Soumission d'Électricité Canada

Projet de loi C-26

Partie 2 — Loi sur la protection des cybersystèmes essentiels

Mai 2023

613.230.9263
info@electricity.ca
electricity.ca | electricite.ca

1500-275 Slater Street
1500-275, rue Slater
Ottawa, Ontario K1P 5H9

LISTE DES RECOMMANDATIONS

Alignement réglementaire en Amérique du Nord

- Ajouter des dispositions permettant à l'*autorité de réglementation* de libérer un opérateur désigné de l'obligation d'élaborer un programme de cybersécurité.
- Encourager le *gouverneur en conseil* à aligner les définitions pertinentes, y compris la définition d'incident de cybersécurité, avec les définitions de la North American Electric Reliability Corporation (NERC).
- Ajouter des dispositions permettant au *gouverneur en conseil de* prendre des mesures et d'établir des mécanismes pour éviter les doubles emplois ou les chevauchements avec les compétences attribuées aux agences de réglementation provinciales.
- S'assurer qu'un *opérateur désigné* ne puisse pas faire l'objet d'une double sanction dans les systèmes qui peuvent avoir plus d'une autorité de réglementation.

Rapports

- Ajouter des dispositions permettant au *gouverneur en conseil de* prendre des mesures et d'établir des mécanismes afin d'harmoniser le processus de déclaration avec les processus existants de déclaration des incidents de cybersécurité.
- Supprimer les références aux périodes de conformité.
- Ajouter des dispositions accordant une protection juridique aux opérateurs en ce qui concerne les renseignements communiqués au Centre de la sécurité des télécommunications en vertu de la présente loi.
- Modifier l'article 14 (1) b) et supprimer les exigences excessives en matière de rapports sur la chaîne d'approvisionnement et l'utilisation de produits et de services de tiers.

Protéger la collaboration existante

- Exempter le Centre canadien pour la cybersécurité de l'obligation de communiquer à d'autres entités les renseignements obtenus en vertu de la présente loi.
- Modifier les sections « Communication et utilisation des renseignements » pour permettre le partage de renseignements avec la NERC.
- Modifier l'article 25 (1), pour permettre aux *opérateurs désignés* de divulguer à des partenaires industriels de confiance qu'une directive a été émise.

Transparence

- Ajouter l'obligation pour le ministre de rendre compte annuellement du nombre de *directives de cybersécurité* émises ainsi que du taux de conformité à ces directives.
- Ajouter des dispositions qui lèvent l'interdiction de divulguer les *directives de cybersécurité* après un délai raisonnable.

Processus d'élaboration des règlements

- Tirer parti des forums existants sur les infrastructures critiques et solliciter leur contribution au cours du processus d'élaboration de la réglementation.

À propos d'Électricité Canada

Électricité Canada est le forum national et la voix du secteur canadien de l'électricité, industrie novatrice et en pleine évolution. Nos membres assurent la production, le transport et la distribution de l'énergie électrique à des clients industriels, commerciaux, résidentiels et institutionnels dans l'ensemble du pays. Ils comprennent des compagnies d'électricité intégrées, des producteurs indépendants, des sociétés de transport et de distribution, des négociants en électricité et des exploitants de réseau, qui alimentent tous les Canadiens en électricité dans chaque province et territoire.

La cybersécurité et le secteur de l'électricité

La cybermenace qui pèse sur l'industrie canadienne de l'électricité s'accroît chaque année, avec une augmentation du nombre et de la sophistication des attaques. Les entreprises d'électricité canadiennes travaillent depuis longtemps à la protection de leurs actifs critiques contre les nouvelles menaces et collaborent entre elles et avec leurs partenaires gouvernementaux sur les problèmes liés à la cybersécurité depuis plus de vingt ans.

En effet, le secteur partage souvent des renseignements et discute de l'élaboration des meilleures pratiques pour un ensemble varié de problèmes liés à la sécurité affectant l'industrie de l'électricité, et travaille en partenariat avec les responsables de la sécurité et du renseignement et les décideurs politiques au Canada et à l'étranger.

