~~TRÈS SECRET//SI//RAC~~

Dossier : CST-2025-07

Bureau du commissaire au renseignement
Office of the Intelligence Commissioner

C.P./P.O. Box 1474, Succursale/Station B
Ottawa, Ontario K1P 5P6
613-992-3044 • télécopieur 613-992-4096

[TRADUCTION FRANÇAISE]

COMMISSAIRE AU RENSEIGNEMENT

DÉCISION ET MOTIFS

AFFAIRE INTÉRESSANT UNE AUTORISATION DE CYBERSÉCURITÉ
POUR DES ACTIVITÉS MENÉES DANS DES INFRASTRUCTURES NON FÉDÉRALES
EN VERTU DU PARAGRAPHE 27(2) DE LA
LOI SUR LE CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS ET DE
L'ARTICLE 14 DE LA *LOI SUR LE COMMISSAIRE AU RENSEIGNEMENT*

[...]

Canada

TABLE DES MATIÈRES

I. APERÇU

1. Il s'agit d'une décision concernant l'examen des conclusions du ministre de la Défense nationale (le ministre) autorisant le Centre de la sécurité des télécommunications (le CST) à aider à protéger l'information électronique et les infrastructures (c.-à-d. les systèmes, les dispositifs et les réseaux informatiques) appartenant à deux entités non fédérales (autorisation).

2. L'autorisation énumère les activités identiques approuvées par le commissaire au renseignement en [...] (décision CST-2024-05) relativement aux deux mêmes entités non fédérales – [...]. Aucune nouvelle activité opérationnelle n'est demandée.

3. Le [...], en vertu du paragraphe 27(2) de la *Loi sur le Centre de la sécurité des télécommunications*, LC 2019, c 13, art 76 (*Loi sur le CST*), le ministre a délivré l'autorisation, que le Bureau du commissaire au renseignement a reçue pour que je l'examine et l'approuve conformément à la *Loi sur le commissaire au renseignement*, LC 2019, c 13, art 50 (*Loi sur le CR*).

4. Pour les motifs ci-après, je suis convaincu que les conclusions tirées par le ministre en vertu des paragraphes 34(1) et (3) de la *Loi sur le CST* relativement aux activités ou aux catégories d'activités énumérées au paragraphe 75 de l'autorisation sont raisonnables.

5. Par conséquent, conformément à l'alinéa 20(1)a) de la *Loi sur le CR*, j'approuve l'autorisation.

II. CONTEXTE

6. Dans le cadre de son mandat, le CST mène des activités de cyberprotection pour défendre certains systèmes, dispositifs et réseaux électroniques ainsi que l'information qu'ils contiennent contre les cybermenaces que posent des criminels et des acteurs parrainés par des États. De plus, le CST fournit des avis et des conseils pour renforcer la posture de cybersécurité de ces systèmes (art 17, *Loi sur le CST*).

7. En l'espèce, les systèmes appartiennent à des entités non fédérales désignées comme étant d'importance pour le gouvernement fédéral – systèmes non fédéraux (art 27(2), *Loi sur le CST*). Pour lancer le processus, le propriétaire ou l'exploitant des systèmes doit demander par écrit l'aide du CST (art 33(3), *Loi sur le CST*).

8. Afin de comprendre les vulnérabilités et les compromissions, le CST accède aux systèmes et acquiert de l'information qu'ils contiennent. Ce faisant, le CST peut devoir contrevenir à certaines lois fédérales ou recueillir de l'information d'une manière qui porterait atteinte à une attente raisonnable de protection en matière de vie privée des Canadiens (citoyens canadiens, résidents permanents ou personnes morales formées sous le régime d'une loi fédérale ou provinciale) ou des personnes se trouvant au Canada. Une autorisation ministérielle est donc requise (art 22(4) et 27(2), *Loi sur le CST*).

9. L'autorisation énonce les conclusions du ministre – les motifs – à l'appui des activités ou des catégories d'activités que le CST peut mener. Le ministre doit, entre autres conditions, conclure que les activités proposées sont nécessaires (art 33(2), *Loi sur le CST*), raisonnables et proportionnelles (art 34, *Loi sur le CST*). Une autorisation est valide pendant une période maximale d'un an après l'approbation du commissaire au renseignement (art 36, *Loi sur le CST*). Ce n'est qu'à la suite de cette approbation que le CST peut mener les activités autorisées.

10. Malgré une autorisation, la *Loi sur le CST* impose des limites quant aux activités de cybersécurité du CST. Les activités du CST ne doivent pas viser des Canadiens ou des personnes se trouvant au Canada et ne peuvent porter atteinte à la *Charte canadienne des droits et libertés* (art 22(1), *Loi sur le CST*). Cependant, lorsqu'il mène ses activités, le CST peut acquérir incidemment de l'information qui se rapporte à des Canadiens ou à des personnes se trouvant au Canada, ce qui signifie qu'elle n'était pas délibérément recherchée (art 23(4) et (5), *Loi sur le CST*). Pour utiliser, analyser, conserver ou divulguer l'information, le CST est tenu par la loi de veiller à ce que des mesures soient en place pour protéger la vie privée des Canadiens et des personnes se trouvant au Canada (art 24, *Loi sur le CST*).

