Objet : Examen du projet de loi C-26 par le Comité permanent de la sécurité publique et nationale de la Chambre des communes

Autorité canadienne pour les enregistrements Internet

Sommaire

1. L'Autorité canadienne pour les enregistrements Internet (CIRA) est heureuse de participer à l'étude par le Comité permanent de la sécurité publique et nationale de la Chambre des communes 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 trois 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 faire en sorte que ses objectifs en matière de cybersécurité cadrent mieux avec les considérations relatives à la surveillance, au partage de l'information et à la transparence.

   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.

   Recommandation 3 : Afin de promouvoir la transparence, la LPCE devrait être modifiée de manière à ce que les renseignements sur les directives de cybersécurité données au cours de l'année précédente soient rendus publics.

3. Les recommandations de CIRA reflète sa position unique en tant que registre de domaine de premier niveau de code de pays[1][2] 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.

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

[1]Un domaine de premier niveau est l'un des domaines du niveau le plus élevé du système hiérarchique des 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.

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 Canadiens. Selon DNS Abuse Institute, le domaine .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 (CDCI) 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·ne·s en ligne. Entre autres :

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

[3] DNS Abuse Institute, « A new phase of measuring DNS abuse », *DNS Abuse Institute*, consulté le 19 juin 2023, https://dnsabuseinstitute.org/wp-content/uploads/2023/06/V3-FINAL-DNSAI-Compass-Report-Combined.pdf
[4] Canada, « Forum canadien pour la résilience des infrastructures numériques », consulté le 19 juin 2023, 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 19 juin 2023, https://crtc.gc.ca/fra/cdci-cisc.htm
[6] ICANN, « Security and Stability Advisory Committee », consulté le 19 juin 2023, https://www.icann.org/groups/ssac

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

c) *Bouclier canadien de CIRA* : service gratuit de cybersécurité qui protège millions de Canadien·ne·s 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 l'ingénierie sociale et les rançongiciels.

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

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·ne·s 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·te·s les Canadien·ne·s 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 2022, pour le compte de CIRA, The Strategic Council a interrogé plus de 500 décideur·euse·s en matière de technologies de l'information et de cybersécurité au sein d'organisations canadiennes. Le sondage a révélé que 29 % d'organisations interrogées ayant subi une brèche de sécurité en 2022.[7]

12. CIRA préconise depuis longtemps l'importance de mesures et de cadres de cybersécurité robustes de la part des gouvernements et des entreprises. Lors de la récente consultation de Sécurité publique Canada sur la Stratégie nationale de cybersécurité, nous avons recommandé

[7] The Strategic Council, « Perceptions and attitudes of Canadian organizations toward cybersecurity », consulté le 19 juinl 2023, https://static.cira.ca/2022-10/CIRA%202022%20Cybersecurity%20Report%20Aug%2031.pdf?VersionId=HP489japmgg3q8vDhTmwNEm2UaU8EGWs

que le gouvernement fournisse des renseignements sur les menaces aux fournisseurs de services de cybersécurité fiables, qu'il continue à financer l'adoption de technologies de cybersécurité pour les organisations de tous types et qu'il s'efforce de sensibiliser les Canadien·ne·s aux cyberrisques.[8]

13. En tant que telles, les recommandations de CIRA à 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.

14. Dans la version actuelle de la LPCE, les directives de cybersécurité données en vertu de son article 20 seraient exemptées des articles 3, 5 et 11 de la *Loi sur les textes réglementaires*.

15. 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)).

16. 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)).

17. CIRA reconnaît le besoin de secret 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.

[8] CIRA, « Protéger les Canadiens : renouveler l'approche nationale en matière de cybersécurité », consulté le 19 juin 2023, https://www.cira.ca/fr/blogue/letat-de-linternet/proteger-les-canadiens-renouveler-lapproche-nationale-en-matiere-de

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.

18. Plusieurs dispositions de la LPCE permettent l'échange de renseignements entre une série de personnes et d'entités. 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.

19. En outre, l'article 23 de la LPCE confère de vastes pouvoirs pour le partage des renseignements fournis conformément à une directive de cybersécurité donnée vertu de l'article 20. 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 ».

20. Bien qu'il puisse y avoir des indications de l'intention du législateur, le projet de loi C-26 ne limite pas explicitement la façon dont les destinataires utilisent les renseignements recueillis en vertu de ces articles.

21. 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. CIRA estime qu'il ne serait pas approprié que le CST utilise les données recueillies en vertu de l'article 16 de la LPCE pour mener à bien des aspects de son mandat autres que ceux liés à la cybersécurité et à 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.

Recommandation 3 : Afin de promouvoir la transparence, la LPCE devrait être modifiée de manière à ce que les renseignements sur les directives de cybersécurité données au cours de l'année précédente soient rendus publics.

22. Les décrets pris en vertu de l'article 20 de la LPCE sont soustraits à l'application des articles 3, 5 et 11 de la *Loi sur les textes réglementaires.* L'exemption de l'article 11 de la *Loi sur les textes réglementaires* prévue par l'article 20 exclut la publication des directives de cybersécurité dans la *Gazette du Canada*.

23. Comme mentionné précédemment, CIRA reconnaît la nécessité d'un certain niveau de secret et de rapidité lorsqu'il s'agit de questions de sécurité nationale et de sécurité publique. Cependant, le secret devrait être contrebalancé par l'ajout de dispositions dans le projet de loi C-26 qui favoriseraient une certaine transparence concernant les directives de cybersécurité données.

24. Si le projet de loi C-26 était adopté, cette transparence renforcerait la confiance accordée par le public à la *Loi* et permettrait aux organismes réglementaires compétents et aux exploitants désignés de mieux comprendre la mise en œuvre de la *Loi* au fil du temps.

25. la LPCE devrait être modifiée de manière à ce que le nombre de directives de cybersécurité données au cours de l'année précédente, ainsi que d'autres renseignements connexes, soit rendu public. Le libellé précis de cette modification proposée se trouve ci-dessous.

Modification proposée à l'article 146 de la LPCE souligné :

146 Dans les trois mois suivant la fin de chaque exercice, le ministre prépare un rapport visant l'application de la présente loi pour cet exercice et en fait déposer une copie devant chaque chambre du Parlement dans les quinze jours de séance suivant l'achèvement du rapport.

Ce rapport indiquera ce qui suit :

(a) le nombre de directives de cybersécurité données au cours de l'année précédente;
(b) le nombre de directives de cybersécurité révoquées au cours de l'année précédente;
(c) le nombre d'exploitants désignés qui ont reçu une directive de cybersécurité au cours de l'année précédente;
(d) les services critiques et systèmes critiques des exploitants désignés qui ont reçu une directive de cybersécurité au cours de l'année précédente.

Conclusion

26. CIRA remercie le Comité permanent de la sécurité publique et nationale de la Chambre des communes de lui avoir donné l'occasion de participer à son étude du projet de loi C-26.

27. Réitérons que CIRA propose trois 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, au partage de l'information et à la transparence.

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.

Recommandation 3 : Afin de promouvoir la transparence, la LPCE devrait être modifiée de manière à ce que les renseignements sur les directives de cybersécurité données au cours de l'année précédente soient rendus publics.

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

29. CIRA demande respectueusement à comparaître devant le Comité permanent de la sécurité publique et nationale de la Chambre des communes dans le cadre de son étude du projet de loi C-26.