Le secteur a établi avec succès des relations avec des partenaires gouvernementaux comme le Centre canadien pour la cybersécurité, Ressources naturelles Canada et Sécurité publique Canada. Il communique souvent avec des partenaires internationaux, notamment le département de l'Énergie des États-Unis (United States Department of Energy), la North American Electric Reliability Corporation (NERC), la Federal Energy Regulatory Commission (FERC), l'Electricity Information Sharing and Analysis Center (E-ISAC) et les autorités de réglementation provinciales. Ces partenariats garantissent l'accès aux renseignements et aux outils permettant à l'industrie de sécuriser ses systèmes critiques.

Recommandations d'Électricité Canada pour la *Loi sur la protection des cybersystèmes essentiels*

Aperçu

Électricité Canada soutient les mesures qui renforcent la sécurité du pays et du secteur de l'électricité. Les gouvernements et l'industrie ont la responsabilité de veiller à ce que nos infrastructures essentielles soient bien protégées contre les menaces, et la collaboration entre les deux est primordiale.

Cependant, cette collaboration repose sur la confiance et dépend de l'échange de renseignements mutuellement bénéfique. Alors que les exigences obligatoires en matière de sécurité peuvent contribuer

à renforcer notre position en matière de sécurité, l'approche adoptée par le projet de loi C-26 risque d'avoir l'effet inverse. Il ne reconnaît pas les normes de sécurité et l'expertise établies au sein de notre secteur. Le projet de loi risque d'ajouter très peu de sécurité à notre secteur et d'ajouter une couche supplémentaire d'exigences réglementaires.

Il est important que le projet de loi C-26 ne crée pas d'obstacles involontaires à la collaboration et qu'il garantisse que les nouvelles mesures sont alignées sur le cadre réglementaire en place. Il devrait fournir des outils et des protocoles pour renforcer la sécurité du secteur des infrastructures essentielles du Canada.

Alignement réglementaire en Amérique du Nord

L'une de nos principales préoccupations concernant le projet de loi C-26 est le risque de créer le dédoublement des systèmes réglementaires et potentiellement concurrents. Plus précisément, le projet de loi pourrait réglementer des domaines qui sont généralement déjà couverts par les exigences existantes des normes de protection des infrastructures critiques (CIP) de la NERC, qui ont été adoptées, appliquées et vérifiées par de nombreux organismes de réglementation provinciaux[1]. De plus, le projet de loi semble étendre la compétence des régulateurs aux domaines de responsabilité provinciale.

Dans l'ensemble, cela risque de créer des conflits entre les différents régulateurs, d'alourdir la charge réglementaire pour les opérateurs, de créer de la confusion et de l'ambiguïté en matière de conformité et d'entraver l'objectif du projet de loi C-26, qui est de rendre nos systèmes critiques plus sûrs.

Il est donc prioritaire de veiller à ce que les mesures prévues par le projet de loi soient alignées sur le cadre réglementaire nord-américain actuel et n'entrent pas en concurrence avec les régulateurs provinciaux.

Recommandation : Ajouter des dispositions permettant à l'autorité de réglementation de libérer un opérateur désigné de l'obligation d'élaborer un programme de cybersécurité.

En vertu de la loi, le *régulateur* n'a pas le pouvoir de libérer un *opérateur désigné* de l'obligation d'élaborer un programme de cybersécurité ou d'en modifier les conditions si des normes adéquates existent déjà. Une disposition à cet effet pourrait être ajoutée à la loi.

