systèmes et des mesures de conformité s'appliquant aux échanges d'informations dans le but d'établir une base de connaissances sur laquelle les examens ultérieurs pourront s'appuyer.

ANNEXE B : RÉUNIONS ET SÉANCES D'INFORMATION

Séance d'information, *Information Sharing: Sharing information for use across aspects of the CSE Mandate*, OSSNR, 7 février 2020.

OSSNR, réunion avec l'avocat du ministère de la Justice à la DSJ du CST, 13 octobre 2020.

OSSNR, réunion avec des analystes du CST, 20 octobre 2020.

ANNEXE C : CONCLUSIONS ET RECOMMANDATIONS

(NC) Conclusion nº 1 : Les échanges internes d'informations entre les volets RE et cybersécurité du mandat du CST n'ont pas été suffisamment examinés quant à leur conformité aux dispositions de la Loi sur la protection des renseignements personnels

(NC) Recommandation nº 1 : L'OSSNR recommande que le CST obtienne de plus amples conseils juridiques concernant ses échanges d'informations entre les volets touchant la cybersécurité et le renseignement étranger de son mandat, plus précisément pour ce qui a trait à leur conformité aux dispositions de la *Loi sur la protection des renseignements personnels*, lesquelles traitent en profondeur des deux questions suivantes :

> 1) établir si les échanges internes d'informations entre les volets touchant la cybersécurité et le renseignement étranger de son mandat constituent des utilisations ou des divulgations d'informations au titre de la *Loi sur la protection des renseignements personnels*;
>
> 2) établir si les utilisations et les divulgations sont réalisées en conformité avec les dispositions des articles 7 et 8 de la *Loi sur la protection des renseignements personnels*.

(NC) Conclusion nº 2 : À l'exception d'une seule, les demandes d'autorisations ministérielles présentées par le chef du CST en 2020 informaient adéquatement le ministre de la Défense nationale que des informations conservées pourraient être utilisées en soutien à un volet distinct.

(NC) Conclusion nº 3: Les demandes d'autorisation de renseignement étranger que le chef du CST a présentées pendant la période visée par le présent examen informaient adéquatement le ministre de la Défense nationale de la façon dont les conditions visées à l'alinéa 34(2)c) avaient été respectées pour ce qui concerne les ICPC collectées en vertu du volet RE du mandat du CST.

(NC) Recommandation nº 2 : Toutes les demandes touchant le renseignement étranger et la cybersécurité présentées par le chef du CST devraient informer adéquatement le ministre de la Défense nationale que des informations conservées pourraient être utilisées en soutien à un volet distinct.

(NC) Conclusion nº 4 : La position du CST voulant que le Centre ne soit pas tenu d'évaluer « l'essentialité » en deux occasions lorsque des informations sont échangées entre le volet renseignement étranger et le volet cybersécurité de son mandat est compatible avec les dispositions des alinéas 34(2)c) et 34(3)d) de la Loi sur le CST.

ANNEXE D : LES INFORMATIONS SUR LES PARTENAIRES ET LES CLIENTS AINSI QUE LES INFORMATIONS PUBLIQUEMENT ACCESSIBLES FAISANT L'OBJET D'ÉCHANGES ENTRE LES VOLETS RENSEIGNEMENT ÉTRANGER ET CYBERSÉCURITÉ

1. (~~Protégé B~~) Dans le cadre du volet cybersécurité, les clients du fédéral, mais aussi d'autres clients peuvent divulguer des informations sur les cybermenaces au CST, qui est l'organisme responsable de la cybersécurité au Canada. Ces clients peuvent également faire appel aux services du CST aux fins d'analyse et d'atténuation de cyberincidents avérés ou soupçonnés. Les informations communiquées peuvent être utilisées à des fins liées au RE, pour peu que cette communication serve à identifier, à isoler, à prévenir ou à atténuer les dommages aux systèmes des institutions fédérales ou aux systèmes d'importance pour le GC.

2. (~~Protégé B~~) Les documents de gouvernance qui encadrent les ententes conclues entre le CST, d'une part, et le GC et les clients non fédéraux, d'autre part, précisent que les informations qui ont été obtenues par le CST par l'intermédiaire du réseau ou du système d'un client et qui se rapportent au volet cybersécurité peuvent être communiquées aux partenaires [informations opérationnelles du CST] ou aux partenaires internes dans le cas des clients du GC) qui œuvrent dans le domaine de la cybersécurité aux fins de découverte, d'isolement, de prévention ou d'atténuation des dommages aux systèmes des institutions fédérales ou aux systèmes d'importance pour le GC[56]. Toutefois, ces documents n'indiquent pas explicitement que les informations provenant des clients pourraient être utilisées à des fins liées au RE. Pour permettre aux entités divulgatrices de donner un consentement qui soit éclairé, l'OSSNR estime qu'il serait approprié que le CST soit parfaitement transparent concernant la façon dont les informations provenant des clients pourraient être utilisées par le CST.

