National Security and Intelligence Review Agency

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

Examen des solutions réseau du CST et des activités connexes en matière de cybersécurité et d'assurance de l'information

OSSNR // Examen 2021-17

SECRET//RÉSERVÉ AUX CANADIENS// SECRET PROFESSIONNEL DE L'AVOCAT

Table des matières

Liste des sigles et acronymes

AELP – Attestation des exigences prévues par la loi et la politique

[redacted]

ARPVP – Attente raisonnable en matière de protection de la vie privée [pour un Canadien ou une personne se trouvant au Canada]

BCCST – Bureau du commissaire du Centre de la sécurité des télécommunications [1996 à 2019]

BCP – Bureau du Conseil privé

CAI – Cybersécurité et assurance de l'information [un volet du mandat du CST; article 17 de la Loi sur le CST]

CCC – Centre canadien pour la cybersécurité (Centre pour la cybersécurité), relève du CST

[redacted]

CP – Communication privée [voir le glossaire]

CPSNR – Comité des parlementaires sur la sécurité nationale et le renseignement

CST – Centre de la sécurité des télécommunications

DI – Demande d'information

[redacted]

EIUI – Équipe d'intervention d'urgence en informatique

EM – Expert en la matière

EPM – Ensemble des politiques relatives à la mission [CST]

GC – Gouvernement du Canada

IAP – Information accessible au public [voir le glossaire]

IC – Indicateur de compromission

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

IMI – Infrastructure mondiale d'information

LDN – *Loi sur la défense nationale* [source du pouvoir légal du CST avant la Loi sur le CST]

Loi sur le CST – *Loi sur le Centre de la sécurité des télécommunications*

[redacted]

MinDN – Ministre de la Défense nationale

[redacted]

PCC – Produit de cybersécurité communicable

PE – Protocole d'entente

SDI – Système désigné comme étant important [ainsi désigné par le ministre au titre du paragraphe 21(1) de la Loi sur le CST]

SI – Solution infonuagique

SIGINT – Signaux électromagnétiques [pour *Signals Intelligence*]

SPC – Services partagés Canada

SR – Solution réseau

SSH – Solution du système hôte

Glossaire

Attente raisonnable d'un Canadien ou d'une personne se trouvant au Canada en matière de protection de la vie privée (ARPVP). L'article 8 de la *Charte canadienne des droits et libertés* indique que chacun a le droit à la protection contre les fouilles, les perquisitions ou les saisies abusives. Aux fins de l'article 8, constitue une « fouille » ou une « perquisition » toute intervention de l'État qui porte atteinte à « l'attente raisonnable d'une personne en matière de protection de la vie privée » (ARPVP). Comme il a été dit précédemment, l'information à l'égard de laquelle un Canadien ou une personne se trouvant au Canada a une ARPVP est exclue de la définition de la notion d'IAP dans la Loi sur le CST. S'agissant de la réalisation du volet touchant le renseignement étranger ou du volet touchant la cybersécurité du mandat organisationnel, les paragraphes 22(3) et 22(4) de la Loi sur le CST interdisent les activités qui portent atteinte à l'ARPVP d'un Canadien ou d'une personne se trouvant au Canada, à moins que ces activités aient été autorisées par le Ministre, conformément à ce qui est énoncé dans la Loi.

Collectivité des cinq. Terme désignant le partenariat qui regroupe le Canada, les États-Unis, le Royaume-Uni, l'Australie et la Nouvelle-Zélande à des fins d'échange de renseignement.

Communication privée (CP). Selon l'article 183 du *Code criminel*. Communication orale ou télécommunication dont l'auteur se trouve au Canada, ou destinée par celui-ci à une personne qui s'y trouve, et qui est faite dans des circonstances telles que son auteur peut raisonnablement s'attendre à ce qu'elle ne soit pas interceptée par un tiers.

Incidemment. Selon le paragraphe 23(5) de la Loi sur le CST : « S'agissant de l'acquisition de l'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. »

Information accessible au public (IAP). Selon l'article 2 de la Loi sur le CST, l'IAP désigne l'information « [p]ubliée ou diffusée à l'intention du grand public, accessible au public dans l'infrastructure mondiale de l'information ou ailleurs ou disponible au public sur demande, par abonnement ou achat. Ne vise pas l'information à l'égard de laquelle un Canadien ou une personne se trouvant au Canada a une attente raisonnable en matière de protection de la vie privée. »

Ministre. Dans le présent rapport, le terme « Ministre » désigne le ministre de la Défense nationale.

Propriétaire de système. Dans le présent rapport, la notion de « propriétaire de système » désigne un ministère ou un organisme du gouvernement du Canada ou encore les entités qui les composent, pour peu qu'ils exercent des fonctions de gestion ou de protection des systèmes informatiques, ce qui peut comprendre les systèmes d'autres ministères ou organismes. S'agissant du programme de cybersécurité responsable des SR du CST, [redacted] ministères ou organismes constituent des « partenaires » du CST dans le contexte de la mise en œuvre de ce programme de cybersécurité responsable des SR (« partenaires SR »). Les partenaires SR possèdent des systèmes faisant partie d'une multiplicité de réseaux connectés à Internet; certains des partenaires offrent également ces

services de protection réseau par SR à d'autres ministères ou organisations. Les [redacted] partenaires SR sont SPC, [redacted] et le CST.

Solution. Dans le présent rapport, la notion de « solution » désigne un système faisant appel à des composantes matérielles et logicielles qui permettent de surveiller les cybermenaces et d'y réagir le cas échéant. Cette notion peut faire appel à un large éventail de capacités particulières.

Utilisateur de système. Dans le présent rapport, le terme « utilisateur de système » désigne une personne qui se sert d'un système informatique ou d'un réseau.

I. SOMMAIRE

1. Le gouvernement du Canada considère la cybersécurité comme l'un des plus importants défis auxquels le Canada et les Canadiens font face sur le plan de l'économie et de la sécurité nationale. C'est d'ailleurs dans ce contexte que l'entrée en vigueur, en 2019, de la *Loi sur le Centre de la sécurité des télécommunications* (Loi sur le CST) donne lieu à des modifications substantielles aux pouvoirs que le Centre de la sécurité des télécommunications (CST, le Centre) exerce dans le cadre de ses activités en matière de cybersécurité et d'assurance de l'information (CAI). Certes, l'acquisition et l'analyse d'importants volumes d'information sont essentielles lorsqu'il s'agit de reconnaître et de prévenir les cybermenaces, mais il faut également comprendre que les activités de CAI sont souvent intrusives et qu'elles soulèvent d'importants enjeux sur le plan de la protection de la vie privée.

2. Le présent examen est le premier que l'OSSNR réalise au sujet des activités CAI du CST. De plus, l'OSSNR a inclus Services partagés Canada (SPC) dans la portée de l'examen, compte tenu de son rôle en tant que propriétaire de systèmes dans une large part des réseaux du gouvernement du Canada. En l'occurrence, l'OSSNR examine les activités de SPC pour la toute première fois.

3. À l'origine, l'examen devait se concentrer sur l'une des trois principales solutions de cybersécurité que le CST emploie pour détecter et contrer les menaces envers l'information numérique et les infrastructures de l'information que le Centre est appelé à protéger, à savoir les solutions réseau (SR). Ce faisant, l'examen a été l'occasion de conceptualiser le cycle de vie de l'information de cybersécurité qui est initialement saisie par les capteurs SR, puis traitée par divers systèmes sur lesquels repose l'écosystème de cyberdéfense du CST.

4. En définitive, l'OSSNR conclut que le CST exploite un ensemble complet et intégré de systèmes, d'outils et de capacités de cybersécurité qui est apte à garantir une protection contre les cybermenaces et qui comporte des mesures visant à protéger la vie privée des Canadiens et des personnes se trouvant au Canada.

5. L'OSSNR a également analysé deux importants domaines thématiques : la transparence et la vie privée. L'OSSNR a formulé des conclusions et des recommandations en matière de transparence relativement à certaines des informations fournies par le CST au ministre de la Défense nationale et aux engagements pris par le Centre dans le cadre de ses demandes d'autorisations ministérielles en prévision d'activités de cybersécurité du CST devant avoir lieu dans l'infrastructure fédérale.

6. L'OSSNR a aussi examiné un cas particulier, celui d'activités d'acquisition, par le CST, d'information de cybersécurité auprès d'une source externe, information qui aurait pu susciter une attente raisonnable de Canadiens ou de personnes se trouvant au Canada en matière de protection de la vie privée. Le CST a poursuivi ces activités après que le commissaire au renseignement eut établi qu'il ne pouvait pas les approuver tel qu'elles avaient été proposées dans la demande d'autorisation ministérielle. L'OSSNR a formulé des conclusions et fait des recommandations concernant la façon dont le CST a traité cette difficulté qui s'est posée en raison d'une incohérence dans la Loi sur le CST, laquelle contraint toute autorisation à n'être délivrée que pour cette activité d'acquisition particulière au titre du volet CAI du mandat du CST.

7. Bien que le CST n'ait que partiellement répondu aux attentes de l'OSSNR au chapitre de la réactivité dans le cadre du présent examen, l'Office de surveillance a été en mesure de vérifier de façon indépendante les informations du CST qui ont été produites tout au long de l'examen.

II. INTRODUCTION

8. Le Centre de la sécurité des télécommunications (CST) ainsi que le Centre canadien pour la cybersécurité (CCC ou Centre pour la cybersécurité) qui relève du CST, ont pour mandat de protéger l'information électronique et les systèmes d'information des institutions fédérales canadiennes, de même que d'autres systèmes d'importance pour le gouvernement du Canada (GC). Avant la création de l'OSSNR, en 2019, c'est le Bureau du commissaire du Centre de la sécurité des télécommunications (BCCST) qui réalisait les examens annuels portant sur les activités de cyberdéfense du CST; le plus récent de ces examens a d'ailleurs été réalisé au début de 2019[1].

9. L'adoption de la *Loi sur le Centre de la sécurité des télécommunications* (Loi sur le CST) a donné lieu à des modifications substantielles aux pouvoirs que le CST exerce quant au volet de cybersécurité et d'assurance de l'information de son mandat (ce que l'on désignera désormais par le terme « volet cybersécurité » ou « volet CAI »)[2]. Le présent examen est le premier que l'OSSNR réalise au sujet des activités CAI exercées par le CST et par le Centre pour la cybersécurité, lequel relève du CST.

10. Le CST se sert d'une multiplicité d'outils, de savoir-faire et de services lorsqu'il exerce les fonctions relevant du volet CAI de son mandat. À titre de complément à ses activités de cybersécurité, le CST a recours à trois types de solutions de cybersécurité[3] : les solutions réseau (SR), les solutions du système hôte (SSH) et les solutions infonuagiques (SI). Les informations générées par ces trois solutions sont combinées à d'autres types d'information pour ensuite alimenter les systèmes de détection et de prévention des intrusions du CST. Ces systèmes permettent ensuite au CST de protéger l'information électronique et les infrastructures de l'information des institutions fédérales, mais aussi les systèmes d'importance du GC.

Fondements législatifs

11. Le présent examen a été réalisé en application des dispositions énoncées au paragraphe 8(1) et à l'alinéa 8(1)b) de la *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement* (Loi sur l'OSSNR)[4].

Portée de l'examen

12. Au départ, compte tenu du recours aux SR dans l'ensemble des réseaux fédéraux depuis 2006[5], l'OSSNR a choisi d'axer son examen sur ce type de solution[6]. Or, à mesure que les

---

[1] Bureau du commissaire du Centre de la sécurité des télécommunications, *Annual Review of the Communications Security Establishment's Cyber Defence Activities under the 2017-2018 Cyber Defence Activities Ministerial Authorization*. Dossier nº 2200-127. Cet examen a conclu que le CST s'était conformé à la loi et n'a donné lieu à aucune recommandation.
[2] *Loi sur le Centre de la sécurité des télécommunications*, L.C. 2019, ch. 13, art. 76 [Loi sur le CST]. Voir l'article 17.
[3] Le terme « solution » désigne un système faisant appel à des composantes matériels et logiciels qui permettent de surveiller les cybermenaces et d'y réagir le cas échéant. Une solution peut faire appel à un large éventail de capacités particulières.
[4] *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement,* L.C. 2019, ch. 13, art. 2.
[5] Pour obtenir de plus amples détails ainsi que le calendrier de développement des capteurs de défense, voir CPSNR, « Rapport spécial sur le cadre et les activités du gouvernement pour défendre ses systèmes et ses réseaux contre les cyberattaques », 11 août 2021. Consultable à l'adresse suivante : https://www.nsicop-cpsnr.ca/reports/rp-2022-02-14/intro-fr.html, page 104.
[6] Rapport annuel 2021 de l'OSSNR, page 33, disponible en ligne à l'adresse suivante : https://nsira-ossnr.gc.ca/wp-content/uploads/Rapport-Annuel-2021-PDF.pdf.

examinateurs de l'OSSNR en apprenaient davantage sur les activités de cybersécurité du CST de même que sur les systèmes et les techniques employées en l'occurrence, il devenait manifeste que la portée initiale de l'examen était trop étroite. Par exemple, en 2019-2020, dans la demande qu'elle a présentée au Ministre pour l'approbation d'activités de cybersécurité dans l'infrastructure fédérale, la cheffe du CST a indiqué que les trois solutions du CST s'appuyaient sur trois sphères principales d'activités : la défense dynamique, l'analyse et la conservation d'information[7]. Bien que les SR constituent une source unique d'information sur les menaces pesant sur l'écosystème de cyberdéfense du CST, l'OSSNR a établi qu'il serait préférable d'examiner les SR dans le contexte plus large des activités CAI du CST. En définitive, le présent examen a laissé de côté l'analyse des solutions infonuagiques et des solutions du système hôte. En revanche, en se concentrant sur les SR, les examinateurs ont pu élargir la portée de leur examen en s'intéressant de façon générale aux activités CAI, pour peu qu'elles aient un lien avec les SR. À titre d'exemple, la deuxième partie de la section Analyse porte sur une étude de cas ayant trait à des sources de données externes qui sont utilisées dans le but d'améliorer les fonctions SR.

13. En première partie du rapport figure un aperçu des SR et des activités connexes du CST en matière de CAI, ce qui comprend les cadres applicables sur le plan juridique et stratégique. Cette section formule une conclusion générale concernant les activités SR et CAI. Ensuite, la section Analyse donne de plus amples détails sur certaines conclusions et recommandations, et se concentre sur le traitement de l'information se rapportant à un Canadien ou à une personne se trouvant au Canada (ICPC), laquelle information peut susciter une attente raisonnable en matière de protection de la vie privée (ARPVP) de la part d'un Canadien ou d'une personne se trouvant au Canada. En outre, l'analyse se divise en deux thèmes :

- la transparence quant à la nature de l'information collectée par une SR;
- l'acquisition, à partir de sources externes, d'information pouvant susciter une ARPVP de la part d'un Canadien ou d'une personne se trouvant au Canada.

14. Les annexes contiennent de l'information contextuelle ou complémentaire. Il convient de noter que l'annexe A décrit, étape par étape, le processus suivant lequel l'information captée par les SR en vient à alimenter l'écosystème de cyberdéfense, et ce, depuis la collecte initiale de ladite information jusqu'à la publication ou la communication de rapports fondés sur l'analyse de l'information en question. Quant à l'annexe B, elle traite de l'utilisation de l'information de cybersécurité dans les divers volets du mandat du CST[8].

Méthodologie

15. La période visée par l'examen s'étend du 1er août 2019 au 17 juin 2021, quoique l'OSSNR s'est également penché sur de l'information, pour peu qu'elle fût pertinente, concernant des éléments antérieurs ou postérieurs à cette période. Dans le présent rapport, le cas particulier exploré dans la partie « Attente raisonnable en matière de protection de la vie privée » de la section Analyse résulte d'activités menées pendant la période visée par l'examen, mais le cas en soi ainsi que la réaction du CST ont nettement eu lieu *après* le mois de juin 2021.

16. L'OSSNR a analysé un large éventail d'information dont disposait le CST, ce qui comprend nombre de documents portant sur ce qui suit : les processus, les conseils juridiques, les informations techniques, les registres d'information et les rapports de conformité, pour ne nommer que ceux-là. Rappelons qu'au nombre de ces documents, il faut également compter les demandes d'autorisations

[7] CST, *Demande concernant les activités de cybersécurité du CST dans les infrastructures fédérales pour 2019-2020*, sections IX à XI.

