Objet : Examen par le Comité sénatorial permanent de la sécurité nationale de la défense et des anciens combattants du projet de loi C-26, *Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois*

CIRA, the Canadian Internet Registration Authority

Sommaire

1. CIRA, l'Autorité canadienne pour les enregistrements Internet est heureuse de participer à l'étude par le Comité sénatorial permanent de la sécurité nationale de la défense et des anciens combattants du projet de loi C-26, la *Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois* (ci-après le « projet de loi C-26 »).

2. CIRA appuie fermement l'objectif du gouvernement du Canada de rehausser le niveau de base de la cybersécurité dans les cybersystèmes essentiels au moyen du projet de loi C-26. CIRA propose deux recommandations constructives à la partie 2 du projet de loi C-26 (la *Loi sur la protection des cybersystèmes essentiels*, ci-après la « LPCE ») afin de mieux aligner ses objectifs de cybersécurité avec les considérations relatives à la surveillance et au partage de l'information.

   Recommandation 1 : Afin d'améliorer la surveillance, la LPCE devrait exiger que les directives de cybersécurité proposées soient examinées par le·la greffier·ère du Conseil privé, en consultation avec le·la sous-ministre de la Justice.

   Recommandation 2 : Afin d'accroître la confiance dans le partage de renseignements proposé par la LPCE, les conditions relatives à l'utilisation des renseignements devraient être renforcées.

3. Les recommandations de CIRA reflète sa position unique en tant que [1]registre[2] de domaine de premier niveau de code de pays du Canada et en tant que fournisseur de cybersécurité. CIRA reconnaît que la LPCE donne au·à la gouverneur·e en conseil (GC) le pouvoir d'ajouter à l'annexe 1 « les services critiques et les systèmes critiques » qui ne sont pas actuellement énumérés dans le projet de loi.

[1] Un domaine de premier niveau est l'un des domaines du niveau le plus élevé du système hiérarchique de noms de domaine d'Internet (par exemple, .COM, .ORG, .CA). Un domaine de premier niveau de code de pays est un domaine de premier niveau qui indique le pays ou l'emplacement géographique du domaine.
[2] Un registre est la base de données de tous les noms de domaine enregistrés sous un certain domaine de premier niveau.

4. En tant que telles, les recommandations de CIRA apporteraient plus de clarté et de confiance aux « organismes réglementaires compétents » et aux « exploitants désignés » tels qu'ils sont actuellement définis dans le projet de loi, ainsi qu'à toute personne ou entité qui sera éventuellement incluse dans le champ d'application du cadre d'appui.

À propos de CIRA

5. CIRA est un organisme à but non lucratif, surtout connu pour l'exploitation du registre .CA, qui gère plus de 3,3 millions de domaines. La mission de CIRA est de bâtir un Internet fiable pour les Canadien·nes. Selon le NetBeacon Institute, .CA est l'un des domaines de premier niveau de code de pays les plus sûrs au monde.[3]

6. Le mandat premier de CIRA concerne l'exploitation sûre, stable et sécuritaire du domaine .CA et des technologies sous-jacentes. Nous relions, protégeons et impliquons également la communauté Internet au Canada et ailleurs en offrant des services de registre, de DNS et de cybersécurité de qualité supérieure.

7. Le personnel de CIRA participe activement à des forums multilatéraux pour promouvoir la sécurité et la résilience d'Internet. Au niveau national, il s'agit du Forum canadien pour la résilience des infrastructures numériques (FCRIN)[4] et du Comité directeur sur l'interconnexion du CRTC (CDIC) du Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC)[5] et, au niveau international, du comité consultatif sur la sécurité et la stabilité (SSAC) de l'Internet Corporation for Assigned Names and Numbers (ICANN)[6].

8. CIRA fournit également des services de cybersécurité pour assurer la sécurité des Canadien·nes en ligne. Ces services sont les suivants :

[3] NetBeacon, « Rapport MAP : Août 2024 », *NetBeacon,* consulté le 10 octobre 2024, https://netbeacon.org/wp-content/uploads/2024/08/MAP-Report-August-2024-.pdf.
[4] Canada, « Forum canadien pour la résilience des infrastructures numériques », consulté le 30 octobre 2024, https://ised-isde.canada.ca/site/gestion-spectre-telecommunications/fr/savoir-plus/comites-intervenants/conseils-comites/forum-canadien-pour-resilience-infrastructures-numeriques-fcrin
[5] CRTC, « Comité directeur sur l'interconnexion du CRTC (CDCI) », consulté le 30 octobre 2024, https://crtc.gc.ca/fra/cdci-cisc.htm
[6] ICANN, « Security and Stability Advisory Committee », consulté le 30 octobre 2024, https://icann.org/group/ssac/

a. *CIRA DNS Firewall* : protection DNS de niveau entreprise pour les entreprises, les municipalités, les établissements pédagogiques, les établissements de santé et autres organisations, qui protège des millions de Canadien·nes contre les maliciels, les rançongiciels et d'autres menaces de sécurité.