3. (~~Protégé B~~) Lorsqu'elles sont communiquées à des partenaires [informations opérationnelles du CST] les informations venant de clients sont anonymisées, et les renseignements permettant d'identifier une personne sont exclus. Tout produit de cybersécurité diffusable qui a été créé à partir d'informations venant d'un client ne doit contenir que l'information nécessaire à l'atténuation d'une cybercompromission[57]. De plus, les entités divulgatrices peuvent également imposer certaines restrictions sur l'utilisation et la communication de leurs données au moment de la divulgation[58].

4. (~~TS~~) En vertu du paragraphe 21(1) de la *Loi sur le CST*, le Centre est autorisé à acquérir et à utiliser les informations publiquement accessibles sans avoir à demander une AM. Actuellement, [lié à un avis ou conseil juridique] [59].

[56] CST, réponse à la DI-09, 20 octobre 2020, Q4; *Modèle_CONOP_Signatures numériques; LdD Autorisation de cybersécurité pour les infrastructures non fédérales; Modèle – LdD (Lettre de demande) Signatures numériques,* reçus en accompagnement de la DI-15, 24 mars 2021, Q4.
[57] EPM, Cybersécurité, section 22.2.
[58] EPM, Cybersécurité, section 20.7. Il convient de noter que l'OSSNR n'a pas été en mesure de vérifier en toute indépendance la collecte, l'utilisation ou les échanges d'informations clients par le CST.
[59] CST, réponse à la DI-11, 17 novembre 2020, Q7. L'OSSNR n'a pas reçu [lié à un avis ou conseil juridique]

ANNEXE E : PROCESSUS D'APPROBATION ET APPROBATION DES ÉCHANGES D'INFORMATIONS

Processus d'approbation des échanges d'ICPC

1. (~~TS//SI~~) Le pouvoir officiel d'autorisation des échanges d'informations est énoncé dans la politique interne du CST et est tributaire de la nature des informations à échanger. La politique du CST exige l'approbation de la gestion (ce qu'on appelle également « autorité de diffusion ») avant tout échange d'ICPC non supprimées entre divers volets. Cependant, la politique ne donne aucune précision quant au processus d'approbation en vigueur. On s'en remet plutôt au secteur opérationnel concerné et aux pratiques opérationnelles qui y sont observées[60]. D'après l'ensemble des politiques relatives à la mission (EPM), toutes les décisions de gestion doivent être enregistrées et conservées dans un dépôt central aux fins de transparence et de reddition de comptes. En outre, ces enregistrements doivent être accessibles aux responsables des examens[61]. Toutefois, dans le cadre du présent examen, l'OSSNR n'a pas été en mesure de vérifier ni d'évaluer en toute indépendance le processus d'approbation visant les échanges d'ICPC en interne.

2. (~~TS~~) En règle générale, le CST exige des approbations de gestion dans le cas des échanges d'informations – contenues dans un rapport – aux fins d'utilisation par divers volets du mandat du CST. Lorsque les informations contiennent des ICPC, le CST élève l'autorité de diffusion au niveau hiérarchique approprié[62]. L'autorité de diffusion appropriée et les conditions de diffusion sont décrites dans la politique (dont il est question plus bas). L'autorité de diffusion est responsable des échanges d'informations et doit être avisée de tout changement apporté aux données et donnant lieu à une modification des informations se rapportant à la vie privée que l'on envisage de communiquer[63].

3. (~~TS~~) Les techniques d'échange automatisé [lié aux priorités du GC] [redacted][64].

Communication d'ICPC du volet cybersécurité au volet renseignement étranger

4. (NC) Les ICPC conservées aux fins du volet cybersécurité peuvent être communiquées au volet RE à titre de produits de cybersécurité communicables (PCC) dès lors que ces produits répondent aux exigences énumérées plus bas. Or, l'autorité de diffusion est établie en fonction de l'impact que la communication des informations peut avoir sur la vie privée d'un individu ou d'une entité, et cet impact est déterminé en fonction du niveau de sensibilité et de la nature des ICPC[65].

[60] CST, réponse à la DI-06, 17 septembre 2020, Q8; CST, réponse à la DI-08, 8 octobre 2020, Q4.
[61] CST, réponse à la DI-06, 17 septembre 2020, Q8.
[62] CST, réponse à la DI-08, 8 octobre 2020, Q4.
[63] CST, réponse à la DI-08, 8 octobre 2020, Q4.
[64] EPM, Cybersécurité, section 25.6; EPM, RE, section 29.2.
[65] Voir EPM, Cybersécurité, section 7.1.