[8] La Loi sur le CST fait état des cinq volets du mandate du CST à savoir le renseignement étranger, les activités CAI, les cyberopérations défensives, les cyberopérations actives de même que l'assistance technique et opérationnelle.

ministérielles que la cheffe du CST a présentées au Ministre relativement à des activités de cybersécurité dans des infrastructures fédérales. Les documents remis à l'OSSNR comprenaient aussi de la correspondance survenue entre le CST et d'autres entités du gouvernement du Canada qui tiraient parti ou envisageaient de tirer parti des SR du CST et des solutions de cybersécurité connexes. De plus, l'OSSNR a eu droit à sept présentations consistant en des séances d'information ou des démonstrations techniques de la part d'experts du CST.

17. Services partagés Canada (SPC) a également été visé par l'examen compte tenu du rôle de propriétaire de systèmes qu'il tient pour une large part des réseaux du GC. L'OSSNR a analysé les documents fournis par SPC; il a également eu droit à une séance d'information et à une démonstration technique de la part d'experts de SPC. En plus de s'avérer pertinente quant à certaines sphères d'analyse de l'OSSNR, l'information de SPC a permis de corroborer de l'information que l'OSSNR avait reçue du CST.

18. Conformément aux dispositions de l'article 13 de la Loi sur l'OSSNR, l'Office de surveillance a coopéré avec le Secrétariat du Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR) de sorte à éviter le dédoublement des tâches[9]. Ainsi, le rapport évite, dans la mesure du possible, de répéter les informations qui étaient déjà traitées dans le document du CPSNR paru en août 2021 et intitulé « Rapport spécial sur le cadre et les activités du gouvernement pour défendre ses systèmes et ses réseaux contre les cyberattaques »[10].

Énoncés généraux

19. Pour ce qui a trait au présent examen, on peut dire globalement que le CST a partiellement répondu aux attentes de l'OSSNR sur le plan de la réactivité. Or, bien que le CST n'ait répondu que partiellement, voire aucunement à bon nombre des attentes de l'OSSNR sur le plan de la réactivité pendant la première moitié du présent examen, il convient de préciser que pendant la seconde moitié de l'examen, le degré de réactivité du CST a répondu aux attentes de l'OSSNR. Puisqu'il faisait appel à SPC pour la première fois aux fins d'un examen, l'OSSNR a dû composer avec des difficultés et des retards quant à la mobilisation de SPC. Toutefois, dès lors que les contacts d'usage ont été établis avec ses représentants, SPC en est venu à répondre aux attentes de l'OSSNR sur le plan de la réactivité.

20. L'OSSNR a été en mesure de vérifier l'information reçue en cours d'examen selon des modalités qui ont satisfait les attentes de l'OSSNR.

III. APERÇU DES SR ET DES ACTIVITÉS CAI

Conclusion n° 1 : L'OSSNR conclut que le CST exploite un ensemble complet et intégré de systèmes, d'outils et de capacités de cybersécurité qui est apte à garantir une protection contre les cybermenaces et qui comporte des mesures visant à protéger la vie privée des Canadiens et des personnes se trouvant au Canada.

En quoi le programme CAI du CST consiste-t-il?

21. Le gouvernement du Canada considère la cybersécurité comme « l'un des enjeux les plus sérieux auxquels [le Canada et les Canadiens font] face sur le plan de l'économie et de la sécurité

[9] *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement,* L.C. 2019, ch. 13, art. 2.
[10] Voir CPSNR, « Rapport spécial sur le cadre et les activités du gouvernement pour défendre ses systèmes et ses réseaux contre les cyberattaques », 11 août 2021. Consultable à l'adresse suivante : https://www.nsicop-cpsnr.ca/reports/rp-2022-02-14/intro-fr.html.

nationale »[11]. Tel qu'il était décrit dans l'Évaluation des cybermenaces nationales 2023-2024 du CST, l'ampleur de la vulnérabilité face aux auteurs de cybermenaces s'est accentuée au cours des dernières années, et les Canadiens de même que les entités canadiennes continuent de prêter le flanc aux cybermenaces, principalement à la cybercriminalité (ce qui comprend les rançongiciels), ainsi qu'aux menaces provenant d'acteurs étatiques dans un contexte où les États se livrent une forte concurrence[12].

22. C'est en octobre 2018 que le GC a créé le Centre canadien pour la cybersécurité, lequel relève du CST. Par ailleurs, la création du Centre pour la cybersécurité a renforcé le rôle et les responsabilités relevant du programme du CST en matière de sécurité des technologies de l'information et du Centre canadien de réponse aux incidents cybernétiques, de même que certaines fonctions du Centre des opérations de sécurité de SPC. Aujourd'hui, le programme CAI du CST fournit à des entités du GC presque exclusivement – ainsi qu'à des systèmes considérés comme étant d'importance – un centre d'opérations de sécurité unifié et centralisé qui mise sur un ensemble complet d'outils manuels ou automatisés d'analyse et d'atténuation qui sont interconnectés. Le programme CAI, qui tire parti d'une intégration de l'information provenant des activités de renseignement étranger du CST, est responsable de la réception et du traitement ultérieur de volumes massifs de données issus d'une diversité de sources, ce qui a pour effet d'améliorer la reconnaissance des menaces et d'activer en temps réel les mesures visant à faire obstacle aux menaces. Les mesures de conformité, y compris celles ayant pour fonction de protéger la vie privée des Canadiens et des personnes se trouvant au Canada, sont greffées aux flux de données dès lors que les cyberincidents sont détectés, puis les étapes requises sont suivies dans le but d'atténuer les menaces en question, voire d'y remédier. L'annexe A décrit le cycle de vie de l'information qui provient des capteurs SR et qui est ensuite traitée au sein de l'écosystème de cyberdéfense du CST.

23. Le programme CAI prodigue également des conseils aux institutions du gouvernement, aux propriétaires de systèmes d'importance et au public concernant les cybermenaces et la cyberdéfense en plus de fournir des services allant de la simple publication de guides à l'application de mesures d'analyse et de soutien.

24. Dans certains cas, des entités autres que celles du GC, voire de l'étranger ont également recours aux solutions CAI du CST. Par exemple, depuis 2020, le National Cyber Security Centre du Royaume-Uni (R.-U.) a adopté et employé les solutions du système hôte (SSH) du CST pour renforcer la sécurisation des réseaux du gouvernement du R.-U.[13] [redacted] Bien que le présent examen n'ait pas permis d'évaluer l'efficacité ni des SR ni des systèmes et activités CAI du CST, l'OSSNR n'a tout de même relevé aucune information qui puisse mettre leur efficacité en doute. Au contraire, l'OSSNR a vu des cas particuliers où l'information acquise par l'intermédiaire des SR avait été mise à profit pour réagir à des cyberactivités malveillantes.

Que sont les solutions du CCC en matière de cybersécurité?

25. Le CST emploie les SR, les SSH et les SI, que l'on désigne souvent par le terme « capteurs », à des fins de cyberdéfense dans les infrastructures de l'information des institutions fédérales participantes et des systèmes d'importances désignés comme tels. Les trois solutions du CST s'ajoutent aux produits commerciaux conçus pour détecter les cyberactivités malveillantes, notamment les logiciels antivirus et pare-feu, et exercent deux fonctions : reconnaître les activités

[11] CST, Avant-propos du ministre de la Défense nationale, « Évaluation des cybermenaces nationales 2020, consultable à l'adresse suivante : https://www.cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2020.
[12] Ibid; message de la cheffe du Centre pour la cybersécurité.
[13] Page Web du CST, Capteurs au niveau de l'hôte, consultable à l'adresse suivante : https://cyber.gc.ca/fr/nouvelles-evenements/capteurs-au-niveau-de-lhote.

malveillantes et offrir une défense contre ces activités. Grâce à des analyses effectuées manuellement ou par automatisation, ces solutions permettent de reconnaître les comportements anormaux et, en cas de comportement malveillant, d'empêcher les activités identiques ou semblables de se reproduire.

26. Parmi les trois solutions, c'est la solution SR qui a été élaborée en premier, en 2006, puis déployée dans les réseaux du GC à partir de 2009[14]. La SR capte tout le trafic entrant et sortant d'un réseau donné, puis envoie cette information au CST par l'intermédiaire d'un TAP physique. De cette façon, le CST recueille un important volume d'information sur l'ensemble du trafic réseau, les courriels, l'information de navigation Internet, etc.[15]

27. La SR permet de collecter des paquets ainsi que les données de paquets. Les paquets sont l'élément de base des données acheminées dans les réseaux, y compris Internet. Les fichiers peuvent être reconstitués à partir des paquets, ce qui permet au CST de collecter des courriels, l'historique de navigation ou d'autres types de données (qu'elles soient entrantes ou sortantes) d'un réseau surveillé au moyen de SR. À la différence de la collecte de paquets par SR, la SSH collecte les données sur les activités et les événements qui ont lieu sur l'hôte, alors que la SI puise dans les journaux d'exploitation et les contenus des services infonuagiques[16]. La collecte de paquets par la SR permet aux analystes du CST d'interroger l'information qui ne se trouve que dans les données réseau et qui, par conséquent, ne se trouverait pas dans l'information collectée par la SSH ou la SI.

28. Les trois solutions de cyberdéfense du CST misent sur deux types de capacités : les capacités passives et les capacités dynamiques[17]. Les capacités passives font appel à des capteurs conçus pour détecter et analyser les cybermenaces au sein des systèmes du GC, ce qui facilite ultérieurement la reconnaissance des cybermenaces. Dans le contexte des SR, les capteurs saisissent le trafic réseau grâce aux capacités de détection du CST, lesquelles sont régulièrement alimentées par des données provenant de sources classifiées ou non classifiées, ce qui permet de reconnaître les activités pouvant poser problème. Dès lors qu'elles détectent des activités anormales ou suspectes, les SR passives sont aptes à alerter les analystes qui, à leur tour, peuvent intervenir manuellement ou déclencher des procédures automatisées.

29. La défense dynamique, que l'on désigne parfois par le terme « mesure d'atténuation », fait appel à des interventions automatisées contre les indicateurs de compromission (IC) reconnus en tant que menaces pour les systèmes et les réseaux du GC. L'intervention automatisée qui caractérise la défense dynamique fait appel à une multiplicité de moyens, notamment les suivants : détection et prévention des balayages malveillants[18]; blocage et filtrage des adresses IP et des domaines

---

[14] Ce type de solution se distingue des solutions du système hôte, lesquelles avaient été ponctuellement déployées dans des systèmes désignés comme étant d'importance pour le gouvernement du Canada, en application du paragraphe 21(1) de la Loi sur le CST.

[15] En 2021, le CST avait collecté en moyenne [redacted] par jour auprès des ministères fédéraux.

[16] Les capteurs SR collectent [redacted] Par conséquent, [redacted] Quant aux SSH et aux SI, elles ne recourent pas à la collecte de paquets.

[17] Les SR passives étaient anciennement désignées par le nom de code [redacted] Pour sa part, la défense dynamique était jadis désignée par le nom de code [redacted]. Notons que les modes passif et dynamique n'ont pas trait uniquement aux SR. En effet, au moment de procéder à l'examen, la défense dynamique était en cours de mise en œuvre pour les SSH et en cours de développement pour les SI. Quant aux capacités passives, elles existaient pour les trois types de capteurs : SR, SSH et SI. Selon la terminologie de l'industrie de la cybersécurité, les SR passives se compareraient aux systèmes de détection des intrusions réseau (NIDS pour *Network Intrusion Detection System*), alors que les SR dynamiques se compareraient plutôt aux systèmes de prévention des intrusions réseau (NIPS, pour *Network Intrusion Prevention System*). Or, les deux types de systèmes fonctionnent en complémentarité.

[18] Les auteurs de menace tentent fréquemment de balayer les réseaux à la recherche de vulnérabilités (p. ex. des logiciels périmés ou de l'information accidentellement exposée). Il est possible d'atténuer, voire de prévenir ces balayages pour peu qu'ils soient détectés.

malveillants; et détection et blocage de certains types de cyberattaques[19]. La défense dynamique exploite les informations tirées des SR, des SSH et des SI – mais provenant aussi de [redacted] de sources ouvertes, de sources classifiées (p. ex. SIGINT), d'analyses de maliciels, d'enquêtes en matière d'informatique judiciaire et de divulgations – concernant les menaces, de sorte à réagir aux cyberactivités malveillantes de façon automatisée, donc sans qu'une intervention humaine soit nécessaire[20]. De plus, les ministères, notamment SPC, peuvent demander au CST de boquer certains IC[21]. La défense dynamique exploite les techniques d'apprentissage machine – une sphère de l'intelligence artificielle – notamment la reconnaissance des modèles servant, entre autres, à la création informatisée de noms de domaines.

30. Comme il est décrit en de plus amples détails à l'annexe A, l'écosystème CAI du CST collecte un important volume de données, et celles-ci franchissent diverses étapes : la collecte, l'analyse, la conservation et l'élimination, la production de rapports ainsi que l'utilisation. La majeure partie des données collectées finit par être supprimée, conformément aux exigences du CST en matière de conservation. Lorsqu'il s'agit de conserver des données plutôt que de les supprimer, le CST jauge leur pertinence, leur utilité et leur caractère essentiel. Les données que le CST décide de conserver peuvent être utilisées pour alimenter les mesures de cyberdéfense et peuvent être communiquées à l'intérieur comme à l'extérieur du GC – souvent selon des méthodes qui suppriment les renseignements personnels se trouvant parmi les données en question.

31. Pour le déploiement de SR dans les divers réseaux du GC, le CST doit d'abord établir un partenariat avec le ministère ou l'organisme qui est propriétaire du système visé. Au moment de l'examen, le CST avait établi [redacted] partenariats avec des entités fédérales (« partenaires SR » ou propriétaires des systèmes faisant partie des réseaux bénéficiant d'une protection) : [redacted] SPC et le CST. Au nombre de ces [redacted] partenaires, certains ont étendu les services SR à d'autres ministères et organismes du GC dont ils géraient les réseaux. Par exemple, comme il administrait les réseaux d'environ 90 entités du GC, SPC a étendu les services SR du CST à ces entités, notamment, le [redacted][22]. En l'occurrence, le contenu de tout le trafic réseau entrant et sortant collecté auprès de ces entités est copié et transmis au CST. Il convient de noter que pendant la période d'examen, les [redacted] partenaires du CST avaient tous recours à certains autres capteurs ou services CAI en plus des solutions SR.

La figure 1 consiste en un schéma par lequel le CST présente ses [redacted] partenaires SR du CST, y compris lui-même[23].

[19] Les exemples fournis plus haut ont été respectivement désignés par les noms de code [redacted].

[20] CST, *Demande concernant les activités de cybersécurité du CST dans les infrastructures fédérales pour 2019-2020*, paragraphe 54.

[21] SPC demande « souvent » au CST de bloquer certains IC.

[22] Au mois d'août 2022, 78 ministères et organismes avaient eu recours au Service Internet d'entreprise (SIE) de SPC; tous avaient recours à la protection SR. De plus, l'OSSNR comprend que certains de ces ministères et organismes chapeautés par SPC ont offert, à leur tour, des services réseau à d'autres entités du GC.

[23] Pour obtenir les appellations complètes correspondant à ces sigles et abréviations, prière de consulter la page se trouvant à l'adresse suivante : https://www.canada.ca/fr/gouvernement/min.html.

32. Comme il a été dit précédemment, le CST acquiert, utilise et analyse l'information de cybersécurité provenant de l'infrastructure mondiale de l'information (IMI) sans compter, à des fins d'optimisation du rendement, l'information provenant de solutions tripartites (SSH, SR et SI)[24]. L'acquisition et l'utilisation de sources d'information autres que ces trois solutions sont abordées dans la section Analyse du présent rapport (section IV).

Fondements juridiques des activités de cybersécurité et d'assurance de l'information (CAI)

33. La Loi sur le CST accorde au CST le pouvoir de mener des activités CAI, et ce volet du mandat est décrit à l'article 17 de la Loi. Il importe d'indiquer que la Loi sur le CST impose des contraintes aux activités CAI. En outre, elles ne peuvent viser des Canadiens ou des personnes se trouvant au Canada et ne doivent aucunement contrevenir aux dispositions de la *Charte canadienne des droits et libertés*[25].