Les normes de fiabilité de la NERC sont appréciées au sein de l'industrie de l'électricité, tant par l'industrie que par les autorités de réglementation provinciales. Elles sont élaborées selon un processus piloté par l'industrie qui garantit qu'il est ouvert à toutes les personnes directement et matériellement concernées par la fiabilité du réseau nord-américain de production-transport d'électricité, qu'il est

[1] Pour faciliter la lecture, l'expression « NERC CIP » est utilisée dans le présent document pour désigner les normes de protection des infrastructures critiques (CIP) de la NERC ainsi que les normes NERC CIP relevant de l'autorité des organismes de réglementation provinciaux.

transparent pour le public, qu'il démontre le consensus pour chaque norme, qu'il équilibre équitablement les intérêts de toutes les parties prenantes, qu'il prévoit un avis raisonnable et la possibilité de formuler des commentaires, et qu'il permet l'élaboration des normes en temps opportun.

Les normes NERC CIP sont les normes de sécurité obligatoires qui s'appliquent à la plupart des entités qui possèdent ou gèrent des installations faisant partie du réseau électrique américain et canadien. Ces normes sont obligatoires et applicables dans presque toutes les provinces connectées au réseau de production-transport d'électricité. Elles exigent des entreprises de services publics nord-américaines qu'elles établissent et respectent un ensemble de mesures de base en matière de cybersécurité.

Considérant la position de notre secteur en matière de cybersécurité et des normes de cybersécurité nord-américaines, le *régulateur* devrait être en mesure de déterminer si les mesures existantes sont suffisantes pour satisfaire aux exigences de la loi et libérer un *opérateur désigné* de ses obligations. Il s'agirait d'une solution simple pour éviter la duplication des efforts et la charge réglementaire.

Recommandation : Encourager le gouverneur en conseil à aligner les définitions pertinentes, y compris la définition d'incident de cybersécurité, avec les définitions de la NERC.

Les règlements qui doivent être élaborés après l'adoption du projet de loi sont susceptibles d'introduire des définitions qui diffèrent du régime réglementaire existant. Cela peut créer de la confusion et de l'ambiguïté inutiles pour les opérateurs.

Les définitions d'un cybersystème critique ou d'un incident de cybersécurité, par exemple, seront probablement différentes de celles utilisées dans les normes NERC CIP. Ces nouvelles définitions pourraient élargir l'éventail des incidents de cybersécurité que les opérateurs doivent signaler.

Le projet de loi devrait ainsi ajouter des dispositions encourageant le *gouverneur en conseil* à aligner les définitions pertinentes avec les définitions déjà élaborées par la NERC.

Recommandation : Ajouter des dispositions permettant au gouverneur en conseil de prendre des mesures et d'établir des mécanismes pour éviter les doubles emplois ou les chevauchements avec les compétences attribuées aux agences de réglementation provinciales.

La *Loi sur la Régie canadienne de l'énergie* stipule que les lois provinciales s'appliquent aux sections intraprovinciales d'une ligne de transport internationale et qu'une province peut désigner une agence de réglementation pour exercer ses pouvoirs, droits et privilèges sur ces sections.

En ce qui a trait aux lignes interprovinciales, la *Loi sur la Régie canadienne de l'énergie* prévoit que pour relever de la compétence de la Régie de l'énergie du Canada, une ligne interprovinciale doit être désignée par arrêté comme une ligne dont la construction et l'exploitation nécessitent la délivrance d'un certificat. Le site web de la Régie de l'énergie du Canada mentionne qu'aucune ligne interprovinciale

n'a reçu une telle désignation à ce jour. Donc, aucune ligne interprovinciale n'est soumise à la compétence de la Régie de l'énergie du Canada.

Le projet de loi C-26 comprend les réseaux de lignes électriques interprovinciales et internationales dans sa liste de systèmes critiques et les soumet à la loi. Il désigne également la Régie de l'énergie du Canada comme *régulateur* de ce système critique.

Compte tenu de ce qui précède, le projet de loi C-26 semble étendre la compétence de la Régie de l'énergie du Canada à des domaines qui relèvent de la compétence provinciale. Comme c'est le cas pour les articles 253 et 254 de la *Loi sur la Régie canadienne de l'énergie*, le projet de loi C-26 ne fait pas de distinction entre les sections intraprovinciales et internationales d'une ligne internationale. Dans le domaine de la cybersécurité, et conformément au projet de loi C-26, la compétence de la Régie de l'énergie du Canada couvrirait l'ensemble de la ligne internationale, y compris ses sections intraprovinciales, soumises actuellement aux lois provinciales et à la compétence de l'organisme de réglementation nommé par la province.