Selon le niveau de sensibilité des ICPC, les gestionnaires ou superviseurs des opérations du Centre canadien pour la cybersécurité (CCC)[66] doivent approuver les PCC contenant des ICPC[67].

5. (NC) D'après le CST, les exigences s'appliquant aux PCC sont les suivantes[68] :

Exigence	Quand et comment l'exigence est appliquée
L'objectif est de fournir des conseils, des avis et des services	Au moment de l'échange. – Pourquoi cette information doit-elle faire l'objet d'un échange?
Le produit ne contient que les informations conservées	La décision d'utiliser ou de conserver les informations est prise au moment où les données brutes sont évaluées dans le but d'en établir la pertinence et la nécessité (et l'essentialité dans le cas des ICPC) pour le volet cybersécurité du mandat.
Protection de la vie privée	Au moment de l'échange, s'il y a lieu (p. ex. restitution au propriétaire de système/à l'administrateur qui a déjà accès aux informations depuis ses propres systèmes ou diffusion à un auditoire élargi moyennant de rigoureuses restrictions visant l'utilisation des informations). Aucune suppression n'est requise lorsque les ICPC sont échangées pour utilisation dans le cadre du volet RE du mandat, pour peu que l'échange vise à soutenir les activités consacrées à la protection des informations électroniques et des infrastructures de l'information du GC ou à la protection des systèmes et réseaux d'importance pour le GC.
Classification et contraintes s'appliquant à l'utilisation et au traitement	S'appliquent à l'utilisation et à la diffusion des informations par le volet RE au moment de l'échange ou à une étape ultérieure. Peuvent comprendre des utilisations subséquentes préapprouvées et, s'il y a lieu, des restrictions imposées par le propriétaire des données/des systèmes. Peuvent être appliquées aux rapports produits finis (RPF) par une plateforme de préparation de rapports (PPR); imposent des restrictions sur les modalités d'utilisation et de diffusion des informations du CST.
Vérifiable	Au moment de l'acquisition; appliqué automatiquement par les systèmes du CST. À toutes les données reçues par le CST, on attribue automatiquement un identifiant unique ainsi que des informations concernant leur origine (p. ex. AM vs non-AM; le client divulgateur, s'il y a lieu, etc.); les contrôles d'accès, s'il y a lieu; le volet du mandat en vertu duquel les données ont été acquises; la date et l'heure de l'acquisition; et les exigences en matière d'utilisation et de traitement.
Diffusion approuvée	Au moment de l'échange. Le niveau de l'autorité de diffusion dépend de la nature des informations. Voir le tableau de la section 25.2 du chapitre consacré à la cybersécurité, dans l'EPM.

[66] Le CCC fait partie du CST. Relevant du volet cybersécurité du mandat du CST, le CCC est chargé d'intervenir au nom du gouvernement en cas d'incidents de cybersécurité.
[67] EPM, Cybersécurité, section 25.2.
[68] CST, réponse à la DI-14, 19 mars 2021, Q5.

Communication d'ICPC du volet renseignement étranger au volet cybersécurité

6. (~~TS~~) Les ICPC obtenues aux fins du volet RE peuvent être communiquées au CCC en tant que produits SIGINT communicables (PSC). Or, avant d'être communiqués, les PSC contenant des informations présentant un intérêt reconnu sur le plan de la vie privée de Canadiens ou se rapportant à du matériel présentant un intérêt sur le plan de la vie privée de Canadiens nécessitent l'approbation du CA SIGINT, quoique ce pouvoir d'approbation puisse être délégué à un autre intervenant[69].

7. (~~TS~~) Le tableau suivant présente succinctement les façons dont les critères énoncés dans la politique peuvent être respectés lorsqu'il s'agit de créer un PSC aux fins d'échange d'informations pour utilisation par le volet cybersécurité.

Exigence	**Quand et comment l'exigence est appliquée**
Les informations se rapportent au contexte du RE	Au moment de l'évaluation. Ce critère doit être respecté préalablement à toute utilisation.
Protection de la vie privée (p. ex. suppression des ICPC)	Au moment de l'échange, s'il y a lieu. La suppression est obligatoire pour ce qui a trait aux ICPC contenues dans un RPF communiqué à l'extérieur du CST. Les clients du CCC qui reçoivent ces RPF peuvent demander ces INC en faisant appel au processus lié aux mesures consécutives. Autrement, aucune suppression n'est requise lorsque les ICPC doivent servir à des fins de cybersécurité, mais il convient alors d'appliquer d'autres mesures de protection de la vie privée, par exemple, des restrictions quant aux destinataires des informations.
Expurgation	S'applique au moment de l'échange ou lorsque l'utilisation par la cybersécurité nécessite que les informations soient nettoyées dans le but de protéger les intérêts du CST.
Sérialisation	Au moment de l'acquisition. Automatiquement appliquée par les systèmes du CST. À toutes les données reçues par le CST, on attribue automatiquement un identifiant unique ainsi que des informations concernant leur origine [exemple d'opérations du CST] les contrôles d'accès, s'il y a lieu; le volet du mandat en vertu duquel les données ont été acquises; la date et l'heure de l'acquisition; et les exigences en matière d'utilisation et de traitement
Restrictions de diffusion	S'appliquent à l'utilisation et à la diffusion des informations par le volet cybersécurité au moment de l'échange ou à une étape ultérieure. Peuvent comprendre l'application de mesures préapprouvées. Peuvent être appliquées aux RPF par une plateforme de préparation de rapports; imposent des restrictions sur les modalités d'utilisation et de diffusion des informations du CST.