11. Une description des entités non fédérales et des activités de cybersécurité visées par l'autorisation figure à l'annexe classifiée de la présente décision (annexe A). L'annexe facilitera la lecture de la version de cette décision qui sera rendue publique. Elle permet aussi de veiller à ce que la décision présente la nature des faits dont j'ai été saisi, lesquels ne seraient autrement accessibles que dans le dossier.

12. Conformément à l'article 23 de la *Loi sur le CR*, le ministre a confirmé dans sa lettre de présentation m'avoir fourni tous les renseignements dont il disposait pour accorder l'autorisation en cause. Le dossier est donc composé de ce qui suit :

a) l'autorisation;
b) la note d'information de la chef du CST (la chef) à l'intention du ministre;
c) la demande de la chef, qui comprend quatorze annexes, dont les suivantes :
    i. lettres de demande des entités non fédérales;
    ii. deux arrêtés ministériels;
    iii. Tableau de conservation et de suppression;
    iv. Ensemble des politiques sur la mission en matière de cybersécurité (EPM) approuvé le 14 février 2025;
    v. Rapport sur les résultats pour 2024-2025;
d) le document d'information – aperçu des activités.

III. NORME DE CONTRÔLE

13. La *Loi sur le CR* exige que le commissaire au renseignement examine si les conclusions du ministre sont raisonnables. J'appliquerai donc la norme de la décision raisonnable, telle qu'elle est appliquée dans les contrôles judiciaires de mesures administratives.

14. Comme la Cour suprême du Canada l'a indiqué, lorsqu'elle procède au contrôle d'une décision selon la norme de la décision raisonnable, la cour de révision doit commencer son analyse à partir des motifs du décideur administratif. Au paragraphe 99 de l'arrêt *Canada (Ministre de la Citoyenneté et de l'Immigration) c Vavilov*, 2019 CSC 65, la Cour suprême du Canada décrit brièvement en quoi consiste une décision raisonnable :

> La cour de révision doit s'assurer de bien comprendre le raisonnement suivi par le décideur afin de déterminer si la décision dans son ensemble est raisonnable. Elle doit donc se demander si la décision possède les caractéristiques d'une décision raisonnable, soit la justification, la transparence et l'intelligibilité, et si la décision est justifiée au regard des contraintes factuelles et juridiques pertinentes qui ont une incidence sur celle-ci.

15. Les contraintes factuelles et juridiques pertinentes peuvent comprendre le régime législatif applicable et l'incidence de la décision. Le régime législatif applicable institué par la *Loi sur le CR* et la *Loi sur le CST* met en évidence la fonction de commissaire au renseignement en tant que mécanisme indépendant qui permet d'assurer un juste équilibre entre les mesures prises par le gouvernement à des fins de sécurité nationale et de renseignement et le respect de la primauté du droit ainsi que des droits et intérêts des Canadiens.

16. Lorsque le commissaire au renseignement est convaincu (*satisfied* en anglais) que les conclusions en cause du ministre sont raisonnables, il « approuve » l'autorisation (art 20(1)a), *Loi sur le CR*). À l'inverse, lorsqu'il n'est pas convaincu qu'elles sont raisonnables, il « n'approuve pas » l'autorisation (art 20(1)b), *Loi sur le CR*). Dans les deux cas, le commissaire au renseignement doit motiver sa décision.

IV. ANALYSE

17. Le [...], la chef a présenté au ministre une demande d'autorisation des activités proposées (demande). La demande énonce une description des entités non fédérales, les activités de cybersécurité que le CST souhaite mener ou continuer et décrit comment le CST analysera, traitera et conservera l'information acquise ainsi que les mesures en place pour protéger la vie privée des Canadiens et des personnes se trouvant au Canada, dans les cas où le CST acquiert incidemment de l'information sur eux.

18. La demande définit également les solutions de cybersécurité à continuer ou à déployer sur les systèmes non fédéraux – avec le consentement des entités non fédérales – pour permettre au CST d'acquérir des données de façon sécuritaire et de prendre des mesures d'atténuation, manuellement ou automatiquement. Les solutions sont les suivantes : [...]

19. Le ministre a conclu qu'il existe des motifs raisonnables de croire que l'autorisation est nécessaire et que les conditions des paragraphes 34(1) et (3) de la *Loi sur le CST* ont été remplies. Il a délivré l'autorisation avec une période de validité d'un an, sous réserve de mon approbation.