34. De par leur nature, les activités CIA s'avèrent souvent intrusives et mettent en jeu des intérêts personnels sur le plan de la vie privée. En l'occurrence, la Loi sur le CST stipule que le ministre peut autoriser des activités CAI qui, par ailleurs, seraient interdites en vertu du paragraphe 22(4) de la Loi. Cela comprend les activités qui contreviendraient aux lois fédérales ou qui feraient appel à l'acquisition, par le CST, d'information issue de l'IMI qui porte atteinte à une ARPVP de la part de Canadiens ou de personnes se trouvant au Canada. Pour délivrer une autorisation, le ministre doit conclure qu'il y a des motifs raisonnables de croire que toute activité qu'il est appelé à autoriser est raisonnable et proportionnelle[26] et qu'elle répond aux autres conditions énoncées au paragraphe 34(3) de la Loi sur le CST, lesquelles sont abordées plus avant dans le présent rapport[27].

35. Le ministre peut délivrer deux types d'autorisations pour les activités CAI : une autorisation visant les infrastructures fédérales [21(1)] et une autorisation visant les infrastructures non fédérales [21(2)]. Comme les SR sont déployées dans les réseaux du GC, les autorisations de CAI examinées aux fins du présent examen ont toutes été autorisées au titre du paragraphe 27(1) plutôt qu'au titre du paragraphe 27(2). En outre, une autorisation délivrée en vertu du paragraphe 27(1) habilite le CST « à accéder à une infrastructure de l'information d'une institution

---

[24] CST, *Demande concernant les activités de cybersécurité du CST dans les infrastructures fédérales pour 2022-2023*, paragraphe 6.
[25] Loi sur le CST, paragraphe 22(1).
[26] Loi sur le CST, paragraphe 34(1) : « Le ministre ne peut délivrer l'autorisation visée aux paragraphes 26(1), 27(1) ou (2), 29(1) ou 30(1) que s'il conclut qu'il y a des motifs raisonnables de croire que l'activité en cause est raisonnable et proportionnelle compte tenu de la nature de l'objectif à atteindre et des activités. »
[27] Les alinéas 34(3)(a), (b), (c) et (d) de la Loi sur le CST renvoient respectivement à : la conservation de l'information; le consentement; la nécessité de l'acquisition de l'information; et les informations se rapportant à un Canadien ou à une personne se trouvant au Canada (ICPC).

fédérale ou à acquérir de l'information qui provient ou passe par cette infrastructure, qui y est destinée ou y est stockée afin d'aider à protéger [...] cette infrastructure contre tout méfait, toute utilisation non autorisée ou toute perturbation de leur fonctionnement[28]. »

36. De plus, comme pour les autorisations délivrées aux fins du volet renseignement étranger du mandat du CST, les autorisations CAI ne sont valides qu'une fois qu'elles ont été approuvées par le commissaire au renseignement[29].

Cadre stratégique s'appliquant aux activités de cybersécurité et d'assurance de l'information (CAI)

37. Au CST, le cadre stratégique interne qui gouverne les activités ayant trait aux activités CAI est décrit dans l'Ensemble des politiques relatives à la mission, Cybersécurité (EPM Cybersécurité). Même s'il ne mentionne pas explicitement le programme SR, l'EPM Cybersécurité énonce néanmoins les exigences stratégiques globales s'appliquant à toutes les activités CAI, y compris celles qui sont menées au titre d'une autorisation, comme pour le programme SR.

38. Par exemple, l'EPM Cybersécurité établit les exigences opérationnelles et stratégiques qui s'appliquent à la gestion de l'information, en l'occurrence, aux données acquises dans le cadre du programme SR. De fait, l'EPM propose des conseils pour ce qui touche l'évaluation des niveaux de sensibilité de l'information, les droits d'accès à l'information, les exigences régissant le traitement de certains types d'information – notamment l'évaluation et la surveillance[30] – ainsi que les exigences s'appliquant à la conservation. L'EPM formule également des énoncés d'orientation relativement à la mobilisation et aux échanges d'information avec des entités externes. En l'occurrence, on y aborde la mobilisation précédant le déploiement d'un outil ou d'un service, mais aussi en situation de communication d'information acquise dans le cadre des activités de cybersécurité.
L'EPM Cybersécurité décrit aussi les aspects de la conformité des opérations dans le contexte de la cybersécurité.

IV. ANALYSE

Transparence quant à la nature de la collecte SR

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

Conclusion n° 2 : L'OSSNR conclut que le CST a traité toutes les informations acquises par les solutions réseau (SR) en tenant compte de l'information se rapportant à des Canadiens ou à des personnes se trouvant au Canada (ICPC) et qu'il a appliqué toutes les mesures permettant de protéger les renseignements personnels se trouvant dans cette information acquise par l'intermédiaire de SR.

Conclusion n° 3 : L'OSSNR conclut qu'en raison de sa nature, l'information acquise par l'intermédiaire de SR comportera toujours de l'information se rapportant à des Canadiens ou à des personnes se trouvant au Canada (ICPC) et qu'il contiendra invariablement de

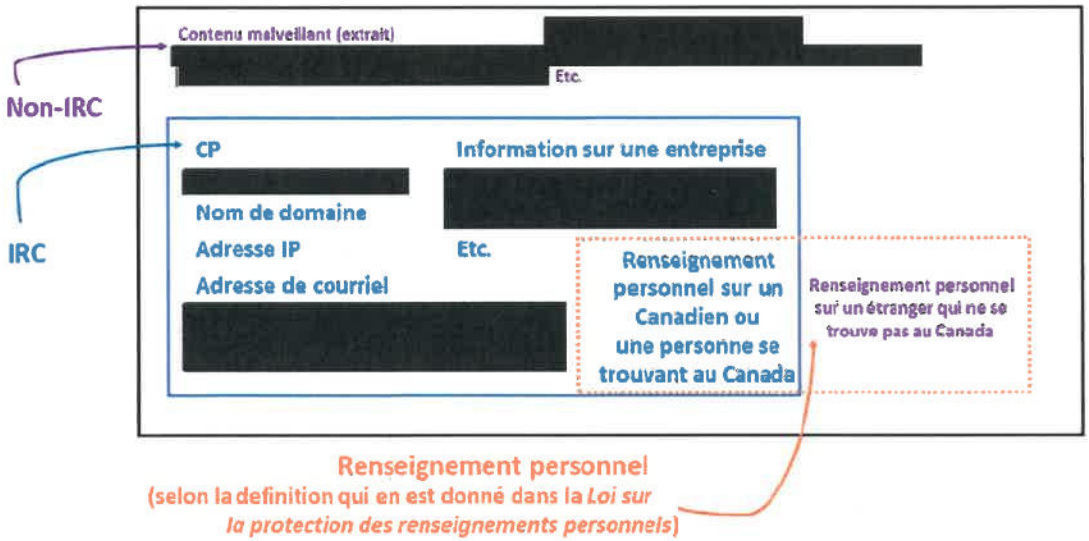
[28] Loi sur le CST, paragraphe 27(1).
[29] Loi sur le CST, article 28. Le commissaire au renseignement vérifie si les conclusions tirées par le ministre qui délivre l'autorisation s'avèrent raisonnables.
[30] Entre autres : les ICPC, l'information accessible au public, les renseignements protégés par le secret professionnel de l'avocat et les communications privées.

l'information à l'égard de laquelle un Canadien ou une personne se trouvant au Canada pourrait avoir une attente raisonnable en matière de protection de la vie privée (ARPVP). Cet aspect n'a pas été communiqué de façon transparente au ministre lors de la présentation des demandes d'autorisation correspondantes.

39. À quelques reprises, le texte de la Loi sur le CST traite de l'ICPC[31] sans toutefois la définir. Selon la politique interne du CST, l'ICPC se définit 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 [...] Les ICPC peuvent également contenir des informations ne permettant pas d'identifier un Canadien ou une personne se trouvant au Canada [...] »[32].

La figure 2 (voir ci-dessous) consiste en un schéma par lequel le CST donne des exemples d'information qui, dans un contexte opérationnel, pourrait, ou non, se rapporter à un Canadien ou à une personne se trouvant au Canada[33]. Il importe de noter que l'ICPC peut comprendre, entre autres, de l'information à l'égard de laquelle un Canadien ou une personne se trouvant au Canada pourrait avoir une ARPVP.



40. Il est permis au CST d'acquérir incidemment de l'ICPC pendant qu'il exerce des activités formellement autorisées de renseignement étranger [paragr. 26(1)], de cybersécurité [paragr. 27(1) ou 27(2)] ou en cas d'urgence (art. 40). Pour délivrer une autorisation, le ministre doit être convaincu que le CST utilisera, analysera ou conservera l'ICPC uniquement si celle-ci répond aux critères d'essentialité énoncés à l'article 34 de la Loi sur le CST, à la différence des principes s'appliquant au

---

[31] 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. Par exemple, la notion est décrite à l'article 34 comme suit : « information acquise au titre [d'une] autorisation qui est identifiée comme se rapportant à un Canadien ou à une personne se trouvant au Canada [...] ».

[32] Rappelons que dans son rapport intitulé « Examen des pratiques d'échange d'informations entre divers volets du mandat du CST » (examen nº 20-07), l'OSSNR s'est également penché sur l'ICPC, notamment au paragraphe 14.

[33] Schéma tiré de la politique interne du CST (EPM Cybersécurité, 2022). Le sigle « IP » correspond au terme « information personnelle ».

volet renseignement étranger et au volet cybersécurité du mandat du CST. Dans le cas de ce dernier, le fait d'établir le caractère « essentiel » signifie d'évaluer si l'information est essentielle pour reconnaître, isoler, prévenir ou atténuer une menace envers (i) l'information électronique ou les infrastructures de l'information des institutions fédérales, ou encore (ii) envers l'information électronique ou les infrastructures de l'information désignées comme étant importantes en vertu des dispositions énoncées au paragraphe 21(1) de la Loi sur le CST (système d'importance)[34]. Pour ce qui a trait au renseignement étranger, le caractère « essentiel » dépend d'une évaluation visant à établir si l'information est essentielle aux affaires internationales, à la défense ou à la sécurité[35].

SR, ICPC et information pouvant porter atteinte à l'ARPVP d'un Canadien ou d'une personne se trouvant au Canada

41. De 2019 à 2021, le CST a généré 1103 produits de cybersécurité communicables (PCC) à partir d'information SR contenant des ICPC[36]. Le CST a indiqué à l'OSSNR qu'il ne communiquait pas les rapports à d'autres entités que le propriétaire du système mentionné dans le rapport, à moins que celui-ci ait donné son consentement[37]. Ainsi, chaque rapport n'identifie qu'un seul ministère après qu'on en ait retiré les éléments pouvant se rapporter à d'autres ministères.

42. Les demandes présentées par le CST en vue d'activités de cybersécurité fédérale ainsi que les autorisations ministérielles correspondantes indiquent à de multiples reprises que les SSH, les SR et les SI ne visent ni les Canadiens ni les personnes se trouvant au Canada, et que les ICPC qui pourraient être acquises pendant la mise en œuvre de ces solutions – y compris l'information pouvant porter atteinte à une ARPVP de la part d'un Canadien ou d'une personne se trouvant au Canada – ne le sont qu'incidemment[38]. S'appuyant sur la Loi sur le CST, plus précisément sur l'énoncé de l'alinéa 23(3)a), le CST est d'avis que [traduction] « depuis l'entrée en vigueur de la Loi sur le CST, le fait de mener des activités de cybersécurité dans un réseau dans le but de contribuer à sa défense n'est pas considéré comme "visant des Canadiens ou des personnes se trouvant au Canada"[39]. Cela s'explique dans la mesure où ni l'intention ni la cible de l'acquisition SR n'ont trait aux ICPC, mais ont plutôt pour objectif de voir si certaines des informations acquises révèlent l'occurrence d'un cyberincident ou la présence d'une cybermenace[40]. »

---

[34] Aux fins de la cybersécurité, le caractère essentiel des besoins est décrit 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 des dommages : (i) aux informations électroniques ou aux infrastructures de l'information des institutions fédérales, dans le cas de l'autorisation visée au paragraphe 27(1), (ii) 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). »

[35] Aux fins du renseignement étranger, le caractère essentiel des besoins est décrit 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. »

[36] Ces PCC comprenaient [redacted]

[37] Toutefois, lors d'une démonstration subséquente, le CST a indiqué qu'il arrivait que certaines informations soient communiquées à une entité autre que le propriétaire de système, par exemple, [redacted]

[38] Le CST estime que toute acquisition d'information portant atteinte à l'ARPVP d'un Canadien ou d'une personne se trouvant au Canada constitue une « acquisition incidente » et considère que ce type d'acquisition ne signifie pas nécessairement que l'information concernée sera évaluée, puis traitée ou utilisée.

[39] Soulignement ajouté par l'OSSNR. L'OSSNR note que divers examens du BCCST portant sur les activités de cyberdéfense abondaient dans le même sens.

[40] L'OSSNR note que cette position [redacted]

43. Dans la demande 2019-2020 qu'elle a présentée au ministre concernant des activités de cybersécurité dans des infrastructures fédérales, la cheffe du CST indique que [traduction] « lors de la conduite d'activités de cybersécurité, des courriels pouvant contenir de l'information se rapportant à des Canadiens ou à des personnes se trouvant au Canada seront incidemment acquis et copiés[41]. » L'autorisation correspondante indique, au sous-alinéa 2f)i) que pendant les activités de cybersécurité, l'acquisition d'ICPC par le CST est « inévitable ».

44. Cependant, les libellés contenus dans les trois demandes annuelles présentées subséquemment en rapport avec les activités de cybersécurité – entre 2020 et le moment de rédiger la présente, en mai 2023 – étaient considérablement plus ambigus quant à l'ampleur des ICPC pouvant être acquises pendant lesdites activités. Par exemple, les demandes indiquent en plusieurs occasions que le CST [traduction] « pourrait acquérir incidemment [des ICPC] » ou que, dans le contexte de l'autorisation, le CST [traduction] « pourrait entreprendre des activités pouvant donner lieu à l'acquisition incidente [d'ICPC][42] ».

45. Toute l'information collectée par voie de SR est [traduction] « présumée contenir des ICPC ». Cette supposition se fonde sur la position du CST qui s'énonce comme suit: [traduction] « comme elles sont collectées dans l'infrastructure canadienne, les données SR sont, par nature, des informations se rapportant à des Canadiens. » Depuis 2020, les demandes d'autorisations soumises au ministre au titre du paragraphe 27(1) de la Loi sur le CST n'expriment pas clairement l'ampleur de cette collecte.

46. Le CST acquiert des *contenus* de communications par l'intermédiaire de SR, ce qui comprend le contenu des courriels envoyés par des adresses électroniques non-GC à des adresses électroniques du GC, et vice versa. Compte tenu de la nature de cette acquisition, certaines des informations acquises par le CST contiendront invariablement de l'information qui porte atteinte à l'ARPVP d'un Canadien ou d'une personne se trouvant au Canada. Or, les autorisations du CST et les demandes correspondantes n'expriment pas clairement cette réalité. Les autorisations comprennent plutôt des libellés indiquant que l'acquisition d'information [traduction] « pose le risque que le CST puisse porter atteinte à une ARPVP »[43] et que la demande correspondante informe le ministre que [traduction] « le CST court le risque d'acquérir de l'information qui porte atteinte à une ARPVP lorsqu'il exécute les activités CAI qui sont décrites »[44]. Les demandes correspondantes contiennent des énoncés conditionnels semblables. Dans les faits, il est certain que les SR acquerront de l'information à l'égard de laquelle des Canadiens ou des personnes se trouvant au Canada auront une ARPVP.

47. L'une des importantes modifications apportées à la Loi sur le CST est l'enchâssement des notions d'ICPC et d'ARPVP. Il s'agit là d'un complément aux « dispositions relatives aux informations personnelles » – notamment la notion de « communication privée » (CO) – évoquées dans le texte de loi qui, auparavant, encadrait les activités du CST, à savoir la partie V.1 de la *Loi sur la défense*

[redacted]

[41] *Demande concernant les activités de cybersécurité du CST dans les infrastructures fédérales pour 2019-2020*, paragraphe 109.
[42] Soulignement ajouté par l'OSSNR. Voir, à titre d'exemple, *Application for CSE cybersecurity activities on federal infrastructures: 2020-2021*, paragraphes 24, 34, 92, 94; *2021-2022*, paragraphes 38, 60, 90, 105; *2022-2023*, paragraphes 43, 79, 115, 132.
[43] Soulignement ajouté par l'OSSNR. Voir, à titre d'exemple, 2020-2021 *Application for CSE cybersecurity activities on federal infrastructures: 2020-2021*, paragraphe 1(a).
[44] Soulignement ajouté par l'OSSNR. Voir, à titre d'exemple, *Application for CSE cybersecurity activities on federal infrastructures: 2020-2021*, paragraphe 72.

nationale[45]. Ce changement se fonde sur le développement et la sophistication accrue des notions juridiques relevant du domaine de la vie privée.

