Electricity Canada | Électricité Canada

Mémoire au Comité permanent de la sécurité publique et nationale

Projet de loi C-8 – *Loi sur la protection des cybersystèmes essentiels*

Novembre 2025

Voix nationale du secteur de l'électricité, Électricité Canada représente les entreprises qui produisent, transportent et distribuent de l'énergie électrique à des clients résidentiels, commerciaux, industriels et institutionnels dans chaque province et territoire.

Les compagnies d'électricité canadiennes défendent depuis longtemps leurs infrastructures contre les cybermenaces. Depuis deux décennies, elles collaborent avec des partenaires gouvernementaux à cette fin.

Électricité Canada estime que les objectifs globaux du projet de loi C-8 sont valables. Nous appuyons une meilleure visibilité du gouvernement fédéral sur les cyberattaques visant les infrastructures critiques et la mise en place d'une approche cohérente et intersectorielle en matière de cybersécurité. Cependant, nous proposons quelques modifications au projet de loi pour qu'il renforce les partenariats avec des organismes fédéraux et consolide la sécurité de notre secteur.

SOMMAIRE DES RECOMMANDATIONS

CHEVAUCHEMENT DE LA RÉGLEMENTATION

1. **Reconnaître les cadres de réglementation équivalents** – Prévoir des dispositions qui permettent à l'organisme de réglementation de reconnaître et d'accepter la conformité à des cadres équivalents. Par exemple, un exploitant qui se conforme aux normes NERC CIP pourrait déjà remplir ses obligations au titre du projet de loi C-8. Les programmes de cybersécurité et la gestion des risques liés à la chaîne d'approvisionnement tomberaient dans cette catégorie d'obligations.

2. **Harmoniser le signalement obligatoire d'incidents** – Habiliter le gouverneur en conseil à mettre en place certains mécanismes d'harmonisation. En effet, le signalement obligatoire au titre du projet de loi C-8, les processus actuels des provinces et les normes NERC CIP doivent s'aligner. L'harmonisation est essentielle pour que les signalements se fassent efficacement et dans les meilleurs délais. Ainsi, les exploitants pourront se concentrer sur les interventions et le rétablissement en cas d'incident.

RISQUES POUR LES PARTENARIATS DU CENTRE POUR LA CYBERSÉCURITÉ

3. **Distinguer nettement les obligations du Centre pour la cybersécurité et celles du CST** – Pour protéger les partenariats du Centre pour la cybersécurité avec les exploitants, le projet de loi devrait être modifié. L'objectif serait d'empêcher la divulgation à des ministères et à des organismes gouvernementaux, y compris les organismes de réglementation, de toute information communiquée au Centre.

ENTITÉS DÉCLARANTES NON PROTÉGÉES

4. **Prévoir des protections et des règles d'exonération (« *safe harbour* ») pour les divulgations** – Modifier le projet de loi C-8 pour qu'aucune mesure réglementaire, coercitive ou juridique ne soit prise à l'endroit d'une entité qui communique de l'information sur la cybersécurité au gouvernement. Ainsi, la confiance sera préservée, la collaboration, renforcée, et le Canada, mieux à même de résister et d'intervenir face aux cybermenaces.

PRÉOCCUPATION N^{O} 1 : CHEVAUCHEMENT DE LA RÉGLEMENTATION

Le projet de loi C-8 risque de dédoubler le cadre de réglementation de la cybersécurité dans le secteur de l'électricité. Ce secteur est déjà régi par la *North American Electric Reliability Corporation* (NERC) et par des organismes de réglementation provinciaux.

