

National Security and Intelligence
Review Agency



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

~~TRÈS SECRET~~ //  // ~~CCS~~

EXAMEN DES AUTORISATIONS MINISTÉRIELLES ET DES ARRÊTÉS MINISTÉRIELS DU CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS (CST) EN VERTU DE LA LOI SUR LE CST

(EXAMEN DE L'OSSNR 08-501-5)

I	SOMMAIRE	3
II	FONDEMENT LÉGISLATIF	5
III	INTRODUCTION	5
IV	CONTEXTE	6
V	CONCLUSIONS ET RECOMMANDATIONS	7
VI	CONCLUSION	20
	ANNEXE A : Objectif	21
	ANNEXE B : Portée et méthode	22
	ANNEXE C : Liste des autorisations ministérielles et des arrêtés ministériels	23
	ANNEXE D : Exposés	26
	ANNEXE E : Conclusions et recommandations	27
	ANNEXE F : LOI SUR LE CST : AIDE-MÉMOIRE	29

I SOMMAIRE

1. (NC) Après l'entrée en vigueur de la *Loi sur le Centre de la sécurité des télécommunications (Loi sur le CST)*, le CST a reçu un nouvel ensemble d'autorisations ministérielles (AM) : des documents écrits par l'entremise desquels le ministre de la Défense nationale autorise le CST à réaliser des activités qui risquent de contrevenir aux autres lois fédérales ou de porter atteinte à une attente raisonnable de protection en matière de vie privée. La *Loi sur le CST* a également conféré au ministre de la Défense nationale le pouvoir de « désigner comme étant importante pour le gouvernement fédéral de l'information électronique, des infrastructures de l'information ou des catégories d'information électronique ou d'infrastructures de l'information » au moyen d'un arrêté ministériel.
2. (NC) L'examen fondamental¹ de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR) sur les AM et les arrêtés ministériels du CST adopte une approche différente à l'égard de l'examen des AM de celle du Bureau du commissaire du Centre de la sécurité des télécommunications (BCCST), l'ancien organisme d'examen indépendant et externe du CST. Même si le BCCST a déjà produit des rapports sur le nombre de communications privées, nous laissons cette question au rapport annuel classifié du CST à l'intention du ministre. En outre, il n'est pas nécessaire d'examiner si les AM sont fondées sur des conclusions raisonnables, car cette responsabilité incombe au commissaire au renseignement. L'OSSNR a choisi d'aborder les AM dans le but d'en apprendre davantage sur les activités opérationnelles du CST et d'examiner les arrêtés ministériels comme un complément aux AM.
3. (NC) Le ministre a autorisé sept AM et trois arrêtés ministériels en 2019 en vertu de la *Loi sur le CST*². L'OSSNR a reçu des exposés complets sur les activités autorisées par chaque AM et a pu se servir de cette information pour orienter son plan d'examen triennal sur le CST.
4. (NC) Selon les documents fournis par le CST, l'OSSNR estime que le CST a fait preuve de rigueur dans le cadre du processus d'application des AM. Toutefois, l'OSSNR a formulé les cinq conclusions suivantes, ainsi que les recommandations connexes, dans le but d'améliorer la transparence et la responsabilisation du CST.
 - (NC) Conclusion n° 1 : Les demandes d'autorisation de la chef du CST fournissaient suffisamment d'information au ministre pour respecter les conditions du paragraphe 33(2) de la *Loi sur le CST*. Les nouvelles demandes comportent plus d'information que les demandes antérieures présentées au titre de la *Loi sur la défense nationale* (LDN) et assurent une plus grande

1. Un examen fondamental vise à fournir un aperçu du sujet afin d'acquérir des connaissances de base et d'éclairer de futurs examens.

2 Voir une liste des autorisations ministérielles et des arrêtés ministériels à l'annexe C.

transparence des activités du CST.

- (S) Conclusion n° 2 : Même si ces activités n'ont pas encore eu lieu, rien ne laisse croire que le CST a pleinement évalué les ramifications, juridiques ou autres, des activités autorisées par l'AM [REDACTED]. [REDACTED]
[REDACTED]
[REDACTED]
- (S) Recommandation n° 1 : Le CST doit chercher à obtenir une évaluation juridique complète des activités autorisées par l'AM [REDACTED] avant d'entreprendre des activités de collecte au titre de cette AM. L'avis juridique doit déterminer si un régime de justification implicite est créé dans l'AM [REDACTED]
- (NC) Conclusion n° 3 : Les lettres de [REDACTED] ayant trait à la consultation du ministre de la Défense nationale avec le ministère des Affaires étrangères pour les cyberopérations actives (COA) et les cyberopérations défensives (COD) n'étaient pas datées. Cette consultation précise avec Affaires mondiales Canada n'a pas été suffisamment documentée.
- (NC) Recommandation n° 2 : Le CST doit s'assurer que le processus de consultation relatif aux COA et aux COD avec Affaires mondiales Canada est suffisamment documenté, le plus précisément possible, pour qu'il soit facile de vérifier si la séquence prévue par la loi est respectée.
- (NC) Conclusion n° 4 : Le CST n'a pas été en mesure de fournir une évaluation de ses obligations au titre du droit international pertinentes pour la réalisation de COA.
- (NC) Recommandation n° 3 : Le CST doit obtenir une évaluation juridique officielle du régime législatif international applicable à la réalisation de COA avant d'entreprendre de telles opérations.
- (NC) Conclusion n° 5 : L'arrêté ministériel intitulé *Arrêté ministériel désignant des destinataires de renseignements canadiens d'identification acquis, utilisés et analysés en vertu d'une autorisation ministérielle de renseignement étranger* comprend [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
- (NC) Recommandation n° 4 : Un arrêté délivré en vertu de l'article 45 de la *Loi sur le CST* doit être le plus précis possible et détailler clairement la liste de personnes ou de catégories de personnes désignées qui peuvent recevoir de

³ Depuis, l'autorisation a été renommée [REDACTED]

l'INCPD divulguée par le CST.

4. (NC) L'examen fondamental a fait ressortir le besoin de se concentrer sur les COA et les COD immédiatement après l'achèvement du présent examen, étant donné que le commissaire au renseignement n'approuve pas ces activités et que ces dernières représentent un nouveau volet du mandat du CST.