48. Selon l'article 24 de la Loi sur le CST, le Centre doit veiller à ce que des mesures soient en place pour protéger la vie privée des Canadiens et des personnes se trouvant au Canada lorsqu'il procède à l'utilisation, à l'analyse et à la communication d'information; certaines de ces mesures sont décrites en annexe A. Le CST a indiqué qu'il était en train [traduction] « de réaliser une série d'évaluations des facteurs relatifs à la vie privée, ce qui permettra d'examiner les activités de création, de collecte et de traitement des renseignements personnels dans le cadre du programme de cybersécurité ». Or, il convient de mentionner que ces évaluations n'avaient pas encore été complétées au moment de procéder au présent examen.

49. Le fait que, de par sa nature, la collecte SR depuis les infrastructures fédérales canadiennes inclura invariablement des ICPC – de même que des informations à l'égard desquelles des Canadiens ou des personnes se trouvant au Canada pourraient avoir une ARPVP – n'est ni une nouveauté ni une surprise. Il serait impensable d'exercer des activités de cybersécurité efficaces dans l'infrastructure électronique des institutions fédérales et dans les infrastructures de l'information si l'on devait s'empêcher de collecter l'information de cette manière. Tout compte fait, étant donné les risques qui pourraient peser sur le droit à la vie privée des Canadiens et des personnes se trouvant au Canada, le ministre devrait tout de même recevoir une information claire et exacte à ce sujet avant de délivrer une autorisation.

Recommandation n°. 1 : L'OSSNR recommande que dans ses demandes d'autorisation, le CST expose clairement au ministre les éléments suivants :

- que les solutions réseau acquièrent de l'information se rapportant à des Canadiens ou des personnes se trouvant au Canada (ICPC), notamment des informations qui contreviennent à l'attente raisonnable de Canadiens ou de personnes se trouvant au Canada en matière de protection de la vie privée (ARPVP);

- que le CST utilise, analyse et conserve ces données dans le cadre de ses activités en matière de cybersécurité et d'assurance de l'information.

Consentement à l'égard des solutions de cybersécurité du CST

50. Suivant les dispositions de l'alinéa 34(3)b) de la Loi sur le CST, avant de délivrer une autorisation de cybersécurité visant les infrastructures fédérales [paragr. 27(1) de la Loi sur le CST], le ministre doit respecter certaines conditions, l'une étant d'avoir des motifs raisonnables de croire que le consentement de toutes les personnes dont les informations pourraient être acquises ne pourrait vraisemblablement pas être obtenu. Dans le cas d'une autorisation de cybersécurité visant les infrastructures non fédérales [paragr. 27(2) de la Loi sur le CST], le CST doit avoir obtenu par écrit, de la part du propriétaire ou de l'opérateur de l'infrastructure concernée, la demande d'exercer les activités à autoriser.

51. Au mois de mai 2023, toutes les autorisations délivrées depuis 2019 pour les activités de cybersécurité dans les infrastructures fédérales comprenaient l'énoncé suivant :

---

[45] À titre d'exemple, voir le paragraphe 273.65(1) de la *Loi sur la défense nationale*. En vertu de la *Loi sur la défense nationale*, le CST est tenu d'obtenir des autorisations ministérielles lorsqu'il envisage d'intercepter des CP. Copie archivée de la LMD consultable en ligne à l'adresse suivante : https://www.laws-lois.justice.gc.ca/fra/lois/n-5/20190712/p1tt3xt3.html.

> [Traduction] « Conformément aux pratiques normalisées du gouvernement, les institutions fédérales doivent aviser les utilisateurs autorisés de ces infrastructures d'information que les activités réseau qu'ils exercent au moyen de leurs dispositifs sont surveillées à des fins de cybersécurité et d'assurance de l'information[46] ».

Cet énoncé concorde avec les dispositions stipulées dans les documents du GC, notamment la Politique sur les services et le numérique du Conseil du Trésor. Selon cette Politique sur les services et le numérique, les administrateurs généraux sont responsables, entre autres, d'informer les utilisateurs autorisés de réseaux et de dispositifs électroniques des « pratiques de surveillance mises en œuvre dans leur propre ministère et par SPC[47] ».

Coopération transparente avec les propriétaires de systèmes

Conclusion n° 4 : L'OSSNR conclut qu'en raison de certaines ambiguïtés dans sa relation avec SPC, le CST n'a pas obtenu, aux fins des activités de cybersécurité et d'assurance de l'information, le consentement des propriétaires de systèmes comme il avait été décrit au ministre.

Conclusion n° 5 : L'OSSNR conclut que SPC n'était pas parfaitement au courant de ses responsabilités en tant que propriétaire de systèmes, contrairement à ce qui est énoncé dans les demandes que le CST a soumises au ministre.

Conclusion n° 6 : L'OSSNR conclut qu'en dépit d'un protocole d'entente établi entre le CST et SPC, il y a des éléments d'incompréhension entre les organisations relativement à l'exercice des responsabilités convenues sur le plan des activités SR dans les réseaux exploités par SPC.

52. Les demandes 2019-2020 et 2020-2021 que la cheffe a présentées au ministre concernant les activités de cybersécurité dans les infrastructures fédérales indiquent [traduction] « que le CST déploie des capacités SSH, SR et SI uniquement sous réserve du consentement éclairé du propriétaire du système faisant partie de l'infrastructure de l'information de l'institution fédérale[48] ». Les deux demandes présentées subséquemment en lien avec les activités de cybersécurité dans des infrastructures fédérales – 2021-2022 et 2022-2023 – ne comportaient pas le qualificatif « éclairé » dans ce contexte.

53. Certes, le CST obtient le consentement du partenaire SR relativement au déploiement des SR, mais ce consentement ne concerne généralement pas les ministères ou les organisations qui accèdent au réseau en question. Par exemple, le Service d'interconnexion Internet (SII) reliait environ 90 ministères et organismes du GC pendant la période de l'examen, alors que le partenariat du CST avait été principalement conclu avec SPC (propriétaire des systèmes pour le réseau SII) et non avec les diverses entités branchées au réseau SII de SPC. En l'occurrence, SPC fait office d'intermédiaire auprès duquel les divers ministères et organismes donnent leur consentement en vue de leur accès audit réseau.

---

[46] *Autorisation des activités de cybersécurité dans les infrastructures fédérales : 2019-2020 et 2020-2021*, paragraphe 2(d), *2021-2022*, paragraphe 37, *2022-2023*, paragraphe 34. Aussi dans les demandes correspondantes : par exemple, *2020-2021*, paragraphe 86 et *2021-2022*, paragraphe 15.

[47] SCT, Politique sur les services et le numérique, section 4.4.2.6, consultable en ligne à l'adresse suivante : https://www.tbs-sct.canada.ca/pol/doc-fra.aspx?id=32603. De plus, conformément à la section 4.4.3.1, l'administrateur général de SPC est responsable de gérer les outils à l'appui de la surveillance des réseaux et des dispositifs électroniques ministériels.

[48] Soulignement ajouté par l'OSSNR. *Demande concernant les activités de cybersécurité du CST dans les infrastructures fédérales pour 2019-2020*, paragraphe 7; *2020-2021*, paragraphe 14.

54. C'est une collaboration de longue date qui existe entre le CST et SPC en matière de SR. Selon le CST, SPC est [traduction] « activement engagé auprès du CST sur plusieurs plans pour ce qui concerne le programme SR », et SPC [traduction] « est parfaitement au fait du programme SR », et ce, depuis le déploiement initial et au fil des diverses modalités d'intervention et des diverses interactions opérationnelles. Vers la fin de l'examen, SPC a indiqué aux représentants de l'OSSNR que [traduction] « SPC a une compréhension approfondie du rôle que le CST tient en matière de protection et de surveillance des réseaux du gouvernement du Canada ». SPC indique ensuite qu'il est convaincu que [traduction] « le CST fournit à SPC l'information dont il a besoin pour réagir efficacement aux incidents et aux événements », tout en faisant valoir que sa relation avec le CST est solide et qu'elle a déjà donné lieu à « bon nombre d'interventions rapides et adéquates ». Néanmoins, pendant les séances d'informations et dans les réponses écrites présentées au cours de la période d'examen, SPC a indiqué qu'il percevait les SR et les fonctions exercées par les capteurs du CST comme des espèces de « boîtes noires[49] ». SPC a également indiqué en cours d'examen qu'on ne lui donnait aucune explication quant aux processus, aux procédures, aux risques ou aux aspects techniques liés aux outils ou aux services de cyberdéfense du CST. Convient-il de noter que SPC s'occupe de la maintenance de son propre ensemble de coupe-feu en plus de la protection offerte par le programme CAI du CST. Bien que le concept de protection multicouche soit une pratique courante en cybersécurité, le manque de visibilité de SPC par rapport aux défenses mises en place par le CST risque d'entraîner des inefficacités sur le plan opérationnel. Par exemple, SPC indique qu'il lui arrive de ne pas être en mesure d'identifier la source d'un blocage ou d'un comportement réseau inattendu.

55. En outre, SPC a confirmé qu'il [traduction] « ne dispose d'aucune mesure particulière permettant d'aviser les ministères relativement au programme SR », hormis les trousses d'orientation et d'intégration qui [traduction] « peuvent contenir des énoncés types concernant le fait que les systèmes sont surveillés pour des raisons de sécurité et qu'il ne faut pas tenir pour acquis que la vie privée de ceux et celles qui travaillent au sein d'un réseau du gouvernement est protégée ». Les pratiques de SPC, en l'occurrence, ne correspondent pas à ce que le CST a décrit au ministre dans ses demandes d'autorisation. Elles ne correspondent pas non plus à la responsabilité qui revient à SPC depuis le protocole d'entente (PE) de mars 2014 conclu entre le CST et SPC, selon lequel il est entendu que SPC informera ses clients concernant le fait que [traduction] « le CST pourrait acquérir leurs données, y compris des renseignements personnels ou des communications privées pendant la conduite de ses activités de cyberdéfense pour le compte de SPC[50] ».

56. C'est par l'intermédiaire de la demande présentée au ministre par la cheffe que le CST a donné l'assurance qu'il obtenait le consentement des propriétaires de systèmes relativement aux données saisies par les capteurs de cybersécurité, y compris les SR. De fait, SPC connaissait mal les modalités suivant lesquelles le CST menait ses activités de cybersécurité. Par conséquent, SPC n'a pas – parce qu'il n'en avait pas les moyens – avisé ses clients que le CST pouvait acquérir leurs informations pendant le déroulement des activités de cybersécurité qu'il était autorisé de mener, sans compter la collecte et la conservation de renseignements personnels et des contenus de communications[51]. Durant le suivi de l'exactitude des faits réalisé pour le présent examen, le CST a indiqué que ce rapport [traduction] « représente la première fois où le CST a été informé du fait que SPC n'était pas au courant de ses propres responsabilités à titre de propriétaire de systèmes[52] ».

---

[49] Note d'information de SPC en réaction à la DI-1 de l'OSSNR, 6 septembre 2022; réponse écrite de SPC à la DI-2, questions 3 et 4, 6 mars 2023.

[50] Document du CST, « Protocole d'entente entre le Centre de la sécurité des télécommunications (CST) et Services partagés Canada (SPC) », p. 2, 27 mars 2014.

[51] Durant le suivi de l'exactitude des faits réalisé pour le présent examen, SPC a contesté cette caractérisation, en contradiction avec les déclarations verbales et écrites qu'il a pourtant faites tout au long de l'examen, comme en témoigne l'énoncé du paragraphe 52.

[52] Le CST a aussi dressé la liste des mécanismes qui, à son avis, avaient veillé à ce que SPC demeure au courant des capacités SR et des mesures de défense réseau du CST. Or, cette mise au courant ne s'est aucunement manifestée lors des interactions que l'OSSNR a eues avec les membres de diverses équipes de SPC dans le cadre du présent examen.

57. Le PE de 2014 conclu entre le CST et SPC établit les modalités et les conditions au titre desquelles les activités de cyberdéfense du CST ont été menées dans les systèmes et les réseaux dont SPC est responsable. Le PE stipule que SPC devra [traduction] « s'assurer que ses clients ont été avisés que le CST pourrait acquérir des données les concernant, notamment des renseignements personnels ou des communications privées, pendant le déroulement des activités de cyberdéfense qu'il exerce pour le compte de SPC ». En revanche, le PE indique qu'avant tout déploiement de moyens dans les réseaux et systèmes de SPC, le CST doit fournir à celui-ci des détails concernant les processus, les procédures et l'aspect technique se rapportant aux outils et aux services, mais aussi aux risques encourus.

58. Toutefois, SPC a initialement indiqué, lors de l'examen, que le PE de 2014 n'était plus en vigueur et qu'il avait été remplacé par un PE conclu en 2018, en prévision de la création du Centre pour la cybersécurité et du transfert des ressources. Or, le PR de 2018 porte sur des considérations d'ordre organisationnel et financier, et ne contient aucune information substantielle concernant les capteurs de cyberdéfense du CST ou la façon dont ils fonctionnent. En raison de son manque d'information concernant les activités de cyberdéfense du CST, le PE de 2014 fait contraste avec les PE reçus par l'OSSNR de la part [redacted] fournissent davantage d'information substantielle concernant les activités de cyberdéfense du CST, y compris les pouvoirs et les types d'activités qui peuvent être menées[53].

59. Hormis ceux conclus avec SPC, les PE signés par le CST et ses partenaires de cyberdéfense remontent à bien avant l'adoption de la Loi sur le CST. Par exemple, les plus récents PE sur les services SR que l'OSSNR a reçus aux fins du présent examen, en l'occurrence entre le [redacted] Conformément à l'article 81 de la Loi sur le CST, les PE que le CST a conclus avant cette Loi ont continué de s'appliquer après son entrée en vigueur, et le CST a confirmé que d'après lui, ce fut également le cas pour le PE conclu avec SPC.

60. Durant le suivi de l'exactitude des faits réalisé pendant les derniers stades de l'examen, SPC a avisé l'OSSNR que – contrairement à ce qu'il avait déclaré initialement – le PE conclu avec le CST en 2014 était toujours en vigueur. En l'occurrence, SPC a ajouté qu'il [traduction] « continuerait à travailler avec le CST pour veiller à ce que les attentes énoncées dans le PE de 2014 correspondent à la teneur des politiques du gouvernement du Canada ».

Recommandation n° 2 : L'OSSNR recommande que le CST renouvelle le PE qu'il a conclu avec SPC en 2014, de sorte à veiller à ce que le CST et SPC remplissent adéquatement leurs engagements respectifs, y compris l'engagement voulant que le CST tienne le ministre au courant de la responsabilité de SPC qui consiste à aviser les propriétaires de systèmes au sujet du programme SR.

---

[53] Voir, à titre d'exemple, [redacted] (CERRID n° 71886V3) et le [redacted] (CERRID n° 162578).

Recommandation n° 3 : L'OSSNR recommande que le CST mette à jour les protocoles d'entente (PE) qu'il a conclus avec tous ses partenaires de cybersécurité. Ainsi, il pourra veiller à ce que ces partenaires expriment leur consentement à l'égard des activités de cybersécurité du CST, et à ce que les ententes soient intégralement conformes aux pouvoirs et aux modalités de gouvernance actuellement en vigueur. Au reste, le CST devrait adopter une pratique de mise à jour régulière de ces PE, de sorte à tenir compte de l'évolution des attributions.

Transparence à l'égard des utilisateurs du système

Conclusion n° 7 : L'OSSNR conclut que le CST n'a pas exposé au ministre les motifs pour lesquels le consentement à l'égard des activités de cybersécurité du CST n'a raisonnablement pas été obtenu de la part des utilisateurs des systèmes du gouvernement du Canada.

61. De manière générale, on relève deux groupes qui utilisent les systèmes du GC : les utilisateurs non-GC (p. ex. le public ou les entités qui interagissent avec le gouvernement fédéral sans en faire partie) et les utilisateurs du GC (p. ex. les employés des institutions du GC). Pour ce qui touche les utilisateurs du premier groupe, le CST a pertinemment expliqué au ministre, conformément à l'alinéa 34(3)b) de la Loi sur le CST, pourquoi leur consentement ne pouvait pas être raisonnablement obtenu. Cependant, aucune explication n'a été fournie au ministre quant aux modalités visant à obtenir le consentement des utilisateurs des systèmes du GC (p. ex. employés du GC) et aux motifs pour lesquels ce consentement n'a pas été obtenu. L'alinéa 34(3)b) est pourtant clair lorsqu'il indique que le ministre doit avoir des motifs raisonnables de croire que le consentement de toutes les personnes dont l'information peut être acquise n'a pas pu être raisonnablement obtenu.