A. Dossier mis à jour

20. Dans des décisions antérieures, j'ai formulé un certain nombre de remarques qui soulèvent des questions juridiques ou factuelles préoccupantes pour améliorer le contenu des futures autorisations ou pour mettre en évidence une question que le CST doit prendre en considération. Je suis heureux de souligner la réactivité du ministre et du CST à ces remarques, ce qui renforce le régime d'autorisation.

21. Les réponses aux remarques dans le présent dossier comprennent des renseignements détaillés additionnels sur les types d'informations que conserve le CST et la communication de rapports avec des partenaires internationaux, ainsi que des renseignements sur les rapports communiqués aux entités non fédérales qu'elle appuie. L'autorisation apporte plus de clarté et de certitude quant aux types d'informations se rapportant aux Canadiens ou aux personnes se trouvant au Canada que le CST a acquises incidemment. Une justification de la présence continue du CST sur les systèmes non fédéraux a également été fournie.

22. Les lettres de demande des entités non fédérales ont également été améliorées par l'ajout des confirmations de l'autorisation légale des entités non fédérales de recueillir et de communiquer de l'information à des fins de cybersécurité. Je souligne que, dans sa note d'information à l'intention du ministre, la chef indique également que le CST continue d'examiner les options afin d'inclure un résumé des mesures prises par les entités non fédérales pour aviser les personnes dont les informations pourraient être acquises à des fins de cybersécurité et obtenir le consentement de ces personnes dans les futures autorisations. C'est avec intérêt que j'attends tout développement dans de futures autorisations.

23. Enfin, compte tenu du contexte de l'autorisation de l'année dernière, j'étais d'avis qu'il était dans l'intérêt public de rendre ma décision rapidement et que les motifs de ma décision ne

devaient pas retarder la mise en œuvre des solutions de cybersécurité par le CST sur les systèmes des entités non fédérales (CST-2024-05). Je remarque que l'une des solutions de cybersécurité approuvées n'a pas encore été déployée auprès de l'une des entités non fédérales, mais que ce retard n'est pas imputable au CST.

B. Les conclusions du ministre sont-elles raisonnables (art 34(1), *Loi sur le CST*)?

24. Le ministre a conclu qu'il avait des motifs raisonnables de croire que les activités sont raisonnables compte tenu de l'objectif qui consiste à aider à protéger l'information électronique et les infrastructures des entités non fédérales, ainsi qu'à éventuellement protéger les systèmes fédéraux et d'autres systèmes d'importance contre tout méfait, toute utilisation non autorisée ou toute perturbation de leur fonctionnement.

25. Le ministre reconnaît que les activités de cybersécurité énoncées dans l'autorisation entraîneront l'acquisition par le CST d'informations à l'égard desquelles les Canadiens ou les personnes se trouvant au Canada ont une attente raisonnable de protection en matière de vie privée. Je suis d'accord avec le ministre et cela confirme la nécessité de cette autorisation. Après avoir examiné le dossier, je suis convaincu que les activités de cybersécurité énoncées dans l'autorisation respectent l'exigence prévue par la loi selon laquelle les activités du CST ne doivent pas viser des Canadiens ou des personnes se trouvant au Canada (art 22(1), *Loi sur le CST*).

26. Pour justifier le caractère raisonnable des activités liées aux entités non fédérales, le ministre se fonde sur trois motifs : 1) l'efficacité des activités pour lesquelles l'autorisation est demandée; 2) la nécessité du soutien du CST compte tenu des rôles importants des entités non fédérales; et 3) la menace envers les systèmes des entités non fédérales que représentent les auteurs de cybermenaces.

27. Premièrement, les activités énoncées dans l'autorisation sont efficaces. Les conclusions du ministre ainsi que d'autres informations contenues dans le dossier montrent que le CST a réussi à détecter et à signaler les vulnérabilités et les compromissions. Sur les directives et les conseils du CST, les entités non fédérales ont mis en œuvre et continuent de mettre en œuvre

les recommandations décrites à l'annexe A. Les recommandations permettent aux entités non fédérales de mieux défendre leurs systèmes et de mieux les protéger contre de futures menaces.

28. Comme le ministre l'a expliqué, les entités non fédérales détiennent de grandes quantités de données et, compte tenu de leur nature, sont des cibles attrayantes pour les auteurs de menaces. Dans le cas de [description de la nature de l'entité non fédérale 1]. Le déploiement continu des solutions de cybersécurité du CST sur les systèmes de [entité non fédérale 2], qui agissent de concert avec les mesures commerciales, permettra au CST de réagir avec la rapidité nécessaire pour atténuer efficacement les compromissions. En fin de compte, elles permettront à [entité non fédérale 2] de protéger ses systèmes contre les dommages supplémentaires causés par des auteurs de menace.