II FONDEMENT LÉGISLATIF

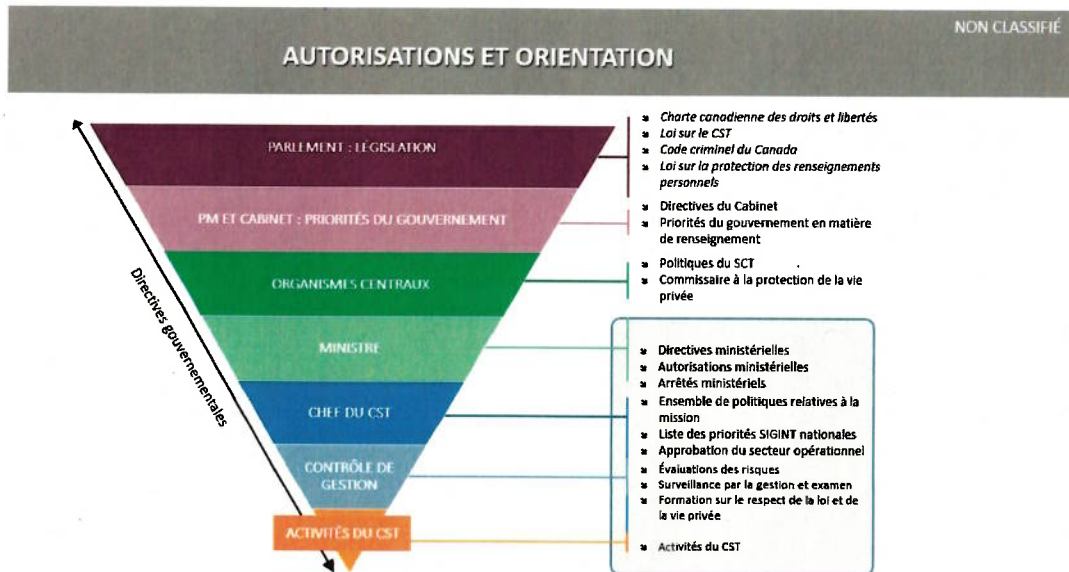
5. (NC) Le présent examen a été réalisé en vertu des pouvoirs prévus aux alinéas 8(1)a) et 8(1)b) de la *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement* (Loi sur l'OSSNR).

III INTRODUCTION

6. (NC) La *Loi sur le Centre de la sécurité des télécommunications* (Loi sur le CST) est entrée en vigueur le 1^{er} août 2019 et remplace la partie V.1 de la *Loi sur la défense nationale* (LDN) comme loi principale régissant le CST. Par la suite, le CST a reçu de nouvelles autorisations ministérielles. En outre, la *Loi sur le CST* confère au ministre de la Défense nationale le pouvoir de « désigner comme étant importante pour le gouvernement fédéral de l'information électronique, des infrastructures de l'information ou des catégories d'information électronique ou d'infrastructures de l'information » par l'entremise d'un arrêté ministériel.

- **Autorisation ministérielle (AM)** : document écrit par l'entremise duquel le ministre autorise le ministère à mener des activités qui risquent de contrevenir aux lois fédérales ou de porter atteinte à une attente raisonnable de protection en matière de vie privée d'un Canadien ou d'une personne se trouvant au Canada.
- **Arrêté ministériel** : instrument par l'entremise duquel un ministre présente des arrêtés et qui ne nécessite pas l'approbation du Cabinet. Les arrêtés sont créés au titre d'un pouvoir législatif ou réglementaire accordé à un ministre.

Ces documents sont rédigés par le CST et délivrés par le ministre de la Défense nationale.



7. (NC) Le présent rapport fournit un aperçu des AM et des arrêtés ministériels du CST, en mettant l'accent sur certaines activités qui ont été récemment autorisées en vertu de la *Loi sur le CST* ou qui n'ont pas fait l'objet d'examen antérieurs par le Bureau du commissaire du Centre de la sécurité des télécommunications (BCCST).

IV CONTEXTE

8. (NC) Le ministre de la Défense nationale délivre des AM, qui permettent au CST de mener des activités qui, autrement, seraient illégales⁴. La *Loi sur le CST* prévoit cinq types d'AM : renseignement étranger, cybersécurité – infrastructures fédérales, cybersécurité – infrastructures non fédérales, cyberopérations actives et cyberopérations défensives. Chaque AM comprend un éventail d'activités pouvant être autorisées⁵.

9. (NC) Pour délivrer une AM au titre de la *Loi sur le CST*, le ministre doit être en mesure de conclure, par l'entremise d'une demande écrite présentée par la chef du CST, qu'il existe des motifs raisonnables de croire que l'autorisation est nécessaire et que les conditions de sa délivrance sont remplies⁶. Comme la LDN, la *Loi sur le CST* énumère les conditions à remplir pour chaque autorisation, notamment une condition

⁴ Conformément aux paragraphes 22(3) et 22(4) de la *Loi sur le CST*, les activités menées par le CST dans la réalisation des volets de son mandat touchant le renseignement étranger et la cybersécurité ne doivent pas contrevenir aux autres lois fédérales ni viser l'acquisition par celui-ci d'information qui porterait atteinte à une attente raisonnable de protection en matière de vie privée, à moins d'être menées au titre d'une autorisation.

⁵ Conformément aux articles 27 et 28 de la *Loi sur le CST*, le ministre de la Défense nationale peut délivrer des autorisations de renseignement étranger et de cybersécurité au CST, habilitant ce dernier à mener les activités précisées dans une AM dans la réalisation de son mandat.

⁶ *Loi sur le CST*, paragraphe 33(2).

générale selon laquelle les activités autorisées doivent être raisonnables et proportionnelles compte tenu de la nature de l'objectif à atteindre et des activités⁷. Le ministre peut également modifier une autorisation si des faits exposés dans la demande d'autorisation ont considérablement changé⁸.

10. (NC) Conformément à l'article 12 de la *Loi sur le commissaire au renseignement* (CR), ce dernier examine et approuve les AM de renseignement étranger et de cybersécurité qui sont délivrées par le ministre de la Défense nationale. Les autorisations de cyberopérations actives et défensives délivrées par le ministre de la Défense nationale ne requièrent pas l'approbation du CR⁹. Les AM des activités autres que les cyberopérations actives et défensives entrent en vigueur seulement après avoir été approuvées par le CR.

11. (NC) Le paragraphe 21(1) de la *Loi sur le CST* confère également au ministre le pouvoir de « désigner comme étant importante pour le gouvernement fédéral de l'information électronique, des infrastructures de l'information ou des catégories d'information électronique ou d'infrastructures de l'information ». En ce qui concerne la divulgation d'information, pour le renseignement étranger et la cybersécurité, l'article 45 confère au ministre le pouvoir de désigner les personnes ou les catégories de personnes qui peuvent recevoir de l'information qui se rapporte à un Canadien ou à une personne se trouvant au Canada.