62. Il n'existe aucune exigence législative qui oblige le CST à aviser les utilisateurs des systèmes du GC qu'il acquiert de l'information de ces systèmes au titre d'une autorisation de cybersécurité. Or, le CST pourrait bien expliquer au ministre qu'il ne peut pas raisonnablement obtenir le consentement de la part de ces utilisateurs. Au lieu de fournir ce type d'explication, le CST répond au ministre que c'est aux institutions fédérales qu'il revient d'aviser leurs propres utilisateurs des infrastructures de l'information du GC en leur disant que leurs dispositifs ou leurs activités réseau sont surveillés à des fins de CAI.

63. Au lieu d'obtenir le consentement de toutes les personnes dont l'information pourrait être acquise, il serait important que des avis pertinents soient transmis – particulièrement aux utilisateurs principaux des systèmes du GC comme les employés du GC – pour leur indiquer que le CST pourrait acquérir et utiliser de l'information provenant de ces systèmes à des fins de cybersécurité. Le CST a indiqué aux représentants de l'OSSNR que le consentement *est bel et bien* obtenu de la part des utilisateurs de systèmes du GC par l'intermédiaire d'un avis destiné aux utilisateurs pour les informer que leurs dispositifs et leurs activités réseau étaient surveillés à des fins de cybersécurité et d'assurance de l'information. Le CST a également déclaré que l'utilisateur avait donné son consentement dès lors qu'il avait réagi à l'avis en question en cliquant sur le bouton d'acquiescement. L'OSSNR ne s'est pas penché sur le contenu de cet avis et n'a pas vérifié si cet avis s'affichait bel et bien à tous les utilisateurs des systèmes du GC. SPC, pour sa part, s'est inscrit en faux contre la notion de consentement dans le présent contexte, faisant remarquer que la politique du Conseil du Trésor exigeait que ces avertissements [traduction] « soient axés sur l'avis plutôt que sur le consentement ».

Recommandation n° 4 : L'OSSNR recommande que le CST explique au ministre les modalités selon lesquelles il obtient le consentement des utilisateurs des systèmes du gouvernement du Canada relativement aux activités qu'il exerce en matière de cybersécurité ou, le cas échéant, les raisons pour lesquelles ce consentement n'a pas pu être raisonnablement obtenu.

Information de sources externes à l'égard de laquelle les Canadiens ou les personnes se trouvant au Canada ont une attente raisonnable en matière de protection de la privée (ARPVP)

64. L'article 17 de la Loi sur le CST permet au Centre d'acquérir, d'utiliser et d'analyser de l'information provenant de l'infrastructure mondiale de l'information ou d'autres sources afin de fournir des avis, des conseils et des services visant à protéger l'information électronique et les infrastructures de l'information des institutions fédérales, mais aussi l'information électronique et les infrastructures de l'information désignées comme étant d'importance pour le gouvernement du Canada (systèmes désignés comme étant importants, ou SDI). Par exemple, le CST peut acquérir, utiliser et analyser de l'information accessible au public (IAP), laquelle est définie dans la Loi comme étant de « [l']information publiée ou diffusée à l'intention du grand public, accessible au public dans l'infrastructure mondiale de l'information ou ailleurs ou disponible au public sur demande, par abonnement ou achat[54]. » Il importe de rappeler que l'IAP ne comprend pas l'information à l'égard de laquelle un Canadien ou une personne se trouvant au Canada a une attente raisonnable en matière de protection de la vie privée.

65. D'après l'alinéa 23(1)a) de la Loi sur le CST, le Centre n'est pas tenu d'obtenir une autorisation avant d'acquérir et d'utiliser l'IAP. Lorsque l'IAP requise contient de l'ICPC, l'alinéa 24a) de la Loi sur le CST exige que le Centre mette en place des mesures visant à protéger la vie privée, lorsqu'il est question d'utiliser, d'analyser, de conserver ou de communiquer l'information acquise dans le cadre des activités menées au titre du volet renseignement étranger ou du volet cybersécurité de son mandat[55]. Certaines de ces mesures sont décrites en annexe A.

66. Une limite s'applique aux activités CAI en vertu du paragraphe 22(4), lequel interdit au CST d'acquérir de l'information à partir de l'infrastructure mondiale de l'information d'une façon qui contreviendrait aux lois fédérales ou qui porterait atteinte à une attente raisonnable en matière de protection de la vie privée d'un Canadien ou d'une personne se trouvant au Canada. Pour ce qui touche les activités CAI, le CST peut acquérir l'information de cette manière uniquement si l'acquisition est exercée au titre d'une autorisation ministérielle délivrée conformément aux dispositions énoncées aux paragraphes 27(1) ou 27(2) de la Loi sur le CST. Ainsi, les activités de cybersécurité du CST qui risquent de 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 peuvent être autorisées uniquement dans les infrastructures de l'information fédérales et dans les systèmes désignés comme étant d'importance pour le gouvernement du Canada.

[54] Loi sur le CST, article 2.
[55] *Autorisation ministérielle visant les activités de cybersécurité du CST dans les infrastructures fédérales pour 2019-2020*, p. 2.

Risques liés à l'acquisition d'information pouvant contenir des renseignements susceptibles de donner lieu à une ARPVP et provenant de sources d'information de cybersécurité non visées par une autorisation

Conclusion nº 8 : L'OSSNR conclut que l'application restrictive que le CST fait des dispositions visées au paragraphe 22(4) de la Loi sur le CST pose des risques sur le plan juridique et sur le plan de la reddition de comptes et, dans au moins un cas, a fait en sorte que le CST a acquis de l'information pouvant porter atteinte à l'attente raisonnable en matière de protection de la vie privée d'un Canadien ou d'une personne se trouvant au Canada. Cette information provenait d'une source qui n'était pas visée par le libellé des autorisations ministérielles.

Conclusion nº 9 : L'OSSNR conclut qu'une divergence entre les paragraphes 27(1) et 22(4) de la Loi sur le CST empêche le CST d'acquérir certaines informations provenant de sources externes, notamment les bases de données commerciales, dont l'information pourrait porter atteinte à l'attente raisonnable en matière de protection de la vie privée d'un Canadien ou d'une personne au Canada. Or, l'acquisition d'une partie de cette information renforcerait la capacité du CST à remplir son mandat en matière de cybersécurité et d'assurance de l'information.

67. Hormis les capteurs des solutions tripartites, l'information de cybersécurité du CST s'accompagne d'information provenant du SIGINT, de communications[56], d'ententes et d'autres sources accessibles au public comme les sources commerciales et les sources ouvertes, ce qui comprend également les bases de données colligées par les courtiers en données. Le CST a remis à l'OSSNR une liste de [redacted] sources externes (autres que les capteurs du CST ou les sources SIGINT) qui ont produit de l'information utilisée par le CST aux fins des activités visées aux autorisations de cybersécurité fédérale et menées pendant le déroulement du présent examen[57]. [redacted] de ce type d'information est monnaie courante dans la sphère de la cybersécurité, dans la mesure où cela permet de rassembler de l'information provenant [redacted]

68. Ces [redacted] sources ont produit de l'information à partir de portions de l'IMI autres que celles auxquelles le CST a accès au titre des autorisations visées aux paragraphes 27(1) et 27 (2)[58]. À ce sujet, prière de consulter la figure 3, plus loin.

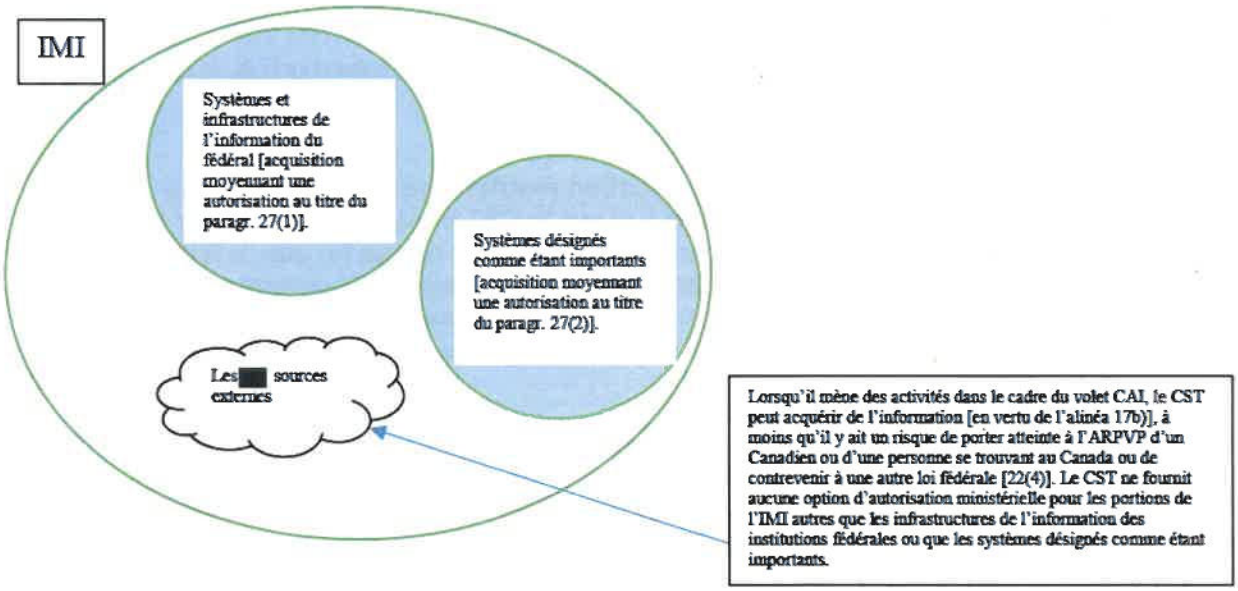
---

[56] Les communications peuvent comprendre celles provenant de ministères clients tout autant que les communications volontaires issues d'autres sources comme les EIUI internationales, les communications publiques concernant les maliciels sur le site mlwr.cyber.gc.ca, l'information échangée entre les partenaires de la Collectivité des cinq, etc.

[57] Cette information peut être communiquée à d'autres volets du mandat du CST. (Dans le cadre de l'examen de l'OSSNR nº 2020-07, DI-11 : [traduction] « [redacted] Généralement, les contrats n'imposent aucune restriction quant à leur utilisation par les divers volets du mandat, [redacted] »)

[58] Particulièrement, le paragraphe 27(1) habilite le CST « à accéder à une infrastructure de l'information d'une institution fédérale », alors que le paragraphe 27(2) habilite le CST « à accéder à une infrastructure de l'information désignée comme étant d'importance pour le gouvernement fédéral en vertu du paragraphe 21(1) [à titre de système désigné comme étant important pour le GC] ».

Figure 3 : L'IMI et les paragraphes 27(1) et 27(2) de la Loi sur le CST



69. Depuis 2020-2021, les demandes d'autorisations de cybersécurité fédérales soumises par la cheffe indiquent que le CST associe l'information sur les cybermenaces qui provient des institutions fédérales avec certaines des sources décrites précédemment, y compris l'information accessible au public[59]. Peu après, au début de 2021, le CST a entamé des discussions internes entre les groupes respectivement responsables de la conformité, des opérations et des questions juridiques. Ces discussions ont été l'occasion d'aborder la question de l'information de sources ouvertes posant un risque d'atteinte à l'ARPVP d'un Canadien ou d'une personne se trouvant au Canada, et ce, dans le contexte des activités d'acquisition du renseignement étranger (art. 16).

70. Selon le CST, la Loi sur le CST [traduction] « ne reconnaît aucune distinction entre un niveau faible ou un niveau élevé d'attente en matière de protection de la vie privée ». Autrement dit, peu importe le niveau d'une ARPVP ou la probabilité d'une atteinte à une ARPVP, et peu importe le volet du mandat dans le cadre duquel une atteinte à l'ARPVP pourrait survenir, le CST est toujours tenu d'obtenir une autorisation au titre des paragraphes 22(3) et 22(4) de la Loi sur le CST dès lors qu'il y a un risque, aussi minime soit-il, que l'information acquise contienne des éléments suscitant une ARPVP.

71. Dans la demande d'autorisation de cybersécurité aux fins d'activités dans des infrastructures fédérales, qu'il a soumise au titre du paragraphe 27(1), le CST a indiqué – pour la première fois – qu'il cherchait à acquérir des informations de cybersécurité de la part de fournisseurs tiers (sources externes), ce qui [traduction] « pourrait comporter un faible risque d'atteinte à l'attente raisonnable en matière de protection de la vie privée d'un Canadien ou d'une personne se trouvant au Canada[60] ». La demande indique que cette question avait été récemment reconnue par le CST.

---

[59] L'OSSNR note que la demande 2019-2020 ne mentionne ce fait nulle part. Les demandes visant les activités de cybersécurité du CST dans les infrastructures fédérales : 2020-2021, paragraphe 13; 2021-2022, paragraphe 19. La demande 2022-2023 fait clairement allusion à ce fait, notamment au paragraphe 6 ainsi qu'aux paragraphes 63 à 74, lesquels n'ont pas été approuvés par le commissaire au renseignement.

[60] *Demande concernant les activités de cybersécurité du CST dans les infrastructures fédérales pour 2022-2023*, section VII, paragraphe 69.

72. La demande que le CST a présentée au ministre indiquait que [traduction] « lorsque le CST acquiert ce type d'information [redacted] on peut inférer que cette activité n'exige aucune autorisation pour avoir lieu, puisque le CST n'acquiert pas directement l'information à partir de l'IMI[61]. » Le CST en est arrivé à ce point de vue en se fondant sur le raisonnement fait par la [redacted] selon lequel des « arguments probants » permettent de conclure que les recherches [redacted] [traduction] « ne constituerait pas une acquisition, par le CST, d'information donnant lieu à une ARPVP à partir de [l'IMI][62] ». [redacted] a tout de même recommandé que le CST [traduction] « considère ces activités comme des techniques d'acquisition aux fins des demandes », tout en reconnaissant qu'il convient de reconnaître que le régime des autorisations de cybersécurité, au titre de a Loi sur le CST, ne peut s'appliquer à cette activité du CST[63]. En définitive, comme il a été dit, le CST a énuméré les activités en question dans sa demande au ministre, en les présentant comme des techniques d'acquisition.

73. Une fois que le ministre a délivré l'autorisation sur la foi des éléments constitutifs de la demande et que ladite autorisation a été acheminée au commissaire au renseignement (CR) pour approbation, celui-ci a décidé de ne pas approuver la partie de l'autorisation ayant trait à l'acquisition d'information provenant de sources externes et posant un risque d'atteinte à l'ARPVP d'un Canadien ou d'une personne se trouvant au Canada. Le CR a conclu qu'aucune information ni aucun raisonnement n'ont été présentés au ministre par le CST pour montrer comment l'acquisition, auprès de tierces parties, d'information posant un risque d'atteinte à l'ARPVP pouvait être autorisée en vertu des dispositions du paragraphe 27(1). En outre, le CR a précisé que [traduction] « à première vue, le libellé du paragraphe 27(1) ne considère ni ne permet la délivrance d'une autorisation en dehors de la sphère d'accès à l'infrastructure de l'information d'une institution fédérale[64] ». L'OSSNR note également que l'acquisition en question ne pouvait non plus être l'objet d'une autorisation au titre du paragraphe 27(2). Tel qu'elle est rédigée, la Loi sur le CST confine les activités du CST dans la majeure partie de l'IMI – hormis les infrastructures de l'information et les SDI – à celles qui n'exigent aucune autorisation.