[69] EPM, RE, section 27.8.

Diffusion approuvée	Au moment de l'échange. Le niveau de l'autorité de diffusion dépend de la nature des informations. Voir le tableau de la section 27.8 du chapitre consacré au RE, dans l'EPM.

Examens internes portant sur les échanges d'informations

8. (~~TS~~) Les échanges d'informations en interne entre divers volets sont assujettis à des examens que le CST réalise en interne sur les échanges automatisés, mais aussi sur les interrogations de données. Le groupe Conformité du SIGINT, l'équipe responsable de la conformité interne des activités relevant du volet RE, a examiné les interrogations provenant du CST pour les années 2019 et 2020, et a confirmé la conformité des activités d'interrogation[70]. Le Programme organisationnel de conformité des activités (POCA) n'a pas été en mesure de prioriser les examens de surveillance de la conformité au cours des deux derniers exercices, ce qui l'a empêché de surveiller d'autres activités pouvant poser un risque élevé en matière de conformité[71].

9. (~~TS~~) Les techniques d'échange automatisé sont également assujetties à des examens. En effet, tous les 12 mois, l'équipe Conformité du SIGINT est tenue de revalider toutes les occurrences d'échanges automatisés survenues entre le volet RE et le volet cybersécurité[72]. Le plus récent examen portant sur la période allant de juillet 2019 à septembre 2020 a permis de confirmer que les [nombre] d'échange automatisé étaient conformes aux exigences de la politique, à l'exception [nombre] que le CST n'a pas été en mesure d'évaluer[73].

[70] CST, réponse à la DI-11, 19 mars 2021, Q5.
[71] CST, réponse à la DI-11, 19 mars 2021, Q5. Toutefois, pendant la période couverte par le présent examen, le CST a indiqué que l'équipe Surveillance de la conformité et gestion des incidents du POCA (IPOC[redacted]) n'avait pas encore rédigé le Internal Compliance Monitoring Plan pour l'exercice 2021-2022 et se propose d'inscrire l'examen des interrogations dans le plan.
[72] EPM, RE, section 29.2. Le premier examen de ce type a été réalisé de juin 2018 à juin 2019, voir *Automated Sharing Between Part (a) and Part (b), Examen réalisé par l'équipe Conformité du SIGINT,* CST, réponse à la DI-04, 20 février 2020, Q1.
[73] *Annual Validation of Automated Sharing (2020) Examen réalisé par l'équipe Conformité du SIGINT*, CST, réponse à la DI-13, 21 janvier 2021, Q2. Rappelons que les difficultés liées à la pandémie se sont répercutées sur la posture opérationnelle du CST en matière de dotation des postes essentiels. Dans ce contexte, l'équipe Conformité SIGINT a réalisé un examen simplifié ayant pour but de valider toutes les occurrences d'échange automatisé. Pour ce qui a trait aux occurrences qui avaient été examinées et jugées conformes en 2019, l'équipe Conformité du SIGINT a simplement cherché à obtenir, du directeur des opérations, une attestation confirmant qu'aucune modification importante n'avait eu lieu depuis le plus récent examen. Dès lors que le directeur des opérations produit une telle attestation, les occurrences sont réputées comme étant conformes.

ANNEXE F : MÉTHODES ET PROCESSUS D'ÉCHANGE

1. (~~TS~~) Dans la présente section sont décrits les processus et les méthodes employés par le CST pour échanger des informations entre le volet RE et le volet cybersécurité. De fait, le Centre dispose d'une multitude de systèmes, de méthodes et de processus qui facilitent les échanges d'informations, que celles-ci soient nettoyées ou non, entre ces volets. Or, il faut savoir que les processus décrits plus bas ne sont pas statiques. En effet, les systèmes, les méthodes et les processus du CST peuvent évoluer[74].