V CONCLUSIONS ET RECOMMANDATIONS

12. (NC) Conformément au paragraphe 26(1) de la *Loi sur le CST*, le ministre peut délivrer une autorisation de renseignement étranger. Trois AM ont été délivrées en vertu du paragraphe 26(1) en 2019:

- a. (S) [REDACTED]
- b. (S) [REDACTED]
- c. (S) [REDACTED]

13. (NC) Une seule autorisation a été délivrée pour chacune de ces sous-sections au titre de la *Loi sur le CST* :

- a. autorisation de cybersécurité – infrastructures fédérales (27[1]);
- b. autorisation de cybersécurité – infrastructures non fédérales (27[2]);
- c. autorisation de cyberopérations défensives (29[1]);
- d. autorisation de cyberopérations actives (30[1]).

⁷ *Loi sur le CST*, article 34.

⁸ *Loi sur le CST*, article 39.

⁹ Les autorisations de cyberopérations actives et défensives nécessitent la participation du ministre des Affaires étrangères.

14. (S) Contrairement aux AM délivrées en vertu de la LDN, les AM délivrées en vertu de la *Loi sur le CST* fournissent de l'information plus approfondie concernant les activités du CST. Les AM de la *Loi sur le CST* comprennent une explication détaillée des catégories d'activités et des exemples qui illustrent la portée des activités autorisées.

15. (NC) Conclusion n° 1 : Les demandes d'autorisation de la chef du CST fournissaient suffisamment d'information au ministre pour respecter les conditions du paragraphe 33(2) de la *Loi sur le CST*. Les nouvelles demandes comportent plus d'information que les demandes antérieures présentées au titre de la LDN et assurent une plus grande transparence des activités du CST.

Autorisation ministérielle (AM) – renseignement étranger –

16. (TS/) [REDACTED]

17. (TS/) La partie sur les activités [REDACTED] des demandes d'AM comprend de l'information sur la nécessité de l'activité. La demande indique qu'entre le 1^{er} juillet 2018 et le 31 décembre 2018, le CST n'a produit aucun rapport concernant [REDACTED]¹². Toutefois, il est indiqué plus loin que [traduction] « la valeur du programme est importante, et que, sans celui-ci, la capacité du CST de produire du renseignement étranger se verrait grandement réduite¹³ ». La demande d'AM ne permet pas de déterminer clairement la valeur de cette activité. L'équipe d'évaluation du CST examine actuellement [REDACTED]¹⁴. Par conséquent, l'OSSNR n'évaluera pas cette activité avant 2022.

¹⁰ [REDACTED]

¹¹ *Application to the Minister of National Defence for Foreign Intelligence Authorization* [REDACTED]
[Demande d'autorisation de renseignement étranger présentée au ministre de la Défense nationale pour [REDACTED]
[REDACTED] p. 1.

¹² Ibid., p. 21.

¹³ Ibid., p. 26.

¹⁴ Réponse du CST à une demande relative à un audit et à des rapports d'évaluation présentée par l'OSSNR, reçue le 3 janvier 2020.

18. (TS) Dans le cadre de l'examen des AM [REDACTED] les employés de l'OSSNR ont examiné la Liste des priorités SIGINT nationales (LPSN). La LPSN découle des exigences permanentes en matière de renseignement et de la directive ministérielle à l'intention du CST, en plus d'autres éléments, comme le démontre l'image suivante. La LPSN constitue une représentation claire, organisée par volets, des priorités du gouvernement en matière de renseignement en ce qui a trait au renseignement d'origine électromagnétique. Elle permet de concentrer les capacités du CST sur les plus importantes priorités en matière de renseignement étranger¹⁵. Le CST, en réponse à une demande d'information, a expliqué [REDACTED] pour gérer ses ressources liées à la LPSN. Le CST a ajouté [REDACTED] de la LPSN¹⁶.



19. (S) Le 21 juin 2019, le ministre de la Défense nationale a délivré une directive au CST sur les priorités en matière de renseignement du gouvernement du Canada pour 2019-2021. Quatre priorités étaient énoncées :



Autorisation ministérielle (AM) – renseignement étranger – [REDACTED]

¹⁵ Application to the Minister of National Defence for Foreign Intelligence Authorization [REDACTED]
[Demande d'autorisation de renseignement étranger présentée au ministre de la Défense nationale pour [REDACTED] p. 3.

¹⁶ Réponse du CST à la demande d'information n° 6 reçue le 23 janvier 2020.

20. (TS//) Cette AM explique que le CST mène

21. (TS) Dans l'AM sur les renseignements sous contrôle exceptionnel (RCE) ⁸ Le personnel de l'OSSNR a reçu un endoctrinement propre au programme pour examiner

22. (TS) Les activités feront l'objet d'un examen plus approfondi par l'OSSNR en 2021-2022.

Autorisation ministérielle (AM) – renseignement étranger –

23. (S) L'AM prévue par la Loi sur le CST. Ces activités du CST est chargé de mener ces activités. Les activités sont classées selon niveaux :

¹⁷ Application to the Minister of National Defence for Foreign Intelligence Authorization [Demande d'autorisation de renseignement étranger présentée au ministre de la Défense nationale] p. 1.

¹⁸ le programme sur les RCE. Les personnes doivent être intégrées dans ce programme précis pour accéder à l'information. En raison de la nature sensible aucune autre information ne sera fournie dans le présent rapport.

[REDACTED]

24. (S// [REDACTED]) Comme l'a expliqué le CST, [REDACTED] peuvent relever d'autres autorisations du renseignement étranger. Le CST a indiqué que [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED] 19 [REDACTED]

25. (S) Le tableau suivant présente le nombre [REDACTED] menées en date du 18 février 2020²¹.

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

26. (TS) L'OSSNR a demandé des évaluations juridiques des secteurs très préoccupants pour les activités relevant de l'AM [REDACTED]. Le CST a fourni un avis juridique [REDACTED]. Dans l'avis, les Services juridiques du CST ont indiqué que [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED] Selon l'avis juridique, [REDACTED]
[REDACTED]

27. (S) Il n'existe aucune restriction quant [REDACTED]

19 [REDACTED]
[REDACTED]

²⁰ Réponse du CST à la question 1 de la demande d'information n° 10, reçue le 12 février 2020.

²¹ Réponse du CST aux questions 2 et 3 de la demande d'information n° 10, reçues le 18 février 2020.