- Le projet de loi propose la réglementation d'actifs et de systèmes qui sont déjà assujettis aux normes de la *North American Electric Reliability Corporation* pour la protection des infrastructures essentielles (normes NERC CIP). La plupart des organismes de réglementation provinciaux appliquent déjà ces normes, en plus d'en vérifier la conformité.
- En vertu des normes NERC CIP, les exploitants du secteur sont déjà tenus de désigner, de catégoriser et de protéger les actifs et les systèmes de cybersécurité essentiels. Ils doivent en outre évaluer les risques personnels que courent les personnes qui accèdent à ces systèmes essentiels. Enfin, ils doivent signaler certains incidents de cybersécurité et gérer les risques liés à la chaîne d'approvisionnement. *(Voir à l'annexe A la liste des normes NERC CIP.)*
- Par ailleurs, des instruments provinciaux de réglementation chevauchent aussi des dispositions du projet de loi C-8. Ainsi, la dernière version de la norme ontarienne de cybersécurité oblige désormais les entités de transport et de distribution d'électricité à signaler les incidents de cybersécurité.
- Le risque de double emploi que posent des aspects clés du projet de loi C-8 est considérable. Avant d'imposer de nouvelles exigences réglementaires au secteur de l'électricité, le gouvernement devrait expliquer clairement comment le projet de loi améliorera la cybersécurité davantage que ne le font les normes NERC CIP et la réglementation des provinces.
- Lorsque la réglementation se chevauche, cela peut nuire à la sécurité. Pensons à la hausse des coûts de conformité, à l'ambiguïté et à la confusion créées et à la réaffectation de ressources qui auraient dû être consacrées aux activités de sécurité proprement dites. Ce ne sont là que quelques répercussions éventuelles du projet de loi C-8 sur le secteur de l'électricité.

RECOMMANDATIONS

1. **Reconnaître les cadres de réglementation équivalents** – Prévoir des dispositions qui permettent à l'organisme de réglementation de reconnaître et d'accepter la conformité à des cadres équivalents. Par exemple, un exploitant qui se conforme aux normes NERC CIP pourrait déjà remplir ses obligations au titre du projet de loi C-8. Les programmes de cybersécurité et la gestion des risques liés à la chaîne d'approvisionnement tomberaient dans cette catégorie d'obligations.
2. **Harmoniser le signalement obligatoire d'incidents** – Habiliter le gouverneur en conseil à mettre en place certains mécanismes d'harmonisation. En effet, le signalement obligatoire au titre du projet de loi C-8, les processus actuels des provinces et les normes NERC CIP doivent s'aligner. L'harmonisation est essentielle pour que les signalements se fassent efficacement et dans les meilleurs délais. Ainsi, les exploitants pourront se concentrer sur les interventions et le rétablissement en cas d'incident.

PRÉOCCUPATION N^{O} 2 : RISQUES POUR LES PARTENARIATS DU CENTRE POUR LA CYBERSÉCURITÉ

Le projet de loi C-8 pourrait nuire aux partenariats établis entre le Centre pour la cybersécurité et les exploitants d'infrastructures essentielles. Confier au Centre de la sécurité des télécommunications (CST) un rôle de conseil auprès des organismes de réglementation et orienter les directives de cybersécurité pourrait dissuader les exploitants de communiquer ouvertement de l'information au Centre pour la cybersécurité, alors que ce dernier a œuvré pendant des années à créer une relation de confiance avec les secteurs des infrastructures essentielles. Permettre que des renseignements communiqués de façon confidentielle au Centre pour la cybersécurité soient divulgués à un organisme de réglementation pourrait freiner la collaboration, miner une relation de confiance établie de longue date et dissuader les entreprises de communiquer de l'information ou de solliciter du soutien.

- En exigeant que le CST remette des rapports d'incident à l'organisme de réglementation, le projet de loi risque de dissuader l'exploitant de soumettre au Centre pour la cybersécurité une information de même nature et aussi abondante qu'auparavant. L'exploitant hésitera aussi à recourir au Centre pour qu'il l'aide à intervenir en cas d'incident. Ainsi, une collaboration ouverte pourrait se transformer en signalements circonspects d'ordre purement juridique, au lieu de se prêter à la résolution de crises.
- Le projet de loi C-8 oblige aussi le CST à encadrer l'organisme de réglementation qui souhaite s'assurer qu'un exploitant atténue bel et bien les risques liés à un tiers ou à la chaîne d'approvisionnement. Vu cette obligation, l'exploitant pourrait hésiter à communiquer au Centre des risques liés à la chaîne d'approvisionnement dans notre secteur, par crainte de se voir imposer des mesures de conformité.
- Le projet de loi permet aussi au personnel du CST de transmettre de l'information à des ministères et à des organismes gouvernementaux pour la publication de directives de cybersécurité. Cela risque de dissuader les divulgations volontaires au Centre, car exposer des vulnérabilités pourrait donner lieu à une directive.
- La relation entre la NERC et l'Electricity Information Sharing and Analysis Center (E-ISAC) montre comment une relation de confiance peut s'établir avec des exploitants d'infrastructures essentielles tout en respectant la réglementation. L'E-ISAC relève de la NERC, mais il jouit d'une autonomie suffisante pour qu'aucune information qu'il reçoit ne soit transmise à celle-ci.