2. (~~TS~~) En général, l'accès aux informations de chacun de ces volets est contrôlé [redacted] [lié à un avis ou conseil juridique] [redacted]

3. (~~TS//SI~~) Par exemple, au Centre pour la cybersécurité, [redacted] [description des opérations du CST] [redacted][75]. [redacted][76].

4. (NC) Tel qu'il est stipulé à l'article 24 de la *Loi sur le CST*, le Centre doit avoir mis en place des mesures visant à protéger la vie privée des Canadiens et des personnes se trouvant au Canada lorsqu'il utilise des informations se rapportant à ces personnes pour atteindre des objectifs fixés pour le volet RE ou le volet cybersécurité du mandat.

5. (~~TS~~) La suppression ou la restriction des ICPC ne sont pas requises par la politique du CST lorsqu'il s'agit d'échanger des informations en interne. En effet, il est de pratique courante d'échanger des ICPC sans suppression entre le volet RE et le volet cybersécurité[77]. Au CST, bien que la politique ne l'exige aucunement, on invite les analystes à anonymiser ou à supprimer les renseignements personnels lorsque ceux-ci ne sont pas essentiels à la compréhension du contexte ou de la nature d'un enjeu[78]. Le CST reconnaît que la suppression et la restriction

[74] Pour voir un exemple, voir CST, réponse à la DI-11, 2 février 2021.
[75] CST, réponse à la DI-11, 2 février 2021, Q11.
[76] CST, réponse à la DI-06, 17 septembre 2020, Q4. [description des opérations du CST] [redacted]
[77] CST, réponse à la DI-09,19 octobre 2020, Q6.
[78] [description des opérations du CST] [redacted]

constituent des pratiques exemplaires, mais qu'elles sont non obligatoires. Par conséquent, le CST estime que le fait de n'avoir ni supprimé, ni restreint, ni anonymisé les informations échangées entre divers volets ne constitue pas en soi une infraction à la loi[79].

Accès intervolets aux données brutes du SIGINT et du Centre pour la cybersécurité

6. (~~TS~~) Lorsqu'ils accèdent aux données d'un autre volet qui ne figurent pas dans un rapport (c.-à-d. les PSC ou les PCC), les analystes sont tenus de respecter les exigences de la politique qui s'appliquent aux données qu'ils sont appelés à consulter.

7. (~~TS//SI~~) Pour ce qui a trait au volet RE, [description des opérations du CST]

8. (~~TS//SI~~) Par exemple, [description des opérations du CST]

[80].

9. (~~TS//SI~~) Lorsqu'ils analysent des données de RE brutes, les membres du personnel du Centre pour la cybersécurité doivent se conformer aux autorisations et aux exigences s'appliquant au renseignement étranger. L'utilisation, le traitement et la conservation de ces informations sont également assujettis aux restrictions s'appliquant aux données du renseignement étranger[81].

10. (~~TS//SI~~) le personnel du SIGINT peut consulter et utiliser les systèmes du Centre pour la cybersécurité à condition de répondre aux critères énoncés à la section 26.1 de l'EPM, Cybersécurité[82]. L'accès aux systèmes du Centre pour la cybersécurité et aux données de cybersécurité brutes est semblablement réservé aux individus qui ont démontré un besoin de connaître, qui ont suivi les formations prescrites et qui ont réussi aux épreuves de connaissances. [description des opérations du CST]

[83].

[79] CST, réponse à la DI-08, 8 octobre 2020, Q4.
[80] CST, réponse à la DI-11, 2 février 2021, Q11. Voir également EPM, RE, section 3.3.
[81] EPM, RE, sections 20 et 26.5.2.
[82] EPM, Cybersécurité, sections 26.1 et 26.2.
[83] CST, réponse à la DI-11, 2 février 2021, Q11.

Rapports – PCC et PSC

11. (NC) Les informations conservées sont échangées en interne suivant des processus officiels de rapports donnant lieu, notamment, à des PSC (ce qui comprend les RPF) ou à des PCC.

12. (~~TS//SI~~) Les membres du personnel du Centre pour la cybersécurité qui sont assujettis aux exigences en matière de cybersécurité peuvent également être des clients internes n'ayant aucun accès aux données RE brutes[84]. Des informations du renseignement étranger sont échangées en tant que PSC avec des membres du personnel de la cybersécurité, ce qui signifie que les informations sont conformes aux exigences de la politique du CST en matière de diffusion, lesquelles prévoient la suppression et une approbation, et qu'elles ont été assujetties aux restrictions imposées aux données de renseignement. Pendant la période visée par le présent examen, [nombre] PSC ont reçu une autorisation de diffusion par le volet RE et ont été mis à la disposition de membres du personnel œuvrant au sein du volet cybersécurité[85].

