
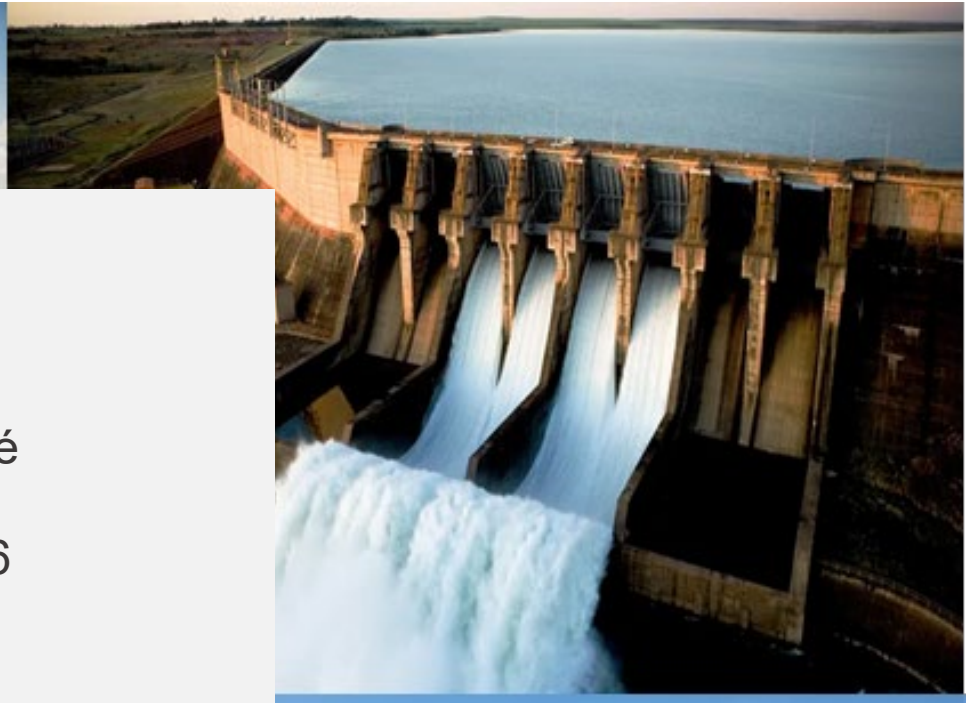

Comité sénatorial permanent de la sécurité publique et nationale
Objet : projet de loi C-26

Novembre 2024

National Centre for Critical Infrastructure Protection, Security and Resilience

NC-CIPSeR

Note d'information : Renforcer la cybersécurité des infrastructures essentielles du Canada

À : Comité sénatorial permanent de la sécurité publique et nationale

De : National Centre for Critical Infrastructure Protection, Security, and Resilience (NC-CIPSeR)

Date : Le 11 novembre 2024

Le National Centre for Critical Infrastructure Protection, Security, and Resilience (NC-CIPSeR) est grandement préoccupé par la hausse croissante des cyberattaques ciblant les infrastructures essentielles (IE). Le Canada doit voir ces intrusions pour ce qu'elles sont : des menaces pour la sécurité nationale.

Le NC-CIPSeR appuie les modifications proposées à la *Loi sur les télécommunications* ainsi que l'édiction de la *Loi sur la protection des cybersystèmes essentiels* (LPCE), proposée dans le projet de loi C-26. Notamment, l'instauration d'un mécanisme national de déclaration pour faire le suivi des cyberattaques, prévu dans la partie 2, permettrait l'obtention de précieux renseignements pour assurer la sécurité des quatre secteurs essentiels.

Le présent mémoire comprend des recommandations liées à la mise en œuvre du projet de loi C-26 et décrit les prochaines étapes importantes pour renforcer la résilience du Canada en matière de cybersécurité. Reconnaissant qu'il est urgent d'agir sur cette question, le NC-CIPSeR demande au Sénat d'adopter le projet de loi C-26 dans sa forme actuelle.

Le National Centre for Critical Infrastructure Protection, Security, and Resilience (NC-CIPSeR)

Le NC-CIPSeR est une organisation fédérale canadienne sans but lucratif, qui a comme mission de renforcer la protection, la sécurité et la résilience des IE partout au pays. Notre mandat est de faire de la recherche menant à des actions concrètes, de fournir des conseils d'experts et de faire de la sensibilisation, tout en favorisant la collaboration stratégique avec le gouvernement, l'industrie et le milieu universitaire pour renforcer la sécurité et la résilience des IE du Canada. Nous nous concentrons sur les dangers et les menaces en constante évolution tels que les cyberattaques, les changements climatiques et les perturbations physiques.