29. Afin d'améliorer la cybersécurité, le ministre affirme que les connaissances et les cybersolutions du CST permettent d'intervenir en cas de menaces inconnues pour les fournisseurs commerciaux de solutions de cybersécurité. En effet, le CST dispose de renseignements spécialisés qui donnent un aperçu unique des capacités et des intentions des auteurs malveillants. Les activités énoncées dans l'autorisation permettent au CST de détecter les menaces de façon sophistiquée et de recommander des mesures d'atténuation ou de prendre des mesures d'atténuation, avec le consentement des entités non fédérales. Les résultats de l'autorisation de l'année dernière appuient également la conclusion du ministre selon laquelle les activités sont efficaces et raisonnables.

30. Le deuxième motif sur lequel se fonde le ministre est lié aux rôles essentiels joués par les entités non fédérales. Selon le ministre, les systèmes des entités non fédérales doivent être sécurisés compte tenu de leur rôle important dans la vie des Canadiens et des personnes se trouvant au Canada. [Entité non fédérale 1] offre des programmes et des services critiques aux Canadiens et est essentielle […]. Pour sa part, [entité non fédérale 2], fournit des services critiques pour soutenir […]. Selon le ministre, […]. L'importance de surveiller continuellement le contexte de la menace par rapport à de nombreux auteurs de menace est renforcée par les compromissions antérieures d'autres systèmes d'importance pour le gouvernement fédéral […]. Comme l'an dernier, j'estime que la description du rôle joué par

les entités non fédérales appuie la conclusion du ministre selon laquelle les activités énoncées dans l'autorisation sont raisonnables.

31. Le troisième motif qui appuie la conclusion du ministre est lié au contexte actuel des cybermenaces. Le dossier décrit les compromissions ainsi que les compromissions possibles des systèmes appartenant aux entités non fédérales – une information que j'ai ajoutée à l'annexe A. D'après l'information fournie par la chef, le ministre conclut que l'état actuel de la cybersécurité des deux entités non fédérales n'est pas suffisant pour découvrir et contrer les méthodes et les capacités sophistiquées déployées par des auteurs de menace avancés et tenaces. Le CST estime que [...]. Les deux entités non fédérales continueront de renforcer leur posture en matière de cybersécurité en mettant en œuvre les recommandations du CST.

32. Je suis d'avis que les conclusions du ministre établissent un fondement factuel pour obtenir l'assistance du CST et reflètent le fait qu'il a pris en considération le lien entre les besoins actuels des entités non fédérales et les activités de cybersécurité proposées, et en est convaincu. Il existe également un lien rationnel entre les activités de cybersécurité et l'efficacité de la protection des systèmes des entités non fédérales. Le ministre compte sur les rôles importants que jouent les entités non fédérales, et j'estime que ces rôles appuient ses conclusions. Par conséquent, j'estime que les conclusions du ministre quant au caractère raisonnable des activités énoncées dans l'autorisation sont raisonnables.

C. Les conclusions du ministre sont-elles proportionnelles (art 34(1), *Loi sur le CST*)

33. Le ministre a également conclu qu'il avait des motifs raisonnables de croire que les activités de cybersécurité proposées autorisées sont « proportionnelles compte tenu de la manière dont elles sont menées, et parce qu'elles ont un lien rationnel avec l'objectif à atteindre et ne porteront qu'une atteinte minimale aux droits et libertés de tiers, et [ceux des entités non fédérales], ainsi qu'à la capacité de tiers d'accéder à de l'équipement ou à des infrastructures ou de les utiliser. »

34. Le ministre indique les raisons pour lesquelles les activités sont nécessaires et utiles, notamment pour acquérir de l'information permettant d'aider à protéger les systèmes non fédéraux et de soutenir d'autres activités du CST. Il reconnaît que les activités peuvent mener

à l'acquisition de grands volumes d'informations pour découvrir des cybermenaces. Bien que les Canadiens et les personnes se trouvant au Canada puissent avoir une attente raisonnable de protection en matière de vie privée à l'égard de certaines informations, le ministre affirme que le CST s'intéresse aux comportements anormaux concernant l'information, plutôt qu'au contenu de l'information. Le CST ne conserve qu'un très faible pourcentage de la quantité totale de données acquises initialement. Je suis convaincu que les conclusions du ministre sont raisonnables en ce qui a trait aux activités autorisées.

35. Le ministre conclut que les activités sont proportionnelles en se fondant sur les mesures et les contrôles internes qu'applique le CST après l'acquisition des informations. Il s'agit des mêmes que celles énoncées dans l'autorisation de l'année dernière.

36. Je peux suivre le raisonnement du ministre lorsqu'il s'est appuyé sur ces mesures. L'accès à l'information acquise se limite aux employés désignés du CST qui sont formés pour manipuler ce type d'information et qui l'utilisent selon le principe du besoin de savoir pour effectuer leur travail. Le ministre était conscient des droits en matière de vie privée en jeu et il a énoncé les mesures mises en place pour les protéger.