b. *CIRA Anycast DNS* : infrastructure de routage qui rapproche le contenu mondial des utilisateur·rices finaux·ales et assure leur sécurité en minimisant les effets des menaces de sécurité.

c. *Bouclier canadien de CIRA* : services de cybersécurité gratuits qui protègent des millions de Canadien·nes contre les menaces en ligne.

d. *Formation en cybersécurité de CIRA* : plateforme de formation et de simulation d'hameçonnage intégrée qui permet aux organisations de sensibiliser leur personnel sur la manière de se protéger contre les cyberrisques comme le piratage psychologique et les rançongiciels.

9. CIRA s'associe à plusieurs organismes pour assurer la mise à jour de ces services et la sécurité des Canadien·nes en ligne, notamment le Centre canadien pour la cybersécurité, le Centre canadien de protection de l'enfance, l'Internet Watch Foundation et Mozilla Firefox.

Introduction

10. CIRA appuie fermement l'objectif du gouvernement du Canada de rehausser le niveau de base de la cybersécurité dans les cybersystèmes essentiels au moyen du projet de loi C-26. Un Internet fiable sous-tend la capacité des Canadien·nes à participer et à contribuer au bien-être économique, social et politique du pays. CIRA soutient les initiatives du gouvernement du Canada visant à mettre en place des mesures et des cadres de cybersécurité qui permettent à tou·tes les Canadien·nes de mieux protéger leurs données, leurs appareils et leurs réseaux.

11. En tant que registre de domaines de premier niveau et fournisseur de services de cybersécurité, les données de CIRA montrent un volume grandissant de cybermenaces de plus en plus virulentes. En 2024, pour le compte de CIRA, le Strategic Counsel a interrogé plus de 500 décideur·euses en matière de cybersécurité au sein d'organisations

canadiennes. Le sondage a montré que 44 % des organisations canadiennes ont subi une cyberattaque (tentative ou réussite) au cours de l'année précédente.[7]

12. CIRA préconise depuis longtemps l'importance de mesures et de cadres de cybersécurité robustes de la part des gouvernements et des entreprises.

13. Plus récemment, le président-directeur général de CIRA, Byron Holland, a comparu devant le Comité permanent de la Chambre des communes sur la sécurité publique et nationale (SECU). Notamment, CIRA et d'autres témoins ont plaidé en faveur de dispositions de transparence améliorées, qui ont été adoptées par les parlementaires et qui sont maintenant reflétées dans la législation.

14. En tant que telles, les recommandations actuelles de CIRA concernant la LPCE apporteraient plus de clarté et de confiance aux « organismes réglementaires compétents » et aux « exploitants désignés » tels qu'ils sont actuellement définis dans le projet de loi, ainsi qu'à toute personne ou entité qui sera éventuellement incluse dans le champ d'application de son cadre d'appui.

Recommandation 1 : Afin d'améliorer la surveillance, la LPCE devrait exiger que les directives de cybersécurité proposées soient examinées par le·la greffier·ère du Conseil privé, en consultation avec le·la sous-ministre de la Justice.

15. Des changements notables ont été apportés au projet de loi C-26 afin d'améliorer la surveillance. Les modifications décrivant les considérations nécessaires que le·la gouverneur·e en conseil (GC) doit prendre en considération avant d'émettre une ordonnance de mise en conformité, permettent de mieux contrôler la manière dont les directives obligatoires sont émises et mises en œuvre.[8]

---

[7] CIRA, « Sondage 2024 de CIRA sur la cybersécurité », consulté le 30 octobre 2024, https://www.cira.ca/fr/ressources/documents/cybersecurite/sondage-2024-cira-cybersecurite/

[8] Ces changements sont décrits plus en détail dans la première et la troisième lecture *du projet de loi C-26, Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois*, 44e Parlement, 2023, partie 2, paragr. 20 à 25.

16. Bien que des mesures aient été prises pour que la législation proposée prévoie davantage de contrôle, dans sa version actuelle, les instructions en matière de cybersécurité données en vertu de l'article 20 ne seraient toujours pas soumises aux articles 3, 5 et 11 de la *Loi sur les textes réglementaires* (article 22(1)).

17. La *Loi sur les textes réglementaires* définit les principaux aspects du processus d'élaboration des règlements. L'article 3 de la *Loi sur les textes réglementaires* décrit le processus par lequel le·la greffier·ère du Conseil privé, en consultation avec le·la sous-ministre de la Justice, examine le projet de règlement pour s'assurer, entre autres, qu'il est « pris dans le cadre du pouvoir conféré par sa loi habilitante » (article 3(2)(a)).