74. Le tableau 1 ci-dessous propose la chronologie des événements ayant trait à cette question :

Date	Événement
2 septembre 2020	Le Centre pour la cybersécurité [redacted]
29 mars 2021	Un groupe du CST [redacted]
26 mai 2022	La cheffe du CST signe la demande 2022-2023 concernant les activités de cybersécurité dans les infrastructures fédérales. La demande contient de nouveaux libellés concernant l'acquisition, à partir de l'IMI, d'information posant le risque de porter atteinte à l'ARPVP d'un Canadien ou d'une personne se trouvant au Canada.
1er juin 2022	Le ministre de la Défense nationale délivre l'autorisation 2022-2023 au titre du paragraphe 27(1) de la Loi sur le CST pour des activités de cybersécurité dans

[61] Ibid.
[62] [redacted]
[63] Ibid., p. 6.
[64] Commissaire au renseignement, dossier nº 2200-B-2022-01, p. 10. Voir la figure 3.

	les infrastructures fédérales. Cette autorisation contient de nouveaux libellés concernant l'acquisition, à partir de l'IMI, d'information qui risque de porter atteinte à une ARPVP.
9 juin 2022	[redacted]
27 juin 2022	Le commissaire au renseignement approuve la demande 2022-2023 pour des activités de cybersécurité dans les infrastructures fédérales, sauf la portion de la demande portant sur l'acquisition, à partir de l'IMI, d'information posant le risque de porter atteinte à une ARPVP.

75. Même si le CR a décidé de ne pas approuver la portion de l'autorisation ministérielle portant sur l'acquisition, à partir de sources externes, d'information de cybersécurité pouvant porter atteinte à l'ARPVP d'un Canadien ou d'une personne se trouvant au Canada, le CST n'en a pas moins continué d'acquérir de l'information à partir de sources tierces[65]. Le CST a poursuivi son acquisition d'information auprès de ces sources, dans la mesure où il était d'avis que l'information en question ne constituait pas, à proprement parler, une acquisition par le CST ou à partir de l'IMI – et qu'en conséquence, la réception par le CST n'était, à son avis, aucunement interdite par les dispositions énoncées au paragraphe 22(4) de la Loi sur le CST[66, 67]. La décision de poursuivre l'acquisition de cette information externe après que le CR a rejeté la portion de l'autorisation s'y rapportant est préoccupante – particulièrement lorsqu'on tient compte de la nature d'au moins l'une de ces sources, dont il est question plus loin.

76. L'enquête de l'OSSNR en la matière a débuté au moment où le CST se penchait déjà sur la question; l'information a donc évolué à mesure que le CST définissait son approche. En novembre 2022, le CST a indiqué qu'il procédait à certaines évaluations, notamment, de considérations touchant la vie privée en rapport avec l'information utilisée dans le cadre des activités CAI faisant appel à des sources autres que les capteurs du CST, sans oublier une évaluation de la mesure dans laquelle ladite information pourrait contenir des éléments donnant lieu à une ARPVP. Selon le CST :

> [Traduction] « Lorsqu'une source a été [redacted] [le CST] élabore un cadre permettant de comprendre les éventualités sur le plan des ARPVP, rappelant que, dans ces cas, l'information [redacted] Dans les cas où le CST acquiert directement l'information et que celle-ci est susceptible de contenir des ICPC, des techniques sont conçues de sorte à prévenir non seulement la collecte d'ICPC, mais aussi toute atteinte à une ARPVP. »

Le CST a également reconnu que [traduction] « il est attendu que la notion d'ARPVP évolue sur le plan de la jurisprudence et des cas d'utilisation » et que le CST [traduction] « continuera de surveiller, d'apprendre et de s'adapter en conséquence. » De plus :

> [Traduction] « La Direction générale, Autorisations, conformité et transparence (ACT) a travaillé en interne [redacted] pour répertorier les sources de données

[65] Le CST a confirmé auprès de l'OSSNR que l'acquisition à partir de ces sources s'était poursuivie dans le cadre du volet CAI (art. 17) du mandat du CST.
[66] En l'occurrence, le CST était d'avis qu'il pouvait continuer de tirer parti de ces sources au titre de l'alinéa 17b) de la Loi sur le CST sans avoir obtenu d'autorisation.
[67] Il importe de noter que l'autorisation ministérielle de 2022-2023 qui a circulé au sein du CST n'a été ni modifiée ni délivrée de nouveau, de sorte que les libellés qui n'avaient pas été approuvés par le commissaire au renseignement n'ont pas été supprimés. Ainsi, la portion du texte qui n'a pas été approuvée est tout de même demeurée telle quelle dans l'autorisation ministérielle de 2022-2023 pendant la durée de la période d'autorisation, comme l'indiquent, par exemple, les paragraphes 47 et 48 de ladite autorisation. En revanche, la demande correspondante a été modifiée et affichait une mise en garde rappelant que les activités demandées dans la nouvelle section n'avaient pas été approuvées par le commissaire au renseignement.

> entrantes employées par le Centre pour la cybersécurité dans le but d'établir les types de données, la provenance des données (c.-à-d. IMI ou autre) et les modes suivant lesquels le Centre pour la cybersécurité a acquis les données ([redacted] communication ou autres modes) […]. D'après cette information, [redacted] a amorcé une évaluation de ces sources pour savoir si la source de données risquait de contenir des ICPC. De façon générale, l'information contenue dans ces [redacted] est de nature technique et ne poserait qu'un faible risque d'atteinte à une ARPVP[68] ».

77. Le CST a ensuite indiqué, en mai 2023, que la mise en place d'un cadre d'évaluation ou de définition de la notion d'ARPVP était difficile, notamment en raison de l'absence de jurisprudence en matière d'ARPVP dans le contexte de la cybersécurité. Concrètement, les opérateurs ont plutôt reçu des directives leur demandant de consulter l'unité interne de la conformité du CST, advenant qu'ils notent des changements dans leurs [redacted] ou leurs sources d'information. Selon le CST, bien que l'information collectée à partir de l'IMI et posant un risque d'atteinte à l'ARPVP d'un Canadien ou d'une personne se trouvant au Canada était déjà enregistrée dans les fonds du CST avant d'être reconnue et supprimée, les mêmes mesures d'atténuation s'imposant à toutes les ICPC étaient également appliquées – au cas par cas – à toute information portant atteinte à une ARPVP dès lors qu'un analyste en prenait connaissance. Le CST a rappelé que dès lors qu'elle est repérée dans les fonds du CST, l'information portant atteinte à une ARPVP est supprimée. Au milieu de 2023, la politique opérationnelle du CST a été retravaillée de sorte à mettre en place un cadre visant à faciliter la formulation de conseils destinés aux opérateurs quant à l'acquisition d'information auprès des sources ouvertes. Le CST a également indiqué à l'OSSNR qu'il faisait preuve de diligence raisonnable pour veiller à ce que [redacted] soient « réputées » et exercent leurs fonctions en toute légalité, bien qu'il n'ait pas été en mesure d'élaborer la question plus avant ni de présenter des exemples illustrant comment il s'y est pris ou envisage de s'y prendre.

78. Directement mobilisée dans ce dossier, l'unité interne de la conformité du CST a mené, notamment, un exercice de catégorisation suivant lequel [redacted] sources externes d'information de cybersécurité ont été examinées pour établir s'il y avait eu acquisition, *par* le CST, d'information *à partir de* l'IMI[69]. L'exercice de catégorisation du CST s'est déroulé [traduction] « suivant la position voulant que l'information acquise [redacted] puis reçue [redacted] par le CST aux fins d'exercice de son mandat ne devrait pas être considérée comme une acquisition par le CST à partir de l'IMI, au sens de la Loi sur le CST. Par conséquent, il y a lieu de considérer que cette information peut être acquise sans avoir à demander une autorisation ministérielle[70] ». Le CST a conclu que [redacted] des [redacted] sources n'avaient pas été acquises par le CST à partir de l'IMI. Par conséquent, il importe de souligner que le CST n'a pas formellement établi si les [redacted] sources contenaient de l'information risquant de porter atteinte à l'ARPVP d'un Canadien ou d'une personne se trouvant au Canada, même si au moins l'une de ces sources contenait de l'information qui, pourtant, posait ce risque. En termes simples, l'approche du CST consistait, dans ce contexte, à traiter la question de l'ARPVP seulement après que l'information pouvant porter atteinte à l'ARPVP avait été relevée dans le fonds du CST, plutôt que de façon proactive.

79. Parmi les [redacted] sources externes d'information de cybersécurité (sources non visées par une autorisation ministérielle), l'OSSNR en a examiné un certain nombre. En l'occurrence, l'OSSNR s'est davantage concentré [redacted] et le CST acquiert de l'information de [redacted] sous diverses formes, notamment, des rapports sur les menaces, des [redacted] d'IC ainsi que des ensembles de

---

[68] Soulignement ajouté par l'OSSNR.

[69] Notons que cet exercice de catégorisation a eu lieu après la décision du CR.

[70] Lorsque l'OSSNR lui a demandé comment il s'assurait que les fournisseurs tiers avaient acquis l'information légitimement, le CST n'a pas été en mesure de fournir des exemples concrets, ne proposant plutôt que des scénarios hypothétiques. L'OSSNR n'a reçu aucune indication montrant que le CST avait adéquatement évalué la légitimité des courtiers en données ou des autres fournisseurs auprès desquels il avait acquis l'information de cybersécurité requise pour ses activités CAI.

données consultables. Compte tenu de sa nature, il est probable qu'une partie de cette information porte atteinte à l'ARPVP d'un Canadien ou d'une personne se trouvant au Canada – y compris l'information autre que celle du GC.

80. Une fois l'exercice de catégorisation achevé, le CST a décidé, dans ce cas précis, que [traduction] « l'interrogation des ensembles de données [redacted] et l'extraction de l'information s'apparentaient à une acquisition par le CST, à partir de l'IMI », mais que des mesures peuvent être prises et le sont concrètement pour prévenir l'acquisition, depuis ces ensembles de données, d'information pouvant porter atteinte à l'ARPVP d'un Canadien ou d'une personne se trouvant au Canada. D'après le CST, tant que ces mesures sont en place et que l'information acquise ne porte aucune atteinte à l'ARPVP d'un Canadien ou d'une personne se trouvant au Canada, le CST peut continuer ce type d'acquisition sans autorisation ministérielle. Compte tenu de l'approche du CST consistant à ne se pencher sur l'information pouvant donner lieu à une ARPVP qu'une fois qu'elle se trouve dans le fonds d'information du CST, il est donc plausible que le CST acquière de l'information portant atteinte à l'ARPVP d'un Canadien ou d'une personne se trouvant au Canada sans avoir obtenu d'autorisation, et ce, malgré l'interdiction énoncée au paragraphe 22(4) de la Loi sur le CST.

81. En définitive, la conclusion générale que tire le CST en affirmant que l'acquisition d'information auprès de sources externes – par exemple, [redacted] – ne constitue pas une acquisition, par le CST, à partir de l'IMI soulève un certain nombre de questions. Selon l'article 2 de la Loi sur le CST, l'IMI est définie en termes généraux comme étant « les émissions électromagnétiques [...] les systèmes de communication, les systèmes et réseaux des technologies de l'information ainsi que les données et les renseignements techniques qu'ils transportent, qui s'y trouvent ou qui les concernent. » Spontanément, la recherche active d'information – par exemple, [redacted] pourrait s'assimiler à une acquisition. Or, l'avis du CST selon lequel sa réception d'information provenant de telles sources externes ne constitue pas une acquisition à partir de l'IMI est discutable et pourrait même comporter des risques.

82. L'acquisition d'information de cybersécurité auprès de sources se trouvant en dehors du cadre défini par voie d'autorisations ministérielles, qui *ne comporte aucun* risque d'atteinte à l'ARPVP d'un Canadien ou d'une personne se trouvant au Canada et qui ne contrevient d'aucune façon à une loi fédérale ne pose aucun problème sur le plan de la conformité. Toutefois, la pratique actuelle du CST consistant à omettre de vérifier, en amont de la procédure d'acquisition, si les sources d'information posent un risque d'atteinte à une ARPVP entraînera indéfiniment le risque que le CST conserve des données non évaluées qui contiendraient de l'information recueillie en dehors d'un cadre législatif et donneraient lieu à une ARPVP. Le Parlement a envisagé la nécessité d'acquérir, d'utiliser et de conserver ce type d'information contenant des éléments suscitant une ARPVP pendant le déroulement des activités CAI du CST. Or, le paragraphe 22(4) de la Loi sur le CST en interdit l'acquisition, l'utilisation et la conservation à moins que ces activités aient été autorisées par le ministre et approuvées par le CR. Ce régime de reddition de comptes ministérielle est donc un élément essentiel pour établir la légitimité de ces activités CAI. Pourtant, l'interprétation restreinte que le CST fait de l'énoncé du paragraphe 22(4) exclut de ce régime certaines de ces activités intrusives ou inhabituelles. De plus, le CST n'a pas précisé si son interprétation des dispositions générales reposait sur une interprétation particulière du terme « acquisition » ou sur la notion « d'infrastructure mondiale de l'information ». En l'occurrence, il y a lieu de se demander si l'interprétation de cette interdiction et des termes qui la ponctuent auront une incidence sur les activités du CST ou sur d'autres volets du mandat organisationnel.

83. Hormis la décision rendue par le commissaire au renseignement en 2022 concernant l'autorisation ministérielle des activités CAI dans les systèmes fédéraux, une décision du CR rendue subséquemment, en 2023, relativement à l'autorisation équivalente de 2023-2024 fut l'occasion d'examiner la décision de 2022 et d'évaluer le régime des autorisations ministérielles s'appliquant aux

activités CAI plus globalement[71]. Outre les faits établis dans le présent rapport, les deux décisions du CR montrent, au fond, que les activités CAI qui peuvent être autorisées au titre du paragraphe 27(1) subissent plus de contraintes que les interdictions énoncées au paragraphe 22(4). En l'occurrence, l'autorisation au titre du paragraphe 27(1) est contrainte en vertu du rapport avec « l'infrastructure de l'information des institutions fédérales ». En revanche, les interdictions analogues respectivement imposées par la loi et par le libellé des autorisations ministérielles s'appliquant au volet renseignement étranger du mandat du CST semblent équivalentes. Autrement dit, s'agissant du renseignement étranger, les activités interdites au titre du paragraphe 22(3) peuvent être autorisées par le ministre en vertu des dispositions énoncées à l'article 26.

84. Les divergences entre le paragraphe 22(4) et le paragraphe 27(1) semblent limiter les activités, notamment l'acquisition de certaines informations provenant de sources externes, qui seraient utiles aux mesures prises dans le cadre du volet CAI du mandat du CST et qui, par ailleurs, ne seraient pas proscrites par la Loi. Dans un document datant d'avril 2023 qui a été remis au ministre et au commissaire au renseignement, la cheffe du CST a qualifié ces divergences [traduction] « d'oubli de la rédaction législative[72] ».

Recommandation n° 5 : L'OSSNR recommande que le CST réévalue la question visant à établir si l'acquisition d'information, par le CST, à partir de l'infrastructure mondiale de l'information [conformément au paragraphe 22(4) de la Loi sur le CST] s'applique à l'information provenant des sources de données tierces. En l'occurrence, il faudrait prévoir une évaluation permettant d'établir si la *Charte canadienne des droits et libertés* peut être invoquée, puis analyser les cas où les sources de données tierces pourraient contenir de l'information portant atteinte à l'attente raisonnable en matière de protection d'un Canadien ou d'une personne se trouvant au Canada.

Recommandation n° 6 : L'OSSNR recommande, pour continuer les mesures d'acquisition qui sont nécessaires aux activités liées à la cybersécurité et à l'assurance de l'information (CAI), que le CST évalue ses sources actuelles d'information CAI – qui sont acquises en dehors du cadre d'une autorisation – pour vérifier si elles portent atteinte à l'attente raisonnable en matière de protection de la vie privée d'un Canadien ou d'une personne se trouvant au Canada. Cette évaluation devrait être réitérée suivant les besoins, pour veiller à ce que cette information ne soit pas acquise sans qu'une autorisation ministérielle ait été préalablement obtenue.

Recommandation n° 7 : L'OSSNR recommande que l'article 27 de la Loi sur le CST soit modifié de sorte à permettre au Ministre d'autoriser le CST à acquérir l'information qui lui est nécessaire dans le cadre du volet cybersécurité et assurance de l'information de son mandat (mais qui pourrait contenir de l'information portant atteinte à l'attente raisonnable en matière de protection de la vie privée d'un Canadien ou d'une personne se trouvant au Canada ou pourrait contrevenir à une autre loi fédérale), à partir de sources autres que les infrastructures de l'information fédérales et les systèmes d'importance pour le gouvernement du Canada.

[71] Commissaire au renseignement, dossier n° 2200-B-2023-02.
[72] Tel que cité dans Commissaire au renseignement, dossier n° 2200-B-2023-02, paragraphe 79.