13. (~~TS//SI~~) Des informations de la cybersécurité peuvent être incluses dans des rapports et être diffusées auprès des membres du personnel SIGINT, pour être ultérieurement utilisées en tant que PCC dans le cadre d'activités du volet RE. Les informations diffusées par l'intermédiaire de PCC doivent répondre aux exigences de la politique du CST en matière de diffusion. Or, leur utilisation ultérieure doit être compatible avec les usages en vigueur au volet cybersécurité du mandat du CST et doit servir à la promotion des priorités du GC[86]. Pendant la période visée par le présent examen, nombre PCC ont été diffusés auprès de destinataires autorisés du SIGINT[87].

Réception des identifiants ayant été éliminés des rapports

14. (~~TS~~) Les ICPC qui ont été supprimées des RPF diffusées dans SLINGSHOT[88] peuvent être fournies aux clients internes du CST moyennant une demande soumise par l'intermédiaire du processus de divulgation externe des INC. Il s'agit là du seul mécanisme par lequel les renseignements personnels supprimés peuvent être obtenus et diffusés. En l'occurrence, les ICPC supprimées peuvent être obtenues en soumettant une demande à l'équipe du Bureau d'intervention du groupe Communication d'informations (D2A). En outre, le demandeur doit faire état des fondements juridiques et des motifs opérationnels qui justifient sa demande avant de

[84] Notons que les catégories des partenaires internes (faisant partie de la CPS) et des clients internes qui reçoivent des rapports de RE ne sont pas mutuellement exclusives.

[85] Il ne faut toutefois pas conclure que le personnel du CCC aurait accédé à certains, voire à tous ces rapports. Or, si l'on en juge aux permissions qui leur ont été accordées, les membres du personnel du CCC auraient accès aux rapports de SLINGSHOT aux fins d'une éventuelle utilisation dans le contexte du volet cybersécurité. Du reste, l'OSSNR n'a pas été en mesure de vérifier plus avant les occurrences d'utilisation ou de consultation de ces rapports.

[86] EPM, Cybersécurité, section 26.2.

[87] Certes, ces rapports ont été mis à la disposition de destinataires autorisés du SIGINT, mais il ne faut pas forcément conclure que tous les éléments ont été consultés ou utilisés par le SIGINT aux fins du renseignement étranger. [description des opérations du CST] Du reste, l'OSSNR n'a pas été en mesure de vérifier plus avant les occurrences d'utilisation ou de consultation de ces rapports.

[88] [description des opérations du CST]

recevoir les informations non supprimées[89]. Entre le 1er août 2019 et le 1er août 2020, [description des opérations du CST][90].

15. (~~TS~~) Même s'il est essentiellement le même que celui qui est employé aux fins du processus de comunication externe, le mécanisme par lequel est diffusée cette information est plutôt considéré comme donnant lieu à une utilisation interne des informations et non à une divulgation en tant que telle. Il n'est donc pas nécessaire que les exigences s'appliquant au régime de divulgation visé aux articles 43 à 46 de la *Loi sur le CST* soient respectées pour que les informations supprimées soient divulguées auprès de clients internes du CST[91].

Rapports conjoints

16. (~~TS//SI~~) Les informations peuvent également être échangées entre le volet renseignement étranger et le volet cybersécurité aux fins de diffusion de renseignement étranger consécutivement aux autorités en matière de cybersécurité. Or, ces informations du renseignement étranger doivent être d'abord utilisées à des fins relevant de la sphère du renseignement étranger. Dès lors, elles peuvent être mises à la disposition du personnel du CCC dans le cadre du volet cybersécurité. Ce n'est que dans un troisième temps que ces informations peuvent être diffusées en vertu desdites autorités[92].

17. (~~TS//SI~~) Pour chacun des volets, l'approbation des échanges visant les informations du renseignement étranger aux fins du volet cybersécurité du mandat doit se soumettre aux autorités d'approbation compétentes en matière de diffusion[93]. [description des opérations du CST][94].

Échanges automatisés (types de PSC ou de PCC)

18. (~~TS~~) La politique du CST définit les échanges automatisés comme suit : [Traduction] « utilisation de techniques ou de processus automatisés pour faciliter la diffusion de [rapports communicables][95] ».

19. (~~TS//SI~~) Le CST a recours à une pluralité de mécanismes automatisés pour échanger des informations entre divers volets. [description des opérations du CST]

20. (~~TS//SI~~) [description des opérations et des systèmes du CST][96] :

[89] EPM, RE, section 28.7; EPM, Cybersécurité, section 25.4.6; CST, réponse à la DI-11, 17 novembre 2020, Q9.
[90] CST, réponse à la DI-08, 10 mars 2021, Q1.
[91] DSJ du CST, réponse à la DI-6, 16 septembre 2020, Q3; CST, réponse à la DI-8, 10 mars 2021, Q2.
[92] EPM, RE, section 27.9.
[93] EPM, RE, section 27.8.1.
[94] CST, réponse à la DI-11, 17 novembre 2020, Q8.
[95] EPM, RE, section 29.2.
[96] Ces informations ont été rassemblées à partir des réponses suivantes : CST, réponse à la DI-7, 19 mars 2020, Q. 4 et 5; CST, réponse à la DI-11, 17 septembre 2020.