37. Quant aux lois fédérales qui sont susceptibles d'être enfreintes, l'exercice de mise en balance du ministre est également évident. L'autorisation indique que leur nombre est limité, parce que le CST mènerait ses activités uniquement sur les systèmes pour lesquels il a reçu le consentement exprès des entités non fédérales. De plus, les activités doivent respecter la portée de celles décrites dans la demande de la chef et se limiter à l'acquisition de l'information pour protéger les systèmes non fédéraux et les systèmes fédéraux. À titre de mesure de protection supplémentaire, en cas de contravention à une loi fédérale qui ne figure pas dans la demande, la chef en informera le ministre et le commissaire au renseignement.

38. Les conclusions du ministre démontrent sa compréhension des droits en matière de vie privée et des mesures en place pour les protéger, ainsi que les incidences possibles sur la primauté du droit. Il explique comment les activités ont cherché à les mettre en balance d'une manière raisonnable. J'estime que ses conclusions sont justifiées et intelligibles. Je suis convaincu que

les conclusions du ministre concernant le caractère proportionnel des activités sont raisonnables.

D. Paragraphe 34(3) de la *Loi sur le CST* – les conditions nécessaires à la délivrance d'une autorisation

39. Après avoir établi que les activités sont raisonnables et proportionnelles en vertu du paragraphe 34(1) de la *Loi sur le CST*, le ministre peut délivrer une autorisation s'il conclut qu'il a des motifs raisonnables de croire que les trois conditions suivantes sont remplies (art 34(3), *Loi sur le CST*) :

a) l'information à acquérir au titre de l'autorisation ne sera pas conservée plus longtemps que ce qui est raisonnablement nécessaire;
b) l'information à acquérir est nécessaire pour découvrir, isoler, prévenir ou atténuer des dommages aux systèmes non fédéraux;
c) les mesures en place permettront d'assurer que l'information acquise au titre de l'autorisation qui est identifiée comme se rapportant à un Canadien et 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 aux systèmes non fédéraux.

i. L'information à acquérir au titre de l'autorisation ne sera pas conservée plus longtemps que ce qui est raisonnablement nécessaire (alinéa 34(3)a))

40. Comme l'a exposé le ministre, les exigences énoncées dans les politiques internes et le calendrier de conservation du CST permettent à ce dernier d'acquérir de grandes quantités d'informations générées par les systèmes des entités non fédérales ou se trouvant dans ceux-ci et de ne pas les conserver plus longtemps que ce qui est nécessaire. Le calendrier de conservation a été élaboré pour tenir compte des principes de gestion de l'information et intégrer les périodes de conservation minimales prévues par la *Loi sur la protection des renseignements personnels*, LRC, 1985, c P-21 et la *Loi sur la Bibliothèque et les Archives du Canada*, LC 2004, c 11.

41. Le ministre précise que les informations recueillies sont principalement traitées par le CST par des moyens automatisés. Bien que certaines des informations soient désignées comme étant « nécessaires » ou « essentielles », toute autre information est considérée comme étant

de l'information non évaluée, même si elle a fait l'objet du processus automatisé. La période maximale de conservation de l'information non évaluée est de 12 mois pour permettre au CST de remonter aux origines d'un événement ou d'examiner son évolution au fil du temps.

42. De plus, avant l'expiration de la période de 12 mois, l'information non évaluée sera automatiquement supprimée, à moins qu'elle soit jugée « nécessaire » ou « essentielle » pour aider à protéger les systèmes non fédéraux, ou les systèmes fédéraux et les systèmes désignés comme étant d'importance. La chef indique dans la demande que les entités non fédérales sont au courant de cette utilisation de l'information et l'acceptent.

43. Comme il est expliqué dans le dossier, le critère du caractère « nécessaire » s'applique à l'information qui, de par sa nature, ne contient aucun élément se rapportant à un Canadien ou à une personne se trouvant au Canada. Cette information aide le CST à réaliser des analyses de détection et de prévention et à renforcer davantage l'écosystème de cyberdéfense. L'information est « nécessaire » lorsqu'elle est requise pour comprendre une cyberactivité malveillante, […] dans le but de protéger les systèmes non fédéraux.

44. En revanche, le critère du caractère « essentiel » s'applique à l'information qui se rapporte à un Canadien ou à une personne se trouvant au Canada, comme […]. Sans cette information, le CST ne serait pas en mesure de découvrir, d'isoler, de prévenir ou d'atténuer des dommages aux systèmes non fédéraux. Le dossier explique que la plupart des analyses sont faites au moyen de processus automatisés qui signalent les comportements anormaux et limitent en conséquence l'exposition des employés au contenu des fichiers.