²² Services juridiques du CST, [REDACTED]
[REDACTED]

[REDACTED]

_____ dans le cadre de l'AM.

On a constaté que des activités

[illegible]

comporte aucun régime de justification de la sorte. L'OSSNR examinera cette question de manière plus approfondie dans un futur examen sur les activités

²⁵. » Le processus d'évaluation du risque

associé à la situation sera abordé dans le cadre d'un examen sur [REDACTED]
[REDACTED] mené par l'OSSNR afin de comprendre [REDACTED]
[REDACTED]

²³ Commentaires du CST sur le rapport, reçus le 22 septembre 2020.

24 CSE Foreign Intelligence Application for [REDACTED] [Demande d'autorisation de renseignement du CST pour [REDACTED] p. 5.

²⁵ Ibid., p. 23.

31. (TS) L'autorisation [REDACTED]

En plus [REDACTED]

le CST [REDACTED]

32. (S) Conclusion n° 2 : Même si ces activités n'ont pas encore eu lieu, rien ne laisse croire que le CST a pleinement évalué les ramifications, juridiques ou autres, des activités autorisées par l'AM [REDACTED]

(S) Recommandation n° 1 : Le CST doit chercher à obtenir une évaluation juridique complète des activités autorisées par l'AM [REDACTED] avant d'entreprendre des activités de collecte au titre de cette AM. L'avis juridique doit déterminer si un régime de justification implicite est créé dans l'AM [REDACTED]

Autorisations ministérielles (AM) – cybersécurité – institutions fédérales

33. (S) L'AM de cybersécurité pour les institutions fédérales ressemble le plus à son prédécesseur de la LDN en terme de portée et d'activités. L'autorisation permet au CST de défendre les réseaux et les systèmes du gouvernement, et de fournir des conseils et de l'orientation pour renforcer la posture en matière de cybersécurité. Le CST mène les activités suivantes dans le cadre de l'AM²⁷ :

- **Capteurs sur le réseau** : comprend la prestation de services de défense du réseau, principalement en déployant des capteurs sur les réseaux informatiques

²⁶ [REDACTED]

[REDACTED] MA Application [Demande d'autorisation ministérielle pour des activités impliquant le recours [REDACTED] pp. 20-1.

²⁷ Application to the Minister of National Defence For Cybersecurity Authorization Activities on Federal Infrastructures [Demande d'autorisation de cybersécurité présentée au ministre de la Défense nationale pour des activités dans l'infrastructure fédérale], pp. 4, 9.

qui permettent au CST d'accéder à tout le trafic réseau qui passe par les institutions fédérales.

- **Capteurs sur l'hôte** : modules logiciels installés sur des appareils ou de l'équipement réseau qui recueillent automatiquement de l'information se trouvant dans les appareils ou passant par ceux-ci, puis transmettent l'information recueillie au CST de façon sécuritaire.
- **Capteurs dans le nuage** : comprend l'application de solutions défensives pour les infrastructures fédérales ayant recours aux services d'infonuagique d'un tiers fournisseur de services.

34. (S) Les capteurs susmentionnés recueillent des données qui sont automatiquement utilisées dans le cadres des activités de défense dynamique du CST pour mettre fin aux cyberactivités malveillantes ou les atténuer. Les activités de défense dynamique permettent au CST d'intervenir immédiatement sur la base de l'information recueillie, protégeant ainsi l'information électronique et les infrastructures de l'information des institutions fédérales. [REDACTED]

35. (NC) L'OSSNR a l'intention d'examiner l'une des trois activités en matière de cybersécurité énumérées dans l'AM des institutions fédérales par année dans le cadre de son plan d'examen triennal sur le CST.

Autorisations ministérielles (AM) – cybersécurité – institutions non fédérales

36. (S) L'AM pour institution non fédérale est un nouvel instrument du CST, car, auparavant, le CST offrait du soutien aux propriétaires de systèmes sous leur propre autorité, et n'était pas en mesure d'utiliser leur gamme d'outil complète. Le CST doit obtenir une AM pour institution non fédérale lorsque le déploiement d'un outil ou d'un service risque d'enfreindre une loi fédérale, ou lorsqu'il existe une attente raisonnable en matière de vie privée.

37. (S) L'OSSNR a également examiné la première AM de cybersécurité ayant permis au CST de recueillir de l'information dans l'infrastructure d'une institution non fédérale. L'AM n'a pas suivi les mêmes processus et échéancier que les autres AM signées par le ministre à l'été 2019. [REDACTED] 2019, le CST a constaté qu'un acteur parrainé par l'état avait considérablement compromis une entreprise canadienne²⁸. Cette entreprise [REDACTED] une infrastructure non fédérale considérée comme étant un système d'importance pour le gouvernement du Canada, tel que défini dans l'arrêté ministériel intitulé *Arrêté ministériel désignant de l'information électronique et des infrastructures de*

²⁸ Réponse du CST à la demande d'information n° 5, reçue le 13 janvier 2020.

²⁹ *Application to the Minister of National Defence for Cybersecurity Activities on Non-Federal Infrastructure* [Demande d'autorisation de cybersécurité présentée au ministre de la Défense nationale pour des activités dans une infrastructure non fédérale], p. 2.

l'information comme étant d'importance pour le gouvernement du Canada.

38. (S) [REDACTED] a officiellement demandé l'aide du CST en [REDACTED] et le ministre a approuvé l'AM peu de temps après. Le CR a ensuite approuvé l'autorisation. La capacité de créer et d'approuver les AM de cybersécurité rapidement démontre que le CST peut intervenir et offrir du soutien rapidement pour atténuer les dommages causés aux systèmes d'importance pour le gouvernement.

39. (NC) La seule question possible cernée [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] L'OSSNR se penchera sur les relations du CST avec le secteur privé en 2022.

Autorisations ministérielles – cyberopérations actives et défensives

40. (NC) Les volets des cyberopérations actives (COA) et des cyberopérations défensives (COD) du mandat et des AM du CST accordent de nouveaux pouvoirs au CST pour qu'il prenne des mesures contre les cibles ou les cybermenaces. Le CR n'approuve pas les AM des COA et des COD. En réponse aux questions de l'OSSNR à cet égard, le CST a expliqué que les COA et les COD constituent des outils permettant de faciliter les activités autorisées, et ne servent pas à intercepter des communications privées. Puisqu'elles ne nécessitent aucune autorisation supplémentaire qui n'est pas déjà comprise dans d'autres AM, l'approbation du CR serait redondante.

41. (NC) Conformément aux paragraphes 29(2) et 30(2) de la *Loi sur le CST*, ce dernier doit consulter le ministre des Affaires étrangères et obtenir son consentement pour mener ces activités.