18. Le système de freins et de contrepoids prévu par la *Loi sur les textes réglementaires* assure la surveillance, la responsabilité et la transparence du processus d'élaboration des règlements. L'article 3 permet de vérifier qu'un règlement proposé ne constitue pas un « usage inhabituel ou inattendu du pouvoir » ((2)(b)) et qu'il « n'empiète pas indûment sur les droits et libertés existants » ((2)(c)). En exemptant ces vérifications, la Loi limite la surveillance, la responsabilité et la transparence dans le processus d'élaboration de la réglementation.

19. En tant que fournisseur de cybersécurité, CIRA reconnaît le besoin de discrétion et de rapidité lorsqu'il s'agit de questions de sécurité nationale et de sécurité publique, y compris dans le cadre des directives de cybersécurité. Cependant, pour renforcer la confiance du public dans le cadre éventuel, l'exemption des directives de cybersécurité de l'article 3 de la Loi sur les textes réglementaires devrait être retirée. Le libellé précis de cette modification proposée se trouve ci-dessous.

Libellé actuel de l'article 22 (1) de la LPCE

22 (1) Est soustrait à l'application des articles 3, 5 et 11 de la Loi sur les textes réglementaires le décret pris en vertu de l'article 20.

Modification proposée à l'article 22 (1) de la LPCE

22 (1) Est soustrait à l'application des articles 5 et 11 de la Loi sur les textes réglementaires le décret pris en vertu de l'article 20.

Recommandation 2 : Afin d'accroître la confiance dans le partage de renseignements proposé par la LPCE, les conditions relatives à l'utilisation des renseignements devraient être renforcées.

20. Plusieurs dispositions de la LPCE permettent l'échange de renseignements entre une série de personnes et d'entités, sans définir explicitement les limites de cet échange de renseignements.

21. Par exemple, l'article 16 autorise les organismes réglementaires compétents qui demandent au Centre de la sécurité des télécommunications (CST) des avis, des conseils ou des services dans certains contextes à fournir au CST certains renseignements, y compris des renseignements confidentiels.

22. L'article 23 confère des pouvoirs étendus pour le partage de renseignements divulgués en vertu d'une directive sur la cybersécurité.

23. Ces renseignements pourraient être partagés avec plusieurs personnes ou entités, notamment le·la chef ou un·e employé·e du CST, le·la directeur·rice ou un·e employé·e du Service canadien du renseignement de sécurité (SCRS), et « toute autre personne ou entité prévue par règlement ».

24. Bien qu'il puisse y avoir des indications de l'intention du législateur, la LPCE ne limite pas explicitement l'utilisation des informations par les destinataires.

25. Par exemple, la Loi sur le CST articule le mandat en cinq parties de l'organisme, qui, en plus de la cybersécurité et de l'assurance de l'information, comprend le renseignement étranger, les cyberopérations défensives, les cyberopérations actives et l'assistance technique et opérationnelle.

26. CIRA estime que les mécanismes de protection supplémentaires décrits ci-dessous permettraient d'atténuer les craintes que le CST puisse utiliser les données recueillies en vertu de l'article 16 de la LPCE pour poursuivre des aspects de son mandat autres que la cybersécurité et l'assurance de l'information.

Modification i)
Modification proposée à l'article 16 de la LPCE soulignée :

(16) L'organisme réglementaire compétent peut fournir au Centre de la sécurité des télécommunications tous renseignements, y compris confidentiels, concernant le programme de cybersécurité d'un exploitant désigné ou toute mesure prise en application de l'article 15 afin que le Centre lui prodigue des avis, des conseils et des services conformément aux aspects liés à la cybersécurité et à l'assurance de l'information de son mandat tel que défini à l'article 17 de la Loi sur le CST concernant l'exercice des attributions qui lui sont conférées sous le régime de la présente loi.

Modification ii)
Ajout proposé à l'article 23 de la LPCE :

(23.1) Tous les renseignements partagés conformément à l'article 23 ne peuvent être utilisés par la personne destinataire qu'aux fins énoncées à l'article 5.

Conclusion

27. CIRA remercie le Comité sénatorial permanent de la sécurité nationale de la défense et des anciens combattants de lui avoir donné l'occasion de participer à son étude du projet de loi C-26.

28. Réitérons que CIRA propose deux recommandations constructives à la partie 2 du projet de loi C-26 (la « LPCE ») afin de faire en sorte que ses objectifs en matière de cybersécurité cadrent mieux avec les considérations relatives à la surveillance et au partage de l'information.

    Recommandation 1 : Afin d'améliorer la surveillance, la LPCE devrait exiger que les directives de cybersécurité proposées soient examinées par le·la greffier·ère du Conseil privé, en consultation avec le·la sous-ministre de la Justice.

    Recommandation 2 : Afin d'accroître la confiance dans le partage de renseignements proposé par la LPCE, les conditions relatives à l'utilisation des renseignements devraient être renforcées.

29. Des informations supplémentaires ou des citations sont disponibles sur demande.