RECOMMANDATION

3. **Distinguer nettement les obligations du Centre pour la cybersécurité et celles du CST** – Pour protéger les partenariats du Centre pour la cybersécurité avec les exploitants, le projet de loi devrait être modifié. L'objectif serait d'empêcher la divulgation à des ministères et à des organismes gouvernementaux, y compris les organismes de réglementation, de toute information communiquée au Centre pour la cybersécurité.

PRÉOCCUPATION N^{O} 3 : ENTITÉS DÉCLARANTES NON PROTÉGÉES

L'entité qui signale au gouvernement des cyberincidents ou des vulnérabilités (l'entité déclarante) pourrait faire l'objet de mesures juridiques, réglementaires ou coercitives. Le projet de loi C-8 ne la protège pas suffisamment de ce risque, ce qui aura pour effet de dissuader les divulgations volontaires. Cela représentera une occasion manquée de créer des règles d'exonération (« safe harbour ») et d'accroître la résilience du Canada face aux cybermenaces.

- La confiance entre le gouvernement et l'industrie doit reposer sur des protections juridiques et réglementaires. L'exploitant qui a la certitude que ses divulgations ne lui attireront pas de mesures coercitives sera plus porté à communiquer une information utile. De ce fait, le Canada sera mieux en mesure d'assurer sa cybersécurité.
- En l'absence de protections ou de dispositions claires assurant l'exonération, l'exploitant pourrait se limiter à divulguer uniquement ce que la loi exige. Cela minerait la collaboration avant et pendant un cyberincident. De plus, l'effet dissuasif ainsi créé empêcherait le Centre pour la cybersécurité d'aider les exploitants efficacement.
- Les législateurs doivent songer aux comportements qu'ils souhaitent favoriser. S'ils veulent que l'industrie et le gouvernement collaborent, ils doivent absolument protéger l'entité qui fait des divulgations, tant obligatoires que volontaires.
- Autoriser l'échange d'information entre un organisme de réglementation et le Centre pour la cybersécurité sans dispositions d'exonération claires, ne rendra pas plus sûrs les secteurs des infrastructures essentielles. En fait, cela nuira à la communication et dissuadera les entreprises de demander de l'aide et de transmettre de l'information, et la conformité réglementaire n'en sera pas pour autant assurée.

RECOMMANDATION

4. **Prévoir des protections et des règles d'exonération claires pour les divulgations –** Modifier le projet de loi C-8 pour qu'aucune mesure réglementaire, coercitive ou juridique ne soit prise à l'endroit d'une entité qui communique de l'information sur la cybersécurité au gouvernement. Ainsi, la confiance sera préservée, la collaboration, renforcée, et le Canada, mieux à même de résister et d'intervenir face aux cybermenaces.

ANNEXE A – NORMES NERC CIP

- CIP-002 : Catégorisation des systèmes électroniques BES
- CIP-003 : Mécanismes de gestion de la sécurité
- CIP-004 : Personnel et formation
- CIP-005 : Périmètres de sécurité électronique
- CIP-006 : Sécurité physique des systèmes électroniques BES
- CIP-007 : Gestion de la sécurité des systèmes
- CIP-008 : Déclaration des incidents et planification des mesures d'intervention
- CIP-009 : Plans de rétablissement des systèmes électroniques BES
- CIP-010 : Gestion des changements de configuration et analyses de vulnérabilité
- CIP-011 : Protection de l'information
- CIP-012 : Communications entre centres de contrôle
- CIP-013 : Gestion des risques dans la chaîne d'approvisionnement
- CIP-014 : Sécurité physique