- Pour les COA, le ministère des Affaires étrangères doit avoir demandé l'autorisation, ou consentir à ce qu'elle soit délivrée.
- Pour les COD, le ministre des Affaires étrangères doit avoir été consulté.

42. (TS) Pendant la période d'examen, le CST a fourni des lettres de consentement du ministre des Affaires étrangères, mais ces lettres n'avaient pas de dates. Le CST n'était pas en mesure de fournir de date, puisqu'il avait reçu les lettres par voie électronique. L'OSSNR a demandé à Affaires mondiales Canada de fournir les dates des lettres, et le ministère a répondu que [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

³⁰ Réponse par courriel d'AMC datée du 3 février 2020.

43. (NC) Conclusion n° 3 : Les lettres de [REDACTED] ayant trait à la consultation du ministre de la Défense nationale avec le ministère des Affaires étrangères pour les COA et les COD n'étaient pas datées. Cette consultation précise avec Affaires mondiales Canada n'a pas été suffisamment documentée.

(NC) Recommandation n° 2 : Le CST doit s'assurer que le processus de consultation relatif aux COA et aux COD avec Affaires mondiales Canada est suffisamment documenté, le plus précisément possible, pour qu'il soit facile de vérifier si la séquence prévue par la loi est respectée.

44. [REDACTED] Il est indiqué dans la demande d'autorisation de COA que les activités doivent [traduction] « être conformes aux obligations du Canada au titre du droit international³¹ », et l'une des conditions de l'AM précise que [traduction] « les activités n'enfreindront pas les obligations du Canada en vertu du droit international³². » Toutefois, lorsqu'on lui a demandé une évaluation de ses obligations, le CST a répondu qu'il [REDACTED]

³. » En outre, le CST a répondu que [REDACTED]

⁴ ». Selon l'OSSNR, le CST n'a pas suffisamment examiné ses obligations au titre du droit international.

45. (NC) Conclusion n° 4 : Le CST n'a pas été en mesure de fournir une évaluation de ses obligations au titre du droit international pertinentes pour la réalisation de COA.

³¹ *Application to the Minister of National Defence for Active Cyber Operations Activities* [Demande d'autorisation présentée au ministre de la Défense nationale pour des activités de cyberopérations actives], p. 1.

³² *Communications Security Establishment Active Cyber Operations Authorization* [Autorisation de cyberopérations actives du Centre de la sécurité des télécommunications pour [REDACTED] paragraphe 11d).

³³ Réponse à la demande d'information n° 7, reçue le 21 février 2020.

³⁴ Commentaires du CST sur l'ébauche du rapport, reçus le 22 septembre 2020.

(NC) Recommandation n° 3 : Le CST doit obtenir une évaluation juridique officielle du régime législatif international applicable à la réalisation de COA avant d'entreprendre de telles opérations.

46. (S) Le 29 novembre 2019, l'OSSNR a reçu un exposé sur les activités liées aux COA et aux COD. L'OSSNR a compris, à partir de l'exposé, [REDACTED]. Toutefois, en réponse à une demande d'information visant à obtenir la première mise à jour après trois mois sur les COA présentée au ministre, le CST [REDACTED]³⁵. Cette réponse était différente de l'information fournie à l'OSSNR lors de l'exposé.

47. (S) En discutant avec le CST, ce dernier a expliqué que [REDACTED].
[REDACTED]
[REDACTED]
[REDACTED] Le 30 janvier 2020, l'OSSNR a envoyé une demande visant à obtenir des précisions concernant toutes les opérations, peu importe l'étape de planification où elles sont rendues, et a demandé si des rapports sur les activités liées aux COA avaient été produits. Le CST [REDACTED]³⁶. Le dernier jour de l'étape de l'examen du présent rapport, le CST a informé l'OSSNR [REDACTED].
[REDACTED]³⁷. Compte tenu de l'information fournie par le CST, l'OSSNR effectuera immédiatement un examen sur les COA et les COD dans le cadre duquel il se penchera sur le cadre stratégique de gouvernance de ces opérations.

Arrêtés ministériels

48. (NC) Comme indiqué à l'article 45 de la *Loi sur le CST*, « le ministre peut désigner, par arrêté, les personnes ou les catégories de personnes pour l'application de l'article 43 et du paragraphe 44(1) » pour la communication d'information nominative sur un Canadien ou une personne se trouvant au Canada (INCPC), si l'information a été utilisée, analysée ou conservée au titre de l'une des activités ou autorisations suivantes :

- Cybersécurité et assurance de l'information;
- Renseignement étranger;
- Situation d'urgence.

49. (NC) En outre, le ministre peut désigner comme étant importante pour le

³⁵ Réponse à la demande d'information n°3, reçue le 10 janvier 2020.

³⁶ Précisions du CST à la demande d'information n° 3, reçues le 14 février 2020.

³⁷ Courriel du CST envoyé le 21 février 2020.

gouvernement fédéral « de l'information électronique, des infrastructures de l'information ou des catégories d'information électronique ou d'infrastructures de l'information » au titre du paragraphe 21(1). Cette désignation est pertinente pour les volets suivants du mandat du CST :

- cyberopérations défensives; paragraphe 18b);
- cybersécurité et assurance de l'information; alinéa 17a)(ii).

50. (NC) L'OSSNR a conclu que les arrêtés ministériels liés à la cybersécurité et à l'assurance de l'information, paragraphes 21(1) et 44(1), étaient clairs et assuraient une transparence accrue.

51. (NC) Le document intitulé *Arrêté ministériel désignant des destinataires de renseignements canadiens d'identification acquis, utilisés et analysés en vertu d'une autorisation ministérielle de renseignement étranger*, de son côté, a soulevé des préoccupations.

52. (TS) Un dossier d'information de huit pages a été préparé pour le ministre de la Défense nationale afin qu'il approuve l'arrêté ministériel. Les sept premières pages consistaient en un aperçu, qui concernait notamment [REDACTED]

53. (S) L'arrêté ministériel se trouvait à la page 8, c'est-à-dire la dernière page de l'aperçu. L'arrêté ministériel énumérait les personnes ou les catégories de personnes désignées comme suit : [REDACTED]

54. (NC) L'OSSNR a compris que l'arrêté ministériel lié aux autorisations de renseignement étranger doit être interprété en tenant compte de l'aperçu de sept pages joint et transmis en un seul dossier.