V. CONCLUSION

85. Le CST et le Centre canadien pour la cybersécurité qui en relève exploitent un écosystème misant sur un ensemble intégré et complet de systèmes, d'outils de capacités en matière de cybersécurité. Cet écosystème protège l'information électronique et les infrastructures de l'information des institutions fédérales canadiennes, mais aussi les infrastructures désignées comme étant importantes pour le gouvernement du Canada. Il est conçu de sorte à appliquer, le cas échéant, des mesures visant à protéger la vie privée des Canadiens et des personnes se trouvant au Canada.

86. Dans le contexte du mandat de l'OSSNR en matière d'examen, il est particulièrement important de savoir que les capteurs SR et les activités qui s'y rattachent dans le cadre du programme CAI acquerront assurément de l'information se rapportant à des Canadiens ou à des personnes se trouvant au Canada, y compris de l'information portant atteinte à l'attente raisonnable en matière de protection de la vie privée d'un Canadien ou d'une personne se trouvant au Canada. L'OSSNR a formulé des conclusions et des recommandations s'appliquant à deux domaines particuliers : la transparence à l'égard du Ministre quant à la nature d'éléments se rapportant à certaines activités SR; et un problème particulier découlant d'une activité d'acquisition d'information à partir de sources externes, acquisition que le CST a continué d'exercer même si le commissaire au renseignement avait refusé de l'approuver.

87. Dans ce dernier cas, le problème découle d'une divergence sur le plan de la législation s'appliquant au CST. En effet, cette divergence semble réduire considérablement la possibilité de délivrer une autorisation qui permettrait d'acquérir une information pourtant nécessaire au déroulement du volet CAI du mandat du CST et qui donnerait au CST les moyens de protéger l'information électronique et les infrastructures de l'information.

88. Pendant la première moitié de la période d'examen, l'OSSNR a de nouveau éprouvé des difficultés du fait que le CST n'a pas réagi en temps opportun lorsqu'on lui a demandé l'accès à l'information que l'OSSNR avait le mandat d'analyser. En revanche, pendant la seconde moitié de l'examen, l'OSSNR a été plutôt satisfait de la réactivité du CST sur ce plan. Malgré les discussions continuelles avec le CST concernant la nécessité d'améliorer l'accès de l'OSSNR à l'information du CST, l'OSSNR a tout de même été en mesure d'examiner l'information reçue pendant la période d'examen, et ce, conformément à ses attentes.

89. L'information étudiée par l'OSSNR pendant le déroulement du présent examen a aussi favorisé le processus de renforcement des connaissances ayant trait au CST. Ce renforcement servira de fondement aux examens qui, à l'avenir, inciteront l'OSSNR à se pencher sur des enjeux plus pointus.

ANNEXE A : Cycle de vie de l'information

90. La présente annexe décrit la façon dont l'information transite dans l'écosystème de cyberdéfense du CST, depuis la collecte initiale – en l'occurrence par l'intermédiaire de capteurs réseau – jusqu'à la publication ou la communication de rapports basés sur cette information. Il est possible que certaines des informations de la présente section n'aient été actuelles que jusqu'à la fin de la période d'examen, soit le 17 juin 2021.

91. L'écosystème CAI du CST collecte un vaste éventail de données, notamment des paquets réseau, des activités/des événements survenus sur l'hôte et des registres/des journaux d'événements. Le cheminement des données se fait en quatre étapes : 1) la collecte, 2) l'analyse, 3) la conservation et l'élimination, et 4) l'établissement de rapport et l'utilisation. Au fil des étapes, les données se déplacent dans divers réseaux, depuis les réseaux non classifiés des partenaires jusqu'aux réseaux du CST. Chaque étape fait appel à plusieurs systèmes techniques qui fonctionnent soit par automatisation soit par intervention humaine. Le traitement et l'analyse des données de cybersécurité ne s'appliquent pas uniquement à un programme de capteurs donné ou à une source d'information particulière; d'ailleurs, les étapes 2 à 4 s'appliquent à toutes les sources de données de cybersécurité. À chacune de ces étapes, le CST a mis en place des mesures ayant pour but de protéger la vie privée des Canadiens et des personnes se trouvant au Canada, notamment des évaluations de la pertinence, de la nécessité et du caractère essentiel; des contrôles d'accès aux informations sensibles; des limites imposées aux mesures de conservation; et des mesures d'automatisation[73]. L'OSSNR n'a pas été en mesure d'examiner toutes les mesures ni de vérifier les détails de leur mise en œuvre, mais la présente section fournira tout de même une description de certaines de ces mesures.

Collecte

92. Les données exploitées par les systèmes CAI du CST sont collectées directement, suivant [redacted] d'un [redacted] SR, [redacted] solutions infonuagiques (SI) et des solutions du système hôte (SSH). Une copie des données est envoyée aux systèmes de traitement dans les réseaux classifié et non classifié du CST. Une fois reçues par les systèmes du CST, les données collectées sont considérées comme étant non évaluées ou encore comme étant « brutes », un qualificatif employé par le CST et repris dans la présente section.

93. Les données brutes sont copiées et sont ensuite traitées tour à tour par divers systèmes. [redacted]

[73] Le CST a fourni des exemples de 12 mesures de protection de la vie privée qu'il applique pendant les activités CAI autorisées. Or, l'OSSNR n'a pas été en mesure d'évaluer l'efficacité de ces mesures.

[redacted][74].

94. À ce stade, les données traitées sont considérées comme n'ayant pas encore été évaluées, puisqu'elles n'ont été traitées que par des fonctions automatisées et que, par conséquent, elles n'ont pas encore été visualisées par un analyste.

Analyse

95. Les analystes de la cybersécurité du CST se servent de plusieurs outils pour accéder aux données de cyberdéfense. Ces outils interrogent les métadonnées extraites en fonction de critères, exploitent des fonctions manuelles et automatisées, activent ces fonctions selon un calendrier et tirent parti de scripts rédigés par les analystes. Grâce à ces outils, les analystes peuvent accéder aux donnes brutes – notamment pour voir [redacted]

96. En plus des capteurs tripartites, l'information de cybersécurité du CST est renforcée par de l'information SIGINT, des renseignements communiqués[75], des ententes et d'autres sources accessibles au public comme [redacted] et les sources ouvertes[76]. Les analystes peuvent manuellement ou automatiquement interroger l'information des sources [redacted] et combiner celle-ci aux données brutes collectées par les capteurs du CST en vue de la préparation de mesures d'atténuation et de l'établissement de rapports.

97. Lorsqu'il relève des données qui répondent aux critères du CST en matière d'utilisation, d'analyse ou de conservation, l'analyste les enregistre dans la base de connaissances de cyberdéfense du CST[77]. Pour qu'elles soient conservées, les données SR doivent respecter le seuil d'essentialité du CST (la question est abordée plus loin dans la section sur la conservation et l'élimination) puisque le CST tient pour acquis que toutes les données SR contiennent des ICPC. Pour exposer les raisons pour lesquelles les données sont conservées, l'analyste doit les marquer en choisissant l'une des trois options possibles. Les données peuvent être conserves pour les motifs suivants : [redacted]

98. Compte tenu de la quantité et de la sensibilité de l'information produite par les divers outils d'analyse, l'accès est réservé au personnel du CST qui a suivi la formation et réussi le test permettant d'obtenir l'attestation des exigences prévues par la loi et la politique (AELP)[78]. Diverses actions du

---

[74] [redacted]

[75] Les communications de renseignements peuvent comprendre celles provenant de ministères clients de même que les communications volontaires de la part d'autres sources, notamment, les EIUI internationales, les divulgations publiques de maliciels sur mlwr.cyber.gc.ca, l'information échangée entre les partenaires de la Collectivité des cinq, etc.

[76] Le CST a recours [redacted] sources [redacted] pour réaliser ses analyses. En outre, cette information peut être mise à la disposition de divers volets du mandat du CST. En l'occurrence, [redacted]

[77] Cette base de connaissances contient l'information CAI évaluée et conservée, de même que l'information évaluée du renseignement étranger portant sur des questions de cybersécurité. L'information stockée dans cette base de connaissances peut être acheminée sous diverses formes à des clients ou des partenaires, et peut être employée pour alimenter des mesures d'atténuation visant à contrer les cybermenaces.

[78] La majeure partie du personnel inscrit à la liste AELP en 2020 et en 2021 ([redacted] % et [redacted] % respectivement) travaillait pour le volet CAI; les autres membres de ce personnel travaillaient pour le volet renseignement étranger ([redacted] % et [redacted] %), ou pour d'autres unités du CST ([redacted] % et [redacted] %). Or, le personnel inscrit à la liste AELP représentait, pour ces deux années, [redacted] % et

système sont enregistrées (par exemple, toutes les interrogations permettant d'accéder aux données traitées sont enregistrées et conservées pendant [redacted]) de sorte à permettre la tenue d'audits[79].

99. Dans certains cas, des processus automatisés évaluent les données à la place des analystes, notamment Assemblyline, un outil d'analyse de maliciels conçu par le CST[80]. Assemblyline effectue des analyses statiques et dynamiques sur des fichiers, notamment les fichiers joints à des courriels, pour reconnaître un maliciel ou tout autre contenu malveillant. Cet outil analyse tous les fichiers extraits automatiquement et alerte l'analyste dès lors qu'il relève des fichiers potentiellement malveillants. À l'aide d'une interface, les analystes peuvent ensuite examiner les fichiers à la recherche d'éléments malveillants; ils peuvent également extraire et conserver les données, s'il y a lieu. Ils ont aussi la possibilité d'automatiser la reconnaissance des fichiers malveillants en créant des filtres à même l'outil Assemblyline. Ces filtres permettent de reconnaître les fichiers comportant certaines caractéristiques. Ainsi, ils sont en mesure de relever les fichiers montrant les mêmes caractéristiques et d'en conserver automatiquement les données.

Conservation et élimination

100. Selon le CST, les données brutes doivent être supprimées [redacted] son acquisition[81] ». Bien que la temporalité soit calculée en fonction des systèmes, la plupart des données brutes sont supprimées bien avant l'échéance [redacted].[82]

101. Les fichiers traités au moyen d'Assemblyline sont assujettis à une approche [redacted] s'agissant de la conservation : [redacted]

102. Selon le niveau de sensibilité des données, le CST est appelé à suivre diverses normes de conservation axées sur des critères allant de la pertinence au caractère essentiel en passant par la nécessité[83] :

- Pertinence : [traduction] « Information pouvant être utilisée pour aider à protéger les systèmes fédéraux ou [les systèmes d'importance] et l'information électronique qu'ils contiennent. »
- Nécessité : Information qui est [traduction] « requise aux fins de compréhension des cyberactivités malveillantes », mais sans laquelle le CST peut tout de même

[redacted] % du nombre total des employés du volet CAI, alors que les pourcentages s'établissaient à [redacted] % et [redacted] % pour le volet renseignement étranger.

[79] L'OSSNR note que même si le CST a manifestement mis en place des mesures avancées de journalisation, il n'est pas évident de savoir de quelle façon le CST s'en sert au quotidien. Lorsque le CST a demandé certains calculs ou certaines réponses fondées sur les registres d'audit, les intervenants concernés du CST ont indiqué que des efforts considérables devraient être déployés pour rendre les registres utilisables. Comme l'OSSNR en a été témoin lors d'une démonstration technique, la capacité du CST à auditer l'information conservée dans les registres n'est pas des plus robuste; c'est d'ailleurs une tâche qui n'est pas forcément exercée régulièrement dans l'ensemble du programme SR.

[80] Une version d'Assemblyline est accessible en ligne à cette adresse : https://www.cyber.gc.ca/en/tools-services/assemblyline.

[81] EPM Cybersécurité, novembre 2020, section 12.2.

[82] Rapport du PCA du CST, « Examen de la conservation des données dans les systèmes du Centre pour la cybersécurité ». Bien qu'on ait conclu que les systèmes suivaient généralement les règles de conservation des données – notamment, en supprimant les données dans les [redacted] – le rapport fait état de plusieurs incidents de conformité où il est arrivé que des données brutes soient restées dans les systèmes plus [redacted] après leur collecte. Ce problème est généralement attribuable aux mises à niveau des logiciels ou à des erreurs de configuration dans les scripts de suppression. Dans ces cas de figure, la procédure consécutive aux incidents de conformité est enclenchée et finit par supprimer les données en question.

[83] EPM Cybersécurité, novembre 2020, Annexe E – Définitions.

reconnaître, isoler, prévenir ou atténuer les sources de dommage.

- Caractère essentiel : Information sans laquelle le CST n'est pas en mesure de reconnaître, d'isoler, de prévenir ou d'atténuer les sources de dommage.

103. Dans le cas des données acquises par l'intermédiaire des SR, le CST considère toute l'information comme de l'ICPC. En l'occurrence, le critère stratégique s'appliquant à la conservation est le caractère essentiel, et les analystes qui conservent lesdites données doivent justifier cette conservation en fonction de ce critère. Cette condition est respectée, comme il a été dit précédemment, suivant l'un de trois motifs : activité malveillante, connaissance de la situation ou développement des capacités[84]. Ces données sont conservées selon les exigences organisationnelles en matière de conservation ou encore; elles peuvent également être supprimées ou encore être acheminées à Bibliothèque et Archives Canada après une période qui varie de 10 à 30 ans en fonction de leur nature.

104. Le traitement selon lequel toute l'information SR constitue de l'ICPC a également une incidence sur la communication. D'après le CST, comme toute ICPC conservée par le CST a déjà été jugée comme étant « essentielle », cette ICPC peut être communiquée pour autant que cette communication soit nécessaire[85]. En l'occurrence, le CST estime qu'il s'agit d'un double seuil – caractère essentiel et nécessité – lorsque de l'ICPC est obtenue au titre d'une autorisation.

105. À ce stade, les données de la base de connaissances sont considérées comme ayant été évaluées, puisqu'elles ont été traitées directement, par un analyste, ou indirectement, en fonction des règles créées par l'analyste. Ces données peuvent ensuite être utilisées pour les produits de cyberdéfense, qu'il s'agisse de rapports ou de mesures défensives.

Établissement de rapports et utilisation

106. Lorsqu'un analyste – ou une procédure d'automatisation programmée par un analyste – reconnaît une menace grâce aux données de cyberdéfense (p. ex. [redacted]), cet analyste peut générer une tâche qui sera exécutée par le système de défense dynamique. Cette tâche est ensuite appliquée [redacted] Or, les ministères du GC qui sont prestataires des services de cyberdéfense du CST ont accès à une information limitée quant aux règles appliquées à leurs infrastructures respectives.

107. Les contenus de rapports sont divers, allant des indicateurs de compromission (IC) non classifiés aux adresses IP ou aux noms de domaines malveillants, à quoi s'ajoutent des produits de cybersécurité plus étoffés et communicables, notamment les rapports d'incidents [redacted]

- L'élaboration des rapports débute dans le réseau classifié. Un rapport peut simplement consister en [redacted] Les gestionnaires vérifient l'analyse et vérifient, par exemple, si toutes les preuves sur lesquelles s'appuie un rapport ont été conservées[86]. Subséquemment à

[84] Ces motifs correspondent aux justifications énoncées dans l'EPM Cybersécurité, novembre 2020, section 9.2.
[85] Document du CST : « *Background on necessary, essential* », mai 2018.
[86] L'ampleur des éléments de preuve retenus peut varier grandement. À titre d'exemple, pendant la démonstration du CST, l'OSSNR a remarqué [redacted] avait été intégralement conservée, [redacted] L'information [redacted] a ultérieurement été utilisée pour étayer un rapport [redacted] Bien que ces [redacted] fussent pertinents aux fins du rapport, on ignore pourquoi [redacted]

l'expurgation[87] et à l'approbation, les rapports peuvent être transférés à un réseau non classifié aux fins de communication à l'extérieur du CST.

- Tout dépendant de leur nature et de leur contenu, les rapports approuvés peuvent être communiqués manuellement à une diversité de partenaires, notamment à la Collectivité des cinq ou [redacted], aux ministères du GC ainsi qu'aux organismes responsables de l'infrastructure essentielle du Canada.
- Les IC peuvent être communiqués automatiquement à ces mêmes partenaires. En outre, les IC sont échangés en temps quasi réel par l'intermédiaire d'Aventail, [redacted]

108. Dans le cadre du volet CAI de son mandat, le CST échange un important volume d'information en interne, mais aussi à l'externe, avec le GC – pour peu que l'information soit pertinente pour le volet CAI du CST et qu'il soit essentiel d'échanger cette information avec une autre entité. Dans le cas des ICPC, ces échanges sont rendus possibles par voie d'arrêtés ministériels[88], lesquels autorisent le CST à communiquer les ICPC acquises par le volet CAI à des personnes ou des catégories de destinataires désignées par le ministre[89]. L'ICPC est généralement communiquée uniquement au propriétaire d'un système touché par un avis aux victimes (p. ex. pour repérer un ordinateur infecté).