45. L'information qui est jugée nécessaire ou essentielle peut être conservée « indéfiniment ou jusqu'à ce qu'elle ne soit plus utile à ces fins ». Cette information fait l'objet d'un suivi conformément au programme de conformité interne du CST. Tous les trimestres, les gestionnaires des opérations « doivent examiner » l'information reconnue conservée qui se rapporte à des Canadiens ou à des personnes se trouvant au Canada afin de vérifier qu'elle est toujours essentielle. Je souligne qu'en réponse aux remarques formulées dans diverses décisions sur cette question, le ministre précise que le programme de conformité interne du CST fait circuler des rappels trimestriels aux analystes de la cybersécurité. De plus, comme

pratique opérationnelle, cette façon de faire se veut un rappel aux gestionnaires des opérations, qui ont la responsabilité de mener l'examen. Je comprends que l'EPM sera mis à jour pour tenir compte de cette exigence et je suis convaincu que les responsabilités des analystes de la cybersécurité et des gestionnaires des opérations seront clairement définies pour assurer la conformité. Je réitère qu'aux fins de mon examen, il est important que l'information présentée au ministre reflète avec exactitude la façon dont le CST mène ses activités et que la politique du CST soit claire pour ses employés (décision CST-2025-01, para 82).

46. Le ministre fait également valoir que l'accès à l'information non évaluée est strictement contrôlé et est limité aux personnes autorisées à mener ou à soutenir des activités de cybersécurité (art 10.2, EPM). Chaque interrogation effectuée à l'égard de l'information acquise non évaluée est enregistrée à des fins d'audit et de reddition de compte. L'information non évaluée ne peut pas être communiquée au-delà du CST. Enfin, le programme de conformité interne du CST dispose d'un processus établi pour intervenir au cas où l'information est conservée plus longtemps que la période autorisée.

47. Je suis d'avis que les conclusions du ministre sont raisonnables. L'information est conservée pour une durée qui permet de manière raisonnable au CST de mener efficacement ses activités de cybersécurité et d'élaborer les cyberinterventions requises afin de suivre le rythme de l'évolution rapide des techniques utilisées par les auteurs de menaces liées à des logiciels malveillants. De plus, les multiples couches de contrôles internes utilisées par le CST limitent l'accès à l'information non évaluée et permettent, en fin de compte, une meilleure protection tant des systèmes non fédéraux que des systèmes fédéraux.

ii. L'information à acquérir est nécessaire pour découvrir, isoler, prévenir ou atténuer des dommages aux systèmes non fédéraux (alinéa 34(3)c)).

48. Comme dans l'autorisation de l'année dernière, le ministre précise que, puisque le CST ne peut pas prédire [...], il doit acquérir une quantité importante d'informations auprès des systèmes non fédéraux qui sont ensuite évaluées pour découvrir les activités malveillantes. Ce faisant, étant donné que les systèmes sont situés au Canada, le ministre confirme que les activités de cybersécurité énoncées dans l'autorisation mèneront à la collecte et à la

conservation d'informations à l'égard desquelles les Canadiens ou les personnes se trouvant au Canada ont une attente raisonnable de protection en matière de vie privée.

49. La demande explique également que, même si les entités non fédérales utilisent des mesures de cybersécurité commerciales, leurs postures actuelles en matière de cybersécurité « sont insuffisantes pour détecter et contrer les méthodes et les capacités sophistiquées déployées par des auteurs de menaces avancés et tenaces ». Les connaissances et l'expertise du CST en matière de cybersécurité sont devenues de plus en plus importantes pour répondre aux outils et aux ressources complexes des auteurs de cybermenaces utilisés pour contourner les mesures de défense commerciales. La demande indique, par exemple, que le ciblage des réseaux appartenant au gouvernement fédéral a été constant [...].

50. Enfin, le ministre donne des exemples de la façon dont l'information acquise au titre de cette autorisation peut aussi être utilisée par le CST pour soutenir des activités au titre d'autres autorisations de cybersécurité et dans le cadre d'autres volets de son mandat. Avant de pouvoir l'utiliser, l'information se rapportant à des Canadiens ou à des personnes se trouvant au Canada doit avoir été évaluée comme étant essentielle à des fins de cybersécurité. L'utilisation, l'analyse, la conservation et la divulgation ultérieures de l'information acquise au titre de l'autorisation sont assujetties aux restrictions et aux conditions énoncées dans l'EPM.

51. Compte tenu de ce qui précède, je suis convaincu que les conclusions du ministre sont raisonnables.

iii. Les mesures visant à protéger la vie privée permettront de faire en sorte 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 aux systèmes non fédéraux (alinéa 34(3)d))

52. L'article 24 de la *Loi sur le CST* exige que le CST ait des mesures en place pour protéger la vie privée des Canadiens et des personnes se trouvant au Canada en ce qui a trait à

l'utilisation, à l'analyse, à la conservation et à la divulgation de l'information qui se rapporte à eux (IRC) et qui a été acquise dans le cadre du volet de son mandat touchant la cybersécurité.