[redacted]

21. (~~TS//SI~~) [description des opérations et des systèmes du CST] [redacted]

22. (~~TS//SI~~) [description des opérations et des systèmes du CST] [redacted]

23. (TS//SI) [description des opérations et des systèmes du CST] [redacted]

24. (~~TS//SI~~) [description des opérations et des systèmes du CST] [redacted]

25. (~~TS//SI~~) [description des opérations et des systèmes du CST] [redacted]

26. (~~TS//SI~~) [description des opérations et des systèmes du CST] [redacted][97], [redacted]

[97] [description des opérations du CST] [redacted]

[redacted]

27. (~~TS//SI~~) [description des opérations et des systèmes du CST] [redacted]

[redacted]

28. (~~TS//SI~~) [description des opérations et des systèmes du CST] [redacted]

29. (~~TS//SI~~) [description des opérations et des systèmes du CST] [redacted]

30. (~~TS//SI~~) [description des opérations et des systèmes du CST] [redacted]

31. (~~TS//SI~~) [description des opérations et des systèmes du CST] [redacted]

[redacted]

[redacted]

32. (~~TS//SI~~) [description des opérations et des systèmes du CST] [redacted]

Autres modalités d'échange

33. (~~TS~~) Il se peut que les échanges d'informations entre deux volets soient réalisés suivant des méthodes plutôt informelles. En intensifiant la collaboration, les analystes se donnent accès à un bassin de connaissances plus important et particulièrement utile pour les deux volets du mandat. En l'occurrence, les analystes peuvent procéder à des échanges de connaissances générales sans avoir à les signaler[98]. En outre, la politique du CST prévoit des échanges d'analyses à l'occasion desquelles les analystes peuvent s'adresser à des partenaires œuvrant au sein d'un volet différent à des fins de collaboration sur des objectifs communs propices aux échanges d'informations[99]. Cependant, tout échange de données doit être conforme aux exigences s'appliquant à la diffusion de PCC ou de PSC, bien que les données ne soient pas tenues d'être diffusées par l'intermédiaire des systèmes officiels de diffusion des produits[100].

[98] CST, réponse à la DI-11, 17 novembre 2020, Q2.
[99] EPM, RE, section 27.14.1; CST, réponse à la DI-7, 19 mars 2021, Q4 et 5.
[100] Le CST a fait remarquer qu'à ce chapitre, les formulations de la politique du CST manquaient de clarté, mais que des précisions seraient apportées dans les versions à venir (EPM, Cybersécurité, section 26.2 : [Traduction] « bien que cette information ne doive pas être officiellement diffusée »). CST, réponse à la DI-14, 19 mars 2021, Q4.

ANNEXE G : POLITIQUE ET BALISES À RESPECTER DANS LE CAS DES ÉCHANGES INTERNES

1. (NC) La politique du CST indique que les ICPC peuvent être échangées en interne pour peu que les échanges respectent les balises énoncées ci-dessous. Or, rappelons que l'OSSNR n'a pas été en mesure de vérifier si ces balises ou les définitions connexes étaient conformes au droit, mais il n'est pas exclu que ce type de vérification ait lieu au cours des prochains examens. Au reste, l'OSSNR n'a pas non plus été en mesure de voir si les exigences de la politique avaient été respectées.

Du volet renseignement étranger au volet cybersécurité

2. (~~TS~~) Pour ce qui a trait au volet RE, les ICPC doivent avoir été jugées essentielles et pertinentes pour les activités de ce volet RE avant que les échanges aient lieu, conformément aux dispositions de l'alinéa 34(2)c) de la *Loi sur le CST*. D'après la politique du CST, les informations doivent avoir été considérées comme étant essentielles pour les affaires internationales, la défense ou la sécurité, ce qui comprend la cybersécurité[101]. Or, l'adjectif « essentiel » n'est pas défini dans la politique du CST, quoique celle-ci énonce les critères suivant lesquels il convient d'évaluer les ICPC dans un contexte de protection de la vie et de la sûreté des individus ou de défense contre les activités criminelles qui menacent la sécurité du Canada[102].

3. (~~TS~~) Pour qu'elles soient échangées aux fins des activités du volet cybersécurité du mandat, les ICPC de RE doivent être pertinentes pour le volet cybersécurité. Or, ces ICPC doivent être évaluées plus avant sur le plan de la nécessité dans le contexte du volet cybersécurité, ce qui permet de savoir si les informations sont nécessaires à la protection des systèmes du GC ou des systèmes désignés comme étant importants. Or, c'est en vertu de la politique qu'il y a lieu de décider d'appliquer les balises délimitant la sphère de nécessité visée au paragraphe 44(1) de la *Loi sur le CST*[103].