Renforcer les infrastructures essentielles du Canada : le rôle du projet de loi C-26 et l'urgence de l'adopter

Le NC-CIPSeR voit le projet de loi C-26 comme l'évolution naturelle des efforts du Canada pour renforcer les IE du pays. En raison de l'interdépendance des quatre secteurs (transports, télécommunications, finances et énergie), les perturbations — qu'elles soient attribuables à des catastrophes naturelles, à des perturbations physiques ou à des cyberincidents — peuvent entraîner de vastes effets en cascade, ce qui met en évidence la nécessité d'assurer une protection et une coordination de toute urgence.

L'engagement du Canada à l'égard de la protection des IE a été énoncé pour la première fois dans le cadre de la Stratégie nationale sur les infrastructures essentielles et du Plan d'action 2021-2023 sur les infrastructures essentielles du Forum national intersectoriel. Les deux font la promotion d'une approche axée sur la collaboration entre les partenaires fédéraux, provinciaux et

du secteur privé. Ces deux cadres priorisent la résilience, l'évaluation des risques et la coordination des interventions.

L'évaluation des cybermenaces nationales 2025-2026 fait état de l'environnement des cybermenaces qui s'intensifient, soulignant en particulier l'augmentation de la prévalence de la cybercriminalité comme service (CaaS) et les risques posés par des acteurs commandités par des États comme la Chine et la Russie. Selon l'évaluation 2025-2026, les rançongiciels et les outils perfectionnés de piratage continuent de cibler les IE du Canada, ce qui montre la nécessité d'adopter les politiques proactives et adaptées en matière de cybersécurité contenues dans le projet de loi C-26.

De plus, l'examen des pratiques du Canada en matière de cybersécurité des IE, mené en 2021 par le Bureau de la vérificatrice générale, a fait ressortir plusieurs lacunes liées à la coordination, aux interventions en cas d'incidents ainsi qu'aux mesures de résilience à l'échelle fédérale. Dans son rapport d'étape de mi-parcours 2024, Sécurité publique Canada réitère cette affirmation et place le projet de loi C-26 en tant que partie intégrante du cadre élargi de la stratégie de résilience des IE du Canada.

Recommandations concernant le projet de loi C-26

Le NC-CIPSeR appuie l'objectif du projet de loi C-26, qui est de protéger les IE du Canada des cybermenaces, et formule les recommandations ci-dessous pour renforcer la mesure législative au moyen de stratégies de mise en œuvre.

1. Intégrer les nouvelles technologies

Intégrer des mécanismes pour suivre l'évolution des exigences de conformité, faisant fond sur des modèles comme les « Objectifs de rendement intersectoriel des États-Unis en matière de cybersécurité » (U.S. Cross-Sector Cybersecurity Performance Goals) ainsi que l'approche de la menace de référence de la Commission canadienne de sûreté nucléaire (Lignes directrices de l'Agence internationale de l'énergie atomique). Grâce à de tels mécanismes, la mesure législative resterait adaptée aux technologies en évolution rapide comme l'intelligence artificielle (IA), le calcul informatique de pointe (CIP) et la cryptographie à résistance quantique.

2. Adopter l'architecture à vérification systématique

Imposer l'adoption de profils communs d'architecture à vérification systématique dans les quatre secteurs des IE afin de renforcer les défenses en matière de cybersécurité contre les menaces complexes et en constante évolution. Une telle directive, arrimée aux discussions et à certains engagements du Groupe des cinq, contribuerait à protéger les IE contre les menaces complexes et en constante évolution.

3. Diffuser de l'information sur la conformité

Prioriser le perfectionnement professionnel continu des professionnels de première ligne des IE, y compris les exploitants, les gestionnaires de TI et des risques ainsi que les groupes d'approvisionnement (chaîne d'approvisionnement) afin de favoriser la conformité. L'offre de ressources et de formation et la diffusion de pratiques exemplaires découlant de la recherche fondée sur les données probantes favoriseraient une culture orientée sur la sécurité et réduiraient la dépendance aux mesures punitives, ce qui rendrait la conformité plus accessible, plus collaborative et plus efficace.

4. Financer les mesures de risque du Canada

Investir dans la recherche spécialisée sur la cybersécurité, les politiques, la continuité des activités, l'évaluation des risques et les interdépendances des IE. Poursuivre les recherches liées aux mesures de rendement, comme les temps d'intervention et les taux de réduction des

incidents, afin de mesurer l'efficacité du projet de loi C-26 et le respect des règlements au fil du temps-. Le suivi de ces mesures permettrait d'apporter des modifications judicieuses, fondées sur les données probantes, au cadre de réglementation à mesure que la technologie et les menaces évoluent.