109. Le CST a indiqué à l'OSSNR qu'il retirait « toute information personnelle » – c'est-à-dire toute information nominative sur un Canadien, toute ICPC et toute communication privée – des rapports avant de remettre ceux-ci à des partenaires, quoique le CST a ensuite ajouté qu'il était possible que ce ne soit pas le cas lorsqu'il [redacted] L'OSSNR a pris connaissance d'exemples de retrait (suppression), par le CST, d'information personnelle lorsqu'il s'est penché sur divers types de rapports de cybersécurité, notamment, à l'occasion d'une démonstration technique. Le CST peut diffuser des rapports ne contenant aucune ICPC à un lectorat plus large; c'est également cas lorsqu'il s'agit de communiquer des IC à des entités des secteurs privé et public par l'intermédiaire d'AVENTAIL[90].

110. Suivant un décret ministériel au titre de l'article 45 de la Loi sur le CST[91], d'autres entités au Canada et à l'étranger, entre autres les entités de la Collectivité des cinq, peuvent recevoir, de la part du CST, de l'information dont l'ICPC n'a pas été supprimée[92]. Dans ces cas de figure, l'ICPC est communiquée sous forme de produits de cybersécurité communicables[93]. D'après la politique interne du CST[94] et en vertu de la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères*, le CST doit procéder à une évaluation des risques de mauvais traitements lorsqu'il communique à des pays étrangers de l'information qui pourrait servir à identifier

---

[redacted] avait été intégralement conservée, [redacted]

[87] [Traduction] « L'expurgation est le processus de modification [...] du matériel permettant de le rendre diffusable auprès de personnes n'ayant pas reçu l'endoctrinement requis. », EPM Renseignement étranger, février 2021, section 25.8.
[88] Loi sur le CST, article 44
[89] Loi sur le CST, article 45.
[90] Pendant l'évaluation des communications d'information aux fins du présent examen, l'OSSNR a obtenu des saisies d'écran des bases de connaissances concernées et a reçu des produits de cybersécurité communicables du CST de même que les autorisations d'approbation connexes.
[91] Arrêté ministériel du CST, « Désignation des destinataires de l'information qui se rapporte à un Canadien ou à une personne se trouvant au Canada qui a été acquise, utilisée ou analysée dans le cadre des volets du mandat touchant la cybersécurité et l'assurance de l'information », 13 août 2021.
[92] Au titre de l'article 45 concernant les arrêtés ministériels, le CST peut communiquer des ICPC à des personnes ou catégories de personnes désignées par l'arrêté, lorsque la communication est nécessaire à la protection de l'information électronique ainsi que des infrastructures de l'information des institutions fédérales et des SDI [comme l'énonce le paragraphe 21(1) de la Loi sur le CST].
[93] EPM Cybersécurité, 2022, section 24.4.3.
[94] Ibid., section 10.4.

une personne, directement ou indirectement. L'OSSNR n'a pas examiné de près cette question ni d'autres ayant trait à la communication d'information de cybersécurité à l'extérieur du CST.

ANNEXE B : Utilisation de l'information de cybersécurité par divers volets

111. L'examen réalisé par l'OSSNR en 2020 et intitulé Examen des pratiques d'échange d'informations entre divers volets du mandat du CST (examen nº 2020-07) s'est penché sur les autorisations juridiques du CST ayant trait à la communication interne d'information entre le volet renseignement étranger et le volet CAI du mandat du CST en accordant une attention particulière à l'ICPC[95]. L'OSSNR a conclu que le cadre stratégique du CST s'appliquant à ce type de communication était conforme aux dispositions de la Loi sur le CST. D'après la politique du CST, une évaluation de la pertinence, de l'essentialité ou de la nécessité de l'ICPC pour chacun des volets concernés est requise pour la communication d'information entre ces volets.

112. Comme le décrivent les demandes de la cheffe au Ministre, l'information acquise au titre de l'autorisation visant les activités de cybersécurité dans l'infrastructure fédérale [traduction] « peut également être utilisée par le CST à d'autres fins permises par la Loi sur le CST. Par exemple, l'information peut servir à faciliter toute autre activité permise en vertu des autorisations visant les activités de renseignement étranger ou encore les opérations de cyberdéfense active ou défensive[96] ». La politique interne du CST en matière de cybersécurité avance également que :

> Sous réserve des conditions imposées par les clients et les entités divulgatrices, les membres du personnel du CST qui mènent des activités relevant d'un autre volet du mandat, sauf le volet touchant l'assistance, peuvent utiliser l'information considérée comme étant pertinente, nécessaire ou essentielle et conservée au titre du volet du mandat touchant la cybersécurité. Cette utilisation doit tout de même cadrer avec le volet du mandat touchant la cybersécurité (c.-à-d. aider à protéger l'information électronique ou les infrastructures des institutions fédérales ou des propriétaires des systèmes d'importance). Il s'agit d'une utilisation autorisée de l'information par le CST[97].

En vertu de l'article 16 de la Loi sur le CST, le volet renseignement étranger du mandat du CST a pour objet « [d'acquérir] secrètement ou d'une autre manière, de l'information à partir de l'infrastructure mondiale de l'information [IMI] 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 du renseignement étranger, en conformité avec les priorités du gouvernement fédéral en matière de renseignement. » Les priorités en matière de renseignement concernent certaines questions qui ont directement trait au volet CAI du mandat du CST, par exemple, « [redacted] » de même que « [redacted] » et « [redacted] »[98].

113. Un exemple d'utilisation, par le renseignement étranger du CST, de l'information CAI *évaluée* est l'usage que fait [redacted] Le CST peut également utiliser l'information CAI évaluée à des fins de cyberopérations défensives ou actives, pour peu que ces opérations soient liées à des activités de cybersécurité – notamment une cyberopération ciblant un cybercriminel qui pourrait représenter une menace pour les systèmes canadiens. Selon le CST, les analystes du SIGINT peuvent également accéder à l'information CAI *non évaluée*, ce qui comprend de l'information collectée en vertu

[95] Examen de l'OSSNR nº 2020-07.
[96] Demandes relatives aux activités de cybersécurité dans l'infrastructure fédérale 2020-2021, paragraphe 58. Quant au paragraphe 59, il avance que ces activités seraient auditables.
[97] CST, EPM Cybersécurité, février 2022, section 26.2.
[98] Ministre de la Défense nationale, Instructions du ministre au CST concernant les priorités du gouvernement du Canada en matière de renseignement pour les exercices 2021 à 2023, émises le 13 août 2021.

d'autorisations de cybersécurité [au titre des paragraphes 27(1) ou 27(2)]. Par exemple, [redacted] Toutefois, le CST a indiqué à l'OSSNR que lorsque les membres du personnel du SIGINT ont accès à l'information CAI brute ou interrogent cette information, ils le font au titre du volet CAI du mandat tu CST.

114. Comme c'est le cas pour les autorisations de cybersécurité accordées au CST, les autorisations visant les activités de renseignement étranger (RE) du CST [paragraphe 26(1) de la Loi sur le CST] font mention de la cybersécurité ainsi que de liens entre l'information du renseignement étranger et les activités CAI. Toutes les autorisations de la sorte stipulent que l'information qui est acquise à leur titre et qui est reconnue comme étant de l'ICPC [traduction] « sera utilisée, analysée ou conservée uniquement si l'information est essentielle aux affaires internationales, à la défense ou à la sécurité, ce qui comprend la cybersécurité[99]. » La politique interne du CST ajoute que :

> [Traduction] Le principal élément à prendre en compte lorsqu'il s'agit de communiquer de l'information de renseignement étranger devant être utilisée aux fins du volet cybersécurité du mandat du CST est la notion d'usage compatible – l'information acquise par le CST dans le cadre du volet renseignement étranger du CST doit être utilisée aux fins des activités du renseignement étranger, mais elle peut être ensuite mise à la disposition de destinataires agissant au titre des autorisations de cybersécurité pour peu que ces destinataires soient admissibles à recevoir et à utiliser ladite information dans le but d'exercer les activités prévues par leur mandat.
>
> [Traduction] Pour transmettre du RE au titre du volet cybersécurité du mandat du CST [...]. L'information doit être évaluée pour établir si elle a quelque valeur sur le plan du RE par rapport aux priorités du GC en matière de renseignement; l'ICPC peut être communiquée uniquement aux membres du personnel de la cybersécurité, pour peu qu'elle réponde au critère de l'aspect essentiel s'appliquant au renseignement étranger et qu'elle soit évaluée, s'il y a lieu, aux fins des activités de cybersécurité [...][100].

Par exemple, les analystes SIGINT du CST peuvent [redacted] ce qui signifie que les analystes du CAI peuvent agir en fonction de cette information pour protéger les systèmes contre les cybermenaces. Ainsi, l'information de cybersécurité acquise au titre du volet renseignement étranger peut être communiquée au CST aux fins d'utilisation dans le contexte des activités du volet CAI.

[99] Par exemple, ce type de libellé apparaît dans toutes les autorisations de renseignement étranger émises pour le CST en 2021-2022. Soulignement ajouté par l'OSSNR.
[100] CST, EPM Renseignement étranger, section 26.9, 18 février 2021 (version 5.0).

ANNEXE C : Conclusions et recommandations

Conclusions

Conclusion n° 1 : L'OSSNR conclut que le CST exploite un ensemble complet et intégré de systèmes, d'outils et de capacités de cybersécurité qui est apte à garantir une protection contre les cybermenaces et qui comporte des mesures visant à protéger la vie privée des Canadiens et des personnes se trouvant au Canada.

Conclusion n° 2 : L'OSSNR conclut que le CST a traité toutes les informations acquises par les solutions réseau (SR) en tenant compte de l'information se rapportant à des Canadiens ou à des personnes se trouvant au Canada (ICPC) et qu'il a appliqué toutes les mesures permettant de protéger les renseignements personnels se trouvant dans cette information acquise par l'intermédiaire de SR.

Conclusion n° 3 : L'OSSNR conclut qu'en raison de sa nature, l'information acquise par l'intermédiaire de SR comportera toujours de l'information se rapportant à des Canadiens ou à des personnes se trouvant au Canada (ICPC) et qu'il contiendra invariablement de l'information à l'égard de laquelle un Canadien ou une personne se trouvant au Canada pourrait avoir une attente raisonnable en matière de protection de la vie privée (ARPVP). Cet aspect n'a pas été communiqué de façon transparente au ministre lors de la présentation des demandes d'autorisation correspondantes.

Conclusion no 4 : L'OSSNR conclut qu'en raison de certaines ambiguïtés dans sa relation avec SPC, le CST n'a pas obtenu, aux fins des activités de cybersécurité et d'assurance de l'information, le consentement des propriétaires de systèmes comme il avait été décrit au ministre.

Conclusion n° 5 : L'OSSNR conclut que SPC n'était pas parfaitement au courant de ses responsabilités en tant que propriétaire de systèmes, contrairement à ce qui est énoncé dans les demandes que le CST a soumises au ministre.

Conclusion n° 6 : L'OSSNR conclut qu'en dépit d'un protocole d'entente établi entre le CST et SPC, il y a des éléments d'incompréhension entre les organisations relativement à l'exercice des responsabilités convenues sur le plan des activités SR dans les réseaux exploités par SPC.

Conclusion n° 7 : L'OSSNR conclut que le CST n'a pas exposé au ministre les motifs pour lesquels le consentement à l'égard des activités de cybersécurité du CST n'a raisonnablement pas été obtenu de la part des utilisateurs des systèmes du gouvernement du Canada.

Conclusion n° 8 : L'OSSNR conclut que l'application restrictive que le CST fait des dispositions visées au paragraphe 22(4) de la Loi sur le CST pose des risques sur le plan juridique et sur le plan de la reddition de comptes et, dans au moins un cas, a fait en sorte que le CST a acquis de l'information pouvant porter atteinte à l'attente raisonnable en matière de protection de la vie privée d'un Canadien ou d'une personne se trouvant au Canada. Cette information provenait d'une source qui n'était pas visée par le libellé des autorisations ministérielles.

Conclusion n° 9 : L'OSSNR conclut qu'une divergence entre les paragraphes 27(1) et 22(4) de la Loi sur le CST empêche le CST d'acquérir certaines informations provenant de sources externes, notamment les bases de données commerciales, dont l'information pourrait porter atteinte à l'attente raisonnable en matière de protection de la vie privée d'un Canadien ou d'une personne au Canada. Or, l'acquisition d'une partie de cette information renforcerait la capacité du CST à remplir son mandat en matière de cybersécurité et d'assurance de l'information.

Recommandations

Recommandation n° 1 : L'OSSNR recommande que dans ses demandes d'autorisation, le CST expose clairement au ministre les éléments suivants :

- que les solutions réseau acquièrent de l'information se rapportant à des Canadiens ou des personnes se trouvant au Canada (ICPC), notamment des informations qui contreviennent à l'attente raisonnable de Canadiens ou de personnes se trouvant au Canada en matière de protection de la vie privée (ARPVP);
- que le CST utilise, analyse et conserve ces données dans le cadre de ses activités en matière de cybersécurité et d'assurance de l'information.

Recommandation n° 2 : L'OSSNR recommande que le CST renouvelle le PE qu'il a conclu avec SPC en 2014, de sorte à veiller à ce que le CST et SPC remplissent adéquatement leurs engagements respectifs, y compris l'engagement voulant que le CST tienne le ministre au courant de la responsabilité de SPC qui consiste à aviser les propriétaires de systèmes au sujet du programme SR.

Recommandation n° 3 : L'OSSNR recommande que le CST mette à jour les protocoles d'entente (PE) qu'il a conclus avec tous ses partenaires de cybersécurité. Ainsi, il pourra veiller à ce que ces partenaires expriment leur consentement à l'égard des activités de cybersécurité du CST et à ce que les ententes soient intégralement conformes aux pouvoirs et aux modalités de gouvernance actuellement en vigueur. Au reste, le CST devrait adopter une pratique de mise à jour régulière de ces PE, de sorte à tenir compte de l'évolution des attributions.

Recommandation n° 4 : L'OSSNR recommande que le CST explique au ministre les modalités selon lesquelles il obtient le consentement des utilisateurs des systèmes du gouvernement du Canada relativement aux activités qu'il exerce en matière de cybersécurité ou, le cas échéant, les raisons pour lesquelles ce consentement n'a pas pu être raisonnablement obtenu.

Recommandation n° 5 : L'OSSNR recommande que le CST réévalue la question visant à établir si l'acquisition d'information, par le CST, à partir de l'infrastructure mondiale de l'information [conformément au paragraphe 22(4) de la Loi sur le CST] s'applique à l'information provenant des sources de données tierces. En l'occurrence, il faudrait prévoir une évaluation permettant d'établir si la *Charte canadienne des droits et libertés* peut être invoquée, puis analyser les cas où les sources de données tierces pourraient contenir de l'information portant atteinte à l'attente raisonnable en matière de protection d'un Canadien ou d'une personne se trouvant au Canada.

Recommandation n° 6 : L'OSSNR recommande, pour continuer les mesures d'acquisition qui sont nécessaires aux activités liées à la cybersécurité et à l'assurance de l'information (CAI), que le CST évalue ses sources actuelles d'information CAI – qui sont acquises en dehors du cadre d'une autorisation – pour vérifier si elles portent atteinte à l'attente raisonnable en matière de protection de la vie privée d'un Canadien ou d'une personne se trouvant au Canada. Cette évaluation devrait être réitérée suivant les besoins, pour veiller à ce que cette information ne soit pas acquise sans qu'une autorisation ministérielle ait été préalablement obtenue.

Recommandation n° 7 : L'OSSNR recommande que l'article 27 de la Loi sur le CST soit modifié de sorte à permettre au Ministre d'autoriser le CST à acquérir l'information qui lui est nécessaire dans le cadre du volet cybersécurité et assurance de l'information de son mandat (mais qui pourrait contenir de l'information portant atteinte à l'attente raisonnable en matière de protection de la vie privée d'un Canadien ou d'une personne se trouvant au Canada ou pourrait contrevenir à une autre loi fédérale),

à partir de sources autres que les infrastructures de l'information fédérales et les systèmes d'importance pour le gouvernement du Canada.