53. Le ministre réitère que l'IRC ne peut être conservée que si elle est jugée essentielle. Les justifications relatives au caractère essentiel doivent être consignées par les employés (art 8.2.2, EPM). À mon avis, ces mesures contribuent à faire en sorte que le CST respecte son obligation prévue par la loi à l'article 24 et appuient les conclusions du ministre.

54. Pour que le CST divulgue de l'IRC, il faut que la divulgation soit nécessaire pour aider à protéger les systèmes non fédéraux, les systèmes fédéraux ou d'autres systèmes d'importance. Les conclusions du ministre et le dossier reflètent l'obligation prévue à l'article 44 de la *Loi sur le CST* qui limite la communication de l'information se rapportant aux personnes et aux catégories de personnes désignées en vertu de l'arrêté ministériel pris conformément à l'article 45 de la *Loi sur le CST*. Ces personnes ou catégories de personnes comprennent, par exemple, les propriétaires ou les administrateurs de systèmes informatiques ou de réseaux utilisés par le gouvernement fédéral ou une entité non fédérale, ainsi que les personnes et les catégories de personnes autorisées au sein d'entités étrangères avec lesquelles le CST a conclu des ententes. Dans mes remarques, je soulève une question concernant les destinataires désignés d'IRC.

55. Avant de communiquer de l'IRC, il faut suivre les mesures établies dans l'EPM (art 24). En effet, l'EPM définit les niveaux d'approbation requis pour la communication, lesquels doivent être consignés. Le CST supprime les informations nominatives, comme l'identité d'une personne. Je remarque dans leurs lettres de demande au CST que les entités non fédérales demandent que tous les renseignements personnels ainsi que tous les renseignements qui leur sont exclusifs et qui sont recueillis à partir de leurs systèmes et conservés soient masqués avant qu'ils ne soient communiqués à l'extérieur de l'entité et du CST.

56. L'EPM établit des politiques complexes visant à contrôler et à protéger l'IRC qui est acquise au titre d'une autorisation de cybersécurité. À mon avis, lorsqu'elles sont suivies, ces

mesures permettent au CST de respecter efficacement l'exigence prévue par la loi de protéger suffisamment cette information. Par conséquent, j'estime que la conclusion du ministre est raisonnable selon laquelle il a des motifs raisonnables de croire que l'IRC ne sera utilisée, analysée ou conservée que si elle est essentielle pour découvrir, isoler, prévenir ou atténuer les dommages aux systèmes des entités non fédérales.

V. REMARQUES

57. J'aimerais faire les trois remarques suivantes, qui ne modifient pas mes constatations concernant le caractère raisonnable des conclusions du ministre.

A. Un dossier complet – désignation des systèmes d'importance

58. Il est important que le ministre comprenne parfaitement comment l'IRC recueillie et conservée par le CST pourrait être communiquée – en particulier comment elle pourrait être communiquée à l'extérieur du Canada. Je suis d'avis que cette information devrait être plus détaillée dans le dossier à l'intention du ministre.

59. Comme il a été mentionné précédemment, l'article 44 de la *Loi sur le CST* limite la communication de l'IRC acquise dans le cadre du volet du mandat du CST touchant la cybersécurité aux personnes et catégories de personnes désignées en vertu d'un arrêté ministériel pris en vertu de l'article 45 de la *Loi sur le CST*. Le 13 juin 2023, conformément à l'article 45 de la *Loi sur le CST*, le ministre en fonction à l'époque a émis l'*Arrêté ministériel désignant les 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 du CST touchant la cybersécurité et l'assurance de l'information* (Arrêté sur les destinataires de l'IRC). Cet arrêté autorise le CST à communiquer de l'IRC à des fins de cybersécurité à des personnes ou à des catégories de personnes désignées, y compris les propriétaires ou les exploitants de systèmes d'importance.

60. Par conséquent, la désignation des systèmes d'importance a une incidence sur comment l'IRC peut être communiquée. Le dossier comprend une copie de l'*Arrêté ministériel*

désignant l'information électronique et les infrastructures de l'information d'importance pour le gouvernement du Canada (Arrêté sur les SDI) datée du 25 août 2020. En plus de désigner des catégories de systèmes d'importance (art 21, *Loi sur le CST*), je remarque que l'article prévoit que l'information électronique et/ou les infrastructures de l'information des entités mentionnées expressément à l'annexe 2 de l'Arrêté sur les SDI sont désignées comme étant importantes pour le gouvernement fédéral – bien que l'annexe 2 ne contient aucune désignation.