55. (NC) Pour déterminer si de l'INCPC a seulement été communiquée à des personnes ou à des catégories de personnes figurant dans l'aperçu de l'arrêté ministériel, l'OSSNR a examiné toutes les demandes relatives à de l'information pouvant être utilisée pour identifier un Canadien, qui ont été présentées par des demandeurs étrangers (demandes de l'extérieur du Canada) et qui ont été approuvées depuis la signature de l'arrêté ministériel [REDACTED]

56. (S//CCS) [REDACTED] demandes fournies par l'équipe [REDACTED] du CST sont réparties comme suit :

[REDACTED]

57. (S) Les demandes de communication d'INCP [REDACTED]

[REDACTED]

58. (S) Lorsqu'on l'a questionné au sujet des incohérences entre le contenu de l'aperçu et l'application par le CST, ce dernier a affirmé que [REDACTED]

[REDACTED]

59. (NC) Même si le CST respecte le contenu de l'arrêté ministériel, il a fallu plusieurs réunions et échanges par écrit pour faire la distinction entre le contenu de l'aperçu (qui énumère clairement des personnes et des catégories de personnes désignées) et l'arrêté ministériel en soi [REDACTED]

[REDACTED]

60. (NC) Conclusion n° 5 : L'arrêté ministériel intitulé *Arrêté ministériel désignant des destinataires de renseignements canadiens d'identification acquis, utilisés et analysés en vertu d'une autorisation ministérielle de renseignement étranger* comprend [REDACTED]

[REDACTED]

[REDACTED]

(NC) Recommandation n° 4 : Un arrêté délivré en vertu de l'article 45 de la *Loi sur le CST* doit être le plus précis possible et détailler clairement la liste de personnes ou de catégories de personnes désignées qui peuvent recevoir de l'INCPC divulguée par le CST.

61. (NC) À la suite de discussions entre le CST et l'OSSNR, le ministre de la Défense nationale a délivré un nouvel arrêté ministériel le 25 août 2020. Il sera abordé dans le cadre d'un examen sur l'article 43 de la *Loi sur le CST* et le critère essentiel.

VI CONCLUSION

62. (NC) L'examen fondamental des AM et des arrêtés ministériels délivrés en vertu de la *Loi sur le CST* a donné à l'OSSNR un aperçu des activités opérationnelles du CST. L'examen a servi à éclairer le plan d'examen triennal sur le CST de l'OSSNR, et à cerner les questions à aborder plus en profondeur dans le cadre de ces examens.

63. (NC) Dans l'ensemble, l'OSSNR tient à souligner les séances d'information du CST sur des sujets couvrant tous les volets des mandats de renseignement étranger et de cybersécurité. L'OSSNR apprécie également la collaboration des employés de l'équipe chargée des examens externes du CST dans le cadre de l'examen.

64. (NC) En se fondant sur le présent examen, l'OSSNR se réjouit de collaborer avec le CST pour approfondir ses connaissances et sa compréhension de la mission du CST et des difficultés auxquelles il fait face.

ANNEXE A : Objectif

(NC) Le présent examen a pour objectif d'examiner l'intégralité des autorisations ministérielles et des arrêtés ministériels délivrés en vertu de la *Loi sur le CST* en 2019 afin que l'OSSNR puisse acquérir des connaissances de base sur lesquelles se fonder pour mener des examens ultérieurement. Le présent examen a joué un rôle essentiel pour éclairer le plan d'examen triennal sur le CST de l'OSSNR.

ANNEXE B : Portée et méthode

(NC) L'intégralité des autorisations ministérielles (AM) et des arrêtés ministériels délivrés par le ministre de la Défense nationale en vertu de la *Loi sur le CST* en 2019, les documents à l'appui fournis par le CST au ministre de la Défense nationale ou au ministre des Affaires étrangères, ainsi que les décisions du commissaire au renseignement ont été examinés dans le cadre du présent examen fondamental.

(NC) En outre, les AM délivrées en vertu de la *Loi sur la défense nationale* en [REDACTED] ont été examinées pour en comparer le contenu avec celui des AM délivrées en vertu de la *Loi sur le CST*.

(NC) Entre le 2 décembre 2019 et le 30 janvier 2020, les chercheurs de l'OSSNR ont présenté onze demandes d'information au CST. L'OSSNR a reçu les réponses entre le 18 décembre 2019 et le 21 février 2020. Le CST a organisé neuf exposés à l'intention de l'OSSNR. Les dates et les sujets sont énumérés à l'annexe D. En outre, on a tenu des réunions informelles avec les homologues des chercheurs de l'OSSNR au CST pour discuter de l'avancement de l'examen et pour fournir des précisions concernant les demandes relatives aux documents et à l'information.

(NC) Les chercheurs ont également examiné les politiques, les procédures et les pratiques du CST liées aux activités opérationnelles autorisées par les AM. De plus, les chercheurs ont examiné toutes les demandes approuvées de divulgation d'information nominative sur un Canadien ou une personne se trouvant au Canada (INCP) à des destinataires à l'extérieur du Canada depuis la signature de l'arrêté ministériel le [REDACTED]

ANNEXE C : Liste des autorisations ministérielles et des arrêtés ministériels

(NC) En 2019, sept autorisations ministérielles ont été délivrées en vertu de la *Loi sur le CST* :

- **(S) Cybersécurité (institutions fédérales)** : autorise les activités sur les infrastructures fédérales qui [traduction] « nécessitent d'accéder à l'information électronique et à l'infrastructure de l'information d'une institution, ainsi que d'acquérir de l'information qui provient ou passe par cette infrastructure, qui y est destinée ou y est stockée afin d'aider à la protéger³⁹. » Les activités autorisées comprennent les capteurs sur l'hôte, sur le réseau et dans le nuage. La chef du CST a signé la demande le [REDACTED] et le ministre l'a approuvée le [REDACTED]. Il convient de noter que l'un des changements causés par le passage des AM de la LDN aux AM de la *Loi sur le CST* est que plutôt que de rendre des comptes au ministre sur le nombre de communications privées, le CST rend maintenant des comptes sur le nombre de communications privées *divulguées*.
- **(S) Cybersécurité (institutions non fédérales)** : autorise les activités de cybersécurité sur [REDACTED] et l'acquisition de l'information qui provient ou passe par cette infrastructure, qui y est destinée ou y est stockée, afin d'aider à la protéger⁴⁰. Le CR a été informé de vive voix de l'AM pour institutions non fédérales le [REDACTED] puis l'AM signé a été transmis du bureau du ministre au CR le [REDACTED].
- **(TS// [REDACTED]) Cyberopérations actives** : autorise le CST à [traduction] « mener des activités en ligne afin de réduire, d'interrompre, d'influencer ou de contrecarrer les capacités, les intentions ou les activités d'une cible étrangère pouvant nuire aux intérêts du Canada liés aux affaires internationales, à la défense ou à la sécurité⁴¹. » La chef du CST a signé la demande le [REDACTED] et le ministre l'a approuvée le [REDACTED].
- **(TS// [REDACTED]) Cyberopérations défensives** : autorise le CST à [traduction] « intervenir directement face aux cybermenaces afin de mieux protéger l'information

³⁹ *Application to the Minister of National Defence for Cybersecurity Authorization Activities on Federal Infrastructures* [Demande d'autorisation de cybersécurité présentée au ministre de la Défense nationale pour des activités dans l'infrastructure fédérale], p. 1.