5. Intégrer les pratiques exemplaires du Groupe des cinq

Pour que les mesures du Canada en matière de cybersécurité des IE s'alignent sur les engagements de notre pays envers les alliés du Groupe des cinq, il est nécessaire d'investir dans le renforcement de nos capacités dans le cadre du projet de loi C-26. Le Canada doit tirer parti de ses partenariats avec le Groupe des cinq pour intégrer les cadres éprouvés et les pratiques évoluées que d'autres pays membres ont mis en place. Cela comprend les normes de l'Australie pour la déclaration des incidents et la résilience, les exigences relatives à la vérification systématique et la programmation sûre pour la mémoire comme celles des États-Unis ainsi que les lignes directrices propres à chaque secteur récemment mises à jour du Royaume-Uni.

Bibliographie

Gouvernement de l'Australie, 2021, *Security Legislation Amendment (Critical Infrastructure) Act 2021*, Security Legislation Amendment (Critical Infrastructure) Bill 2021 – Parlement d'Australie.

Gouvernement de l'Australie, 2023, *Critical Infrastructure Resilience Strategy*, Critical-infrastructure-resilience-strategy-2023.pdf.

Centre canadien pour la cybersécurité, 2024, Évaluation des cybermenaces nationales, Évaluation des cybermenaces nationales 2025-2026 – Centre canadien pour la cybersécurité.

CISA, 2023, Objectifs de rendement intersectoriel en matière de cybersécurité, Cross-Sector Cybersecurity Performance Goals (CPGs) | CISA.

Gouvernement du Canada, 2024, « Groupe des 5 Partenaires – Adaptation à l'évolution des menaces : Résumé des approches en matière de sécurité et de résilience des infrastructures essentielles du Groupe des 5 Partenaires », 2024-dptng-vlvng-thrts-fr.pdf.

Gouvernement du Canada, 2024, Rapports conjoints du Groupe des cinq, Bulletin conjoint sur l'exploration de la sécurité de la mémoire dans des projets de source ouverte critiques – Centre canadien pour la cybersécurité et Exploring Memory Safety in Critical Open Source Projects | CISA.

Agence internationale de l'énergie atomique, « Design Basis Threat », https://www.iaea.org/topics/security-of-nuclear-and-other-radioactive-material/design-basis-threat.

Macaulay et Bhasker, 2024, « High Performance Computing Infrastructure and Zero Trust Architecture », High Performance Computing Infrastructure and Zero Trust Architecture | Pulse & Praxis: *The Journal for Critical Infrastructure Protection, Security and Resilience*.

Bureau de la vérificatrice générale du Canada, 2024, *La lutte contre la cybercriminalité*, Rapport 7 — La lutte contre la cybercriminalité.

Parlement du Canada, 2021, Projet de loi C-26, *Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois*, C-26 (44-1) – LEGISinfo – Parlement du Canada.

Sécurité publique Canada, 2024, *Perturbations à l'horizon*, PH4-198-2024-fra.pdf.

Sécurité publique Canada, 2022, *Stratégie nationale sur les infrastructures essentielles : Rapport sur ce que nous avons entendu*, PS4-296-2022-fra.pdf.

Sécurité publique Canada, 2024, *Stratégie nationale de cybersécurité 2019-2024 : Rapport sur l'examen de mi-parcours*, Stratégie nationale de cybersécurité 2019-2024 : Rapport sur l'examen de mi-parcours.

Sécurité publique Canada (2009, 2010, 2023), Stratégie nationale sur les infrastructures essentielles; Plan d'action sur les infrastructures essentielles, Stratégie nationale sur les infrastructures essentielles.

Sécurité publique Canada, 2021, Plan d'action 2021-2023 sur les infrastructures essentielles du Forum national intersectoriel, 2021-ctn-pln-crtcl-nfrstrctr-fr.pdf.

SecurityWeek, 2023, Orientation sur la sécurité de la mémoire, « Five Eyes Agencies Publish Guidance on Eliminating Memory Safety Bugs ».

La Maison-Blanche, 2021, Décret visant l'amélioration de la cybersécurité du pays, Executive Order 14028: Improving the Nation's Cybersecurity, Maison-Blanche.

Gouvernement du Royaume-Uni, 2022, Lignes directrices du National Cyber Security Centre sur les normes propres à chaque secteur en matière de cybersécurité, National Cyber Security Centre - NCSC.GOV.UK.

National Centre for Critical Infrastructure Protection, Security and Resilience
À l'attention de l'Université Carleton, 1125, prom. du Colonel-By, Ottawa (Ontario) K1S 5B6