61. Toutefois, l'Arrêté sur les SDI ne semble pas être le seul arrêté désignant les systèmes d'importance. Selon le rapport annuel public du CST de 2022-2023, l'information électronique et les infrastructures de l'information de l'Ukraine et de la Lettonie ont été désignées comme étant importantes pour le gouvernement fédéral par deux arrêtés distincts pris le 17 mars 2022. Le rapport précise qu'il s'agit de la première fois que le ministre a utilisé ses pouvoirs pour désigner des entités à l'extérieur du Canada comme étant des systèmes d'importance. De plus, le rapport annuel du CST de 2024-2025 confirme que, au 31 mars 2025, des arrêtés désignant l'information électronique et les infrastructures de l'information des gouvernements de l'Ukraine et de la Lettonie étaient en vigueur. Le dossier ne contient pas d'information concernant ces arrêtés ni n'aborde toute communication éventuelle d'IRC en vertu de ceux-ci. Bien qu'il ne soit pas nécessaire de verser une copie de ces arrêtés au dossier, le ministre devrait néanmoins avoir une vue d'ensemble des endroits où l'IRC pourrait être communiquée.

B. Contenu des lettres de demande

62. Dans la décision CST-2025-01, j'ai formulé une remarque selon laquelle il serait utile que les lettres de demande donnent un aperçu général des raisons pour lesquelles l'entité non fédérale demande le soutien du CST. En réponse, comme il a été reconnu dans la décision CST-2025-06, le dossier suivant relatif à une autorisation pour une entité non fédérale comprenait des lettres de demande renfermant certaines informations à cet effet. Ces lettres font partie du fondement factuel que le ministre doit examiner, et le ministre mentionne expressément qu'il s'est appuyé sur elles dans les autorisations en vigueur.

63. Je suis d'avis que les lettres peuvent être modifiées de façon à mieux refléter les circonstances de la demande, en particulier, il faudrait préciser s'il s'agit d'une demande initiale ou d'un renouvellement d'une autorisation. Sans cette information au dossier, il n'est pas clair, d'après les lettres actuelles, que les entités non fédérales ont déjà bénéficié de l'aide du CST au titre d'une ancienne autorisation.

64. Je suis conscient de facteurs qui peuvent limiter le niveau de détail pouvant être inclus dans les lettres de demande, par exemple pour des raisons de sécurité ou simplement parce que l'entité non fédérale ne comprend pas encore pleinement l'effet d'une compromission. Néanmoins, comme première étape qui déclenche le processus menant à une autorisation de cybersécurité, une lettre de demande sert de moyen de fournir au ministre et à moi-même un contexte utile pour mieux comprendre la justification de la demande ou pourquoi le soutien continu du CST est nécessaire.

65. Enfin, j'ai remarqué que l'une des lettres de demande au dossier est datée […], qui vient après la date de la signature de l'autorisation et après que le BCR l'a reçu pour que je l'examine. De plus, la demande et l'autorisation ne font référence qu'à une seule demande écrite. Bien que de telles erreurs de rédaction apparentes ne nuisent pas à elles seules au caractère raisonnable des conclusions du ministre, je réitère ma remarque précédente selon laquelle une accumulation suffisante de ces dernières pourrait le miner (décision CST-2023-05).

C. Obligation d'avis – [Déploiement de certaines capacités de cybersécurité]

66. Dans une note d'information autonome datée […], fournie à mon bureau, la chef informait le ministre que le CST avait pour la première fois déployé [certaines capacités de cybersécurité] Ce faisant, la chef a rempli une obligation d'avis dans plusieurs autorisations actives.

67. Je souligne toutefois que la demande – également datée […] – et l'autorisation n'ont pas été mises à jour et continuent d'indiquer que [les capacités de cybersécurité] n'ont pas encore été déployées. Cela souligne l'importance de mettre à jour, ou au besoin, de corriger après coup, les dossiers pour que le ministre reçoive une information à jour.

68. J'espère recevoir plus d'informations à l'avenir sur le déploiement et l'impact de ces capacités.

VI. CONCLUSIONS

69. D'après mon examen du dossier, je suis convaincu que les conclusions tirées par le ministre en vertu des paragraphes 34(1) et (3) de la *Loi sur le CST* à l'égard des activités énumérées au paragraphe 75 de l'autorisation sont raisonnables.

70. J'approuve donc, en vertu de l'alinéa 20(1)a) de la *Loi sur le CR*, l'autorisation de cybersécurité pour des activités menées dans des infrastructures non fédérales délivrée par le ministre le […].

71. Comme le ministre l'a indiqué, et en vertu du paragraphe 36(1) de la *Loi sur le CST*, cette autorisation expire un an après la date de mon approbation.

72. Conformément à l'article 21 de la *Loi sur le CR*, une copie de la présente décision sera remise à l'Office de surveillance des activités en matière de sécurité nationale et de renseignement afin de l'aider à réaliser les éléments de son mandat au titre des alinéas 8(1)a) à c) de la *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement*, LC 2019, c 13, art 2.

[…]

(Original signé)

L'honorable Simon Noël, c.r.
Commissaire au renseignement