⁴⁰ *Application to the Minister of National Defence for Cybersecurity Authorization Activities on Non-Federal Infrastructures* [Demande d'autorisation de cybersécurité présentée au ministre de la Défense nationale pour des activités dans une infrastructure non fédérale], p. 1.

⁴¹ *Application Made By The Chief, Communications Security Establishment (CSE) To The Minister Of National Defence (MND) For An Authorization Under Subsection 30(1) Of The Communications Security Establishment Act (CSE Act)* [Demande d'autorisation du chef du Centre de la sécurité des télécommunications (CST) présentée au ministre de la Défense nationale (MinDN) au titre du paragraphe 30(1) de la *Loi sur le Centre de la sécurité des télécommunications (Loi sur le CST)*], p. 4.

et le ministre l'a approuvée le [REDACTED]

- CST a signé la demande le [REDACTED] et le ministre l'a approuvée le [REDACTED]

- et le ministre l'a approuvée le [REDACTED]

- et le ministre l'a approuvée le [REDACTED]

22 juillet 2019 :

- l'INPC recueillie dans le cadre d'une AM du renseignement étranger.

⁴³ Application to the Minister of National Defence for Foreign Intelligence Authorization p. 1.

[REDACTED] p. 1.

■ p.1.

- **(S) Arrêté ministériel désignant des destinataires de renseignements canadiens d'identification obtenus, utilisés et analysés en vertu d'une autorisation ministérielle visant les volets cybersécurité et assurance de l'information du mandat.** : Cet arrêté ministériel désigne les personnes ou les catégories de personnes qui peuvent recevoir de l'INCPD recueillie dans le cadre d'une AM de cybersécurité.
- **(S) Arrêté ministériel désignant de l'information électronique et des infrastructures de l'information comme étant d'importance pour le gouvernement du Canada** : Cet arrêté ministériel désigne l'infrastructure essentielle, l'information, les entités et les organisations considérées comme étant d'importance. Cette désignation permet au CST de fournir de l'assistance en matière de cybersécurité au titre d'AM de cyberopérations défensives et d'institution non fédérale.

ANNEXE D : Exposés

- (NC) 29 novembre 2019 : COA et COD
- (NC) 20 décembre 2019 : arrêtés ministériels
- (TS/[REDACTED]) 29 janvier 2020 : [REDACTED]
- (TS) 29 janvier 2020 : [REDACTED]
- (NC) 29 janvier 2020 : [REDACTED]
- (NC) 6 février 2020 : [REDACTED]
- (S) 7 février 2020 : exposé sur la cybersécurité (axé sur les capteurs sur le réseau, sur l'hôte et dans le nuage)
- (NC) 7 février 2020 : aperçu stratégique et législatif
- (NC) 5 août 2020 : réunion d'ordre juridique sur les personnes désignées pouvant recevoir de l'INCPC découlant du renseignement étranger au titre de l'arrêté ministériel

ANNEXE E : Conclusions et recommandations

- (NC) **Conclusion n° 1** : Les demandes d'autorisation de la chef du CST fournissaient suffisamment d'information au ministre pour respecter les conditions du paragraphe 33(2) de la *Loi sur le CST*. Les nouvelles demandes comportent plus d'information que les demandes antérieures présentées au titre de la LDN et assurent une plus grande transparence des activités du CST.
- (S) **Conclusion n° 2** : Même si ces activités n'ont pas encore eu lieu, rien ne laisse croire que le CST a pleinement évalué les ramifications, juridiques ou autres, des activités autorisées par l'AM [REDACTED]⁴⁵. [REDACTED]
[REDACTED]
[REDACTED]
- (S) **Recommandation n° 1** : Le CST doit chercher à obtenir une évaluation juridique complète des activités autorisées par l'AM [REDACTED] avant d'entreprendre des activités de collecte au titre de cette AM. L'avis juridique doit déterminer si un régime de justification implicite est créé dans l'AM [REDACTED]
- (NC) **Conclusion n° 3** : Les lettres de [REDACTED] ayant trait à la consultation du ministre de la Défense nationale avec le ministère des Affaires étrangères pour les COA et les COD n'étaient pas datées. Cette consultation précise avec Affaires mondiales Canada n'a pas été suffisamment documentée.
- (NC) **Recommandation n° 2** : Le CST doit s'assurer que le processus de consultation relatif aux COA et aux COD avec Affaires mondiales Canada est suffisamment documenté, le plus précisément possible, pour qu'il soit facile de vérifier si la séquence prévue par la loi est respectée.
- (NC) **Conclusion n° 4** : Le CST n'a pas été en mesure de fournir une évaluation de ses obligations au titre du droit international pertinentes pour la réalisation de COA.
- (NC) **Recommandation n° 3** : Le CST doit obtenir une évaluation juridique officielle du régime législatif international applicable à la réalisation de COA avant d'entreprendre de telles opérations.
- (NC) **Conclusion n° 5** : L'arrêté ministériel intitulé *Arrêté ministériel désignant des destinataires de renseignements canadiens d'identification acquis, utilisés et analysés en vertu d'une autorisation ministérielle de renseignement étranger* comprend [REDACTED]
[REDACTED]
[REDACTED]

⁴⁵ Depuis, l'autorisation a été renommée [REDACTED]

- (NC) **Recommandation n° 4** : Un arrêté délivré en vertu de l'article 45 de la *Loi sur le CST* doit être le plus précis possible et détailler clairement la liste de personnes ou de catégories de personnes désignées qui peuvent recevoir de l'INPCPC divulguée par le CST.