4. (~~TS~~) La politique du CST exige le respect du principe de nécessité, [redacted] [description des opérations du CST] Ces informations sont nécessaires à l'exercice du mandat de cybersécurité dans la mesure où elles contribuent à la protection des systèmes du GC, mais aussi des systèmes et réseaux d'importance (notamment le blocage de certains types de trafic). Toutefois, les individus et les entités identifiables ne sont pas les points de mire de l'activité[104]. Or, dans le contexte de la cybersécurité, le CST estime que le risque de préjudice à l'attente raisonnable en matière de protection de la vie privée de l'individu est relativement faible et que, par conséquent, le seuil de nécessité justifie la communication d'ICPC acquises par le RE vers le volet cybersécurité[105].

[101] Voir EPM, RE, section 18.7. Toutefois, la politique du CST renvoie spécifiquement aux communications privées et non aux ICPC.
[102] EPM, RE, section 18.7.
[103] CST, réponse à la DI-04, 17 septembre 2020, Q6 et Q7.
[104] CST, réponse à la DI-14, 19 mars 2021, Q5.
[105] CST, réponse à la DI-11, 19 mars 2021, Q14.

Du volet cybersécurité au volet renseignement étranger

5. (~~TS//SI~~) Dans le contexte du volet cybersécurité, les ICPC acquises en vertu d'une AM doivent avoir été jugées pertinentes, mais aussi essentielles avant tout échange[106], conformément au critère d'essentialité énoncé à l'alinéa 34(3)d) de la *Loi sur le CST*. Or, d'après la politique du CST, les ICPC sont considérées comme étant essentielles lorsque, sans elles, le CST ne serait en mesure de protéger ni les systèmes des institutions fédérales, ni les réseaux et systèmes d'importance, ni les informations électroniques que ces systèmes et réseaux contiennent[107]. Toutefois, les ICPC qui ne sont pas acquises en vertu d'une AM, notamment les renseignements sur les clients[108], ne doivent répondre qu'au critère de nécessité[109].

6. (~~TS~~) Les ICPC échangées sont également évaluées sur le plan de l'essentialité pour le volet RE (c.-à-d. essentiel pour les affaires internationales, la défense ou la sécurité), qu'une AM de cybersécurité ait été délivrée ou non. La décision d'évaluer plus avant les ICPC acquises par la cybersécurité sur le plan de l'essentialité et selon les critères du RE relève de la politique, [description des opérations du CST] [110].

7. (~~TS//SI~~) Comme l'a expliqué le CST, les ICPC acquises par la cybersécurité et échangées en interne en guise de soutien au volet RE ont pour objet de protéger les institutions fédérales ou les réseaux et systèmes d'importance, mais aussi les informations électroniques qui y sont conservées. Ces ICPC servent à identifier les menaces étrangères qui pèsent sur les systèmes canadiens[111], un objectif qui cadre parfaitement avec les [lié aux priorités du GC]

[106] CST, réponse à la DI-09, 19 octobre 2020, Q3.
[107] Selon la politique du CST, sont « essentielles » les informations dont le CST doit absolument disposer pour être en mesure de contribuer à la protection des systèmes des institutions fédérales ou des réseaux et systèmes d'importance, mais aussi des informations électroniques qui y sont conservées. EPM, Cybersécurité, section 9.2.2.
[108] Le « client » est une entité qui fait appel aux services offerts par le Centre pour la cybersécurité après avoir conclu une entente à titre de client (par exemple, les institutions fédérales et les responsables des réseaux et systèmes d'importances peuvent être des clients). Le terme « client » s'applique également aux consommateurs, aux abonnés et à ceux qui ont accès aux services du Centre pour la cybersécurité, notamment aux cyberalertes.
[109] CST, réponse à la DI-7, 19 mars 2021, Q4. Selon la politique du CST, sont « nécessaires » les informations dont les intervenants responsables de la protection des institutions fédérales et des systèmes désignés comme étant d'importance ont besoin pour comprendre suffisamment les cyberactivités malveillantes, notamment, les schèmes de comportement, les capacités, les intentions ou les schèmes de vulnérabilité. EPM, Cybersécurité, section 10.3.1.
[110] CST, réponse à la DI-14, 19 mars 2021, Q5; CST, réponse à la DI-11, 19 mars 2021, Q.14.
[111] CST, réponse à la DI-14, 11 février 2021, Q3.

ANNEXE H : ÉCHANGES INTERNES DES ICPC AU CST