ANNEXE F : LOI SUR LE CST : AIDE-MÉMOIRE

NON CLASSIFIÉ

LA LOI SUR LE CST

	RENSEIGNEMENT ÉTRANGER 16	CYBERSÉCURITÉ ET ASSURANCE DE L'INFORMATION 17	CYBEROPÉRATIONS DÉFENSIVES (COD) 18	CYBEROPÉRATIONS ACTIVES (COA) 19	ASSISTANCE TECHNIQUE ET OPÉRATIONNELLE 20
MANDAT	LES ACTIVITÉS NE DOIVENT VISER NI LES CANADIENS NI LES PERSONNES SE TROUVANT AU CANADA ET NE DOIVENT PAS ALLER À L'ENCONTRE DE LA CHARTRE CANADIENNE DES DROITS ET LIBERTÉS.				Le CST PEUT FAIRE L'OBJET DE DEMANDES de la part d'organismes légitimes chargés de l'application de la loi et de la sécurité, des Forces armées canadiennes (FAC) et du ministre de la Défense nationale (MDN).
CONDITIONS	ACTIVITÉS EXIGEANT UNE AUTORISATION MINISTÉRIELLE (AM)				
	Les AM protègent le CST lorsque ses activités contreviennent à d'autres lois du Parlement ("ou de tout autre État étranger en ce qui concerne le renseignement étranger, les COD et les COA seulement"); ou lorsque ses activités portent atteinte à une attente raisonnable de protection en matière de la vie privée d'un Canadien ou d'une personne au Canada.				
	- Les activités doivent être raisonnables, nécessaires et proportionnées. - L'information non sélectionnée ne pourrait raisonnablement pas être acquise autrement. - Des mesures sont en place pour protéger la vie privée des Canadiens ou des personnes se trouvant au Canada.	- Les activités doivent être raisonnables, nécessaires et proportionnées. - Des mesures sont en place pour protéger la vie privée des Canadiens ou des personnes se trouvant au Canada.	- Les activités doivent être raisonnables et proportionnées. - L'objectif d'une COA ou d'une COD ne peut raisonnablement pas être atteint autrement. - Toute information dont se sert le CST pour planifier ou mener une COD ou une COA doit être acquise en vertu d'une AM de renseignement étranger ou de cybersécurité.		
	IL EST STRICTEMENT INTERDIT POUR LE CST DE FAIRE CE QUI SUIT : - causer, volontairement ou par négligence criminelle, des lésions corporelles à un individu ou la mort de celui-ci; - entraver le cours de la justice ou de la démocratie.				
	L'information jugée comme se rapportant à un Canadien ou à une personne se trouvant au Canada sera utilisée, analysée ou conservée uniquement si elle est essentielle...	Désignation : Le MDN peut désigner comme étant importante pour le GC de l'information électronique, des infrastructures de l'information ou des catégories d'information électronique ou d'infrastructures de l'information.			
	... à la défense, à la sécurité ou aux affaires internationales	... pour repérer, isoler, prévenir ou atténuer les activités dommageables visant les systèmes d'importance			
	MESURES POUR PROTÉGER LA VIE PRIVÉE				
	- Politiques, formation, conservation, suppression, approbations de la gestion, LCA, vérifications, examens, DSJ, D2 - Une information nominative sur un Canadien peut seulement être divulguée à des personnes ou à des catégories de personnes définies, si la divulgation est essentielle à la défense, à la sécurité, à la cybersécurité ou aux affaires internationales. - Une information relative à des Canadiens ou à des personnes se trouvant au Canada peut être divulguée aux personnes ou aux catégories de personnes définies, si la divulgation est nécessaire à la protection des systèmes d'importance.				
	Utilisation d'information accessible publiquement qui a été publiée ou diffusée à l'intention du grand public, qui est accessible au public dans l'IMI ou ailleurs, ou qui est accessible au public sur demande, par abonnement ou achat (ne comprend pas l'information pour laquelle un Canadien ou une personne se trouvant au Canada a une attente raisonnable en matière de protection de la vie privée) Mise à l'essai ou évaluation de produits, de logiciels et de systèmes afin de trouver des vulnérabilités - Analyse de l'information et prestation de conseils concernant les investissements étrangers au Canada à l'intention des ministres de SP et d'ISDE aux termes de la Loi sur l'investissement Canada - Acquisition, utilisation, analyse, conservation ou divulgation d'information sur l'infrastructure à des fins de recherche et de développement ou de mise à l'essai de systèmes ou de conduite d'activités de cybersécurité et d'assurance de l'information au sein de l'infrastructure à partir de laquelle celle-ci a été acquise - Aux fins de CYBERSÉCURITÉ ET D'ASSURANCE DE L'INFORMATION uniquement : Mener des activités au sein des infrastructures de l'information pour repérer, isoler, prévenir ou atténuer les activités ou les conséquences des maliciels sur l'infrastructure - Aux fins de CYBERSÉCURITÉ ET D'ASSURANCE DE L'INFORMATION uniquement : Mener des activités de recherche et de développement pour offrir des avis et des conseils sur l'intégrité des chaînes d'approvisionnement et sur la fiabilité de l'équipement, des services et des communications électroniques				
	APPROBATION PAR LE MINISTRE DE LA DÉFENSE NATIONALE				
Le MDN doit avoir des motifs raisonnables de croire que les conditions énoncées dans la loi sont respectées, notamment que les activités de renseignement étranger et de cybersécurité sont raisonnables, nécessaires et proportionnées et que les activités relatives aux COD et aux COA sont raisonnables et proportionnées.					
EXCEPTIONS	... approbation donnée si le ministre des Affaires étrangères est consulté ... approbation donnée si le ministre des Affaires étrangères en fait la demande ou donne son consentement				
	APPROBATION PAR LE COMMISSAIRE AU RENSEIGNEMENT (CR)				
APPROBATIONS	- Le CR doit être convaincu que les conclusions ministérielles sont raisonnables. - Le CR approuve les AM du CST avant que le CST mène des opérations en vertu de celles-ci.				
	OFFICE DE SURVEILLANCE DES ACTIVITÉS EN MATIÈRE DE SÉCURITÉ NATIONALE (OSSNR)				
SURVEILLANCE	- Examiner toutes les activités du CST ainsi que toutes les activités relatives à la sécurité nationale qui sont menées à l'échelle du GC; - Examiner les activités du CST pour veiller à leur conformité aux lois et aux directives ministérielles, de même que le caractère raisonnable et la nécessité que le CST exerce ses pouvoirs; - Enquêter sur les plaintes contre le CST.				
	COMITÉ DES PARLEMENTAIRES SUR LA SÉCURITÉ NATIONALE ET LE RENSEIGNEMENT (CPSNR)				
EXAMEN	Examiner les activités du CST qui concernent le renseignement ou la sécurité nationale, y compris les mesures mises en place par l'organisme pour protéger la vie privée des Canadiens ou des personnes se trouvant au Canada.				



Centre de la sécurité des télécommunications

Communications Security Establishment

Canada