Bien qu'aucune ligne interprovinciale n'ait été nommée par un arrêté du gouvernement fédéral en vertu de la *Loi sur la Régie canadienne de l'énergie*, la loi pourrait s'appliquer à cette ligne en l'absence de désignation. L'annexe 1 du projet de loi C-26 ne fait aucune distinction à cet égard. Dans le domaine de la cybersécurité, toutes les lignes interprovinciales relèveraient de la compétence de la *Régie canadienne de l'énergie*, y compris celles qui n'ont pas été désignées.

Pour éviter des systèmes réglementaires concurrents, la loi se doit d'être plus claire; en reconnaissant, dans la loi, l'application des lois provinciales et la compétence de l'organisme de réglementation de la province sur les lignes interprovinciales non désignées et sur la section intraprovinciale d'une ligne de transport international, par exemple. Elle doit également comprendre des dispositions permettant au *gouverneur en conseil* de prendre des mesures et d'établir des mécanismes pour éviter les doubles emplois ou les chevauchements avec d'autres juridictions.

Recommandation : S'assurer qu'un opérateur désigné ne puisse pas faire l'objet d'une double sanction dans les systèmes qui peuvent avoir plus d'une autorité de réglementation.

Les régulateurs provinciaux ont le pouvoir d'imposer des sanctions et des pénalités en cas de violation d'une norme de fiabilité. Comme le projet de loi C-26 réglementerait des domaines déjà couverts par les exigences de la NERC CIP, un opérateur pourrait être injustement soumis à une double sanction en cas de violation. Le projet de loi devrait ajouter des dispositions qui éliminent la possibilité d'une double sanction dans les systèmes qui peuvent avoir plus d'un régulateur.

Rapports

La déclaration obligatoire des incidents liés à la cybersécurité est un élément primordial du projet de loi C-26. Il s'agit d'une rupture importante par rapport à la pratique actuelle, où le signalement des incidents par les opérateurs aux autorités fédérales est volontaire. Bien que nous comprenions

l'importance pour le gouvernement fédéral d'être avisé rapidement et de manière cohérente des incidents liés à la cybersécurité, nous constatons d'importantes lacunes dans le projet de loi. Des amendements sont nécessaires pour s'assurer que les exigences en matière d'avis ne sont pas redondantes ou excessives, et pour garantir que les opérateurs ne s'exposent pas à des risques juridiques en se conformant à ces exigences ou en partageant volontairement des renseignements avec leurs partenaires fédéraux.

Recommandation : Ajouter des dispositions permettant au gouverneur en conseil de prendre des mesures et d'établir des mécanismes afin d'harmoniser le processus de déclaration avec les processus existants de déclaration des incidents de cybersécurité.

Les entités réglementées par la NERC sont déjà soumises à l'obligation de signaler les incidents liés à la cybersécurité. Un incident de cybersécurité doit être signalé à l'Electricity Information Sharing and Analysis Center (E-ISAC) dans l'heure qui suit la détermination qu'il doit être déclaré, ou avant la fin du jour civil suivant la détermination qu'un incident lié à la cybersécurité était une tentative de compromettre un cybersystème.

Comme il a été indiqué précédemment, le projet de loi C-26 donne une définition d'un incident de cybersécurité différente de celle étant utilisée dans les normes NERC CIP. Cette nouvelle définition pourrait élargir l'éventail des incidents liés à la cybersécurité qui doivent être signalés au Centre de la sécurité des télécommunications (CST).

L'harmonisation des processus de notification semble nécessaire, puisqu'en cas d'urgence, la décision d'aviser ou non d'un incident lié à la cybersécurité, que ce soit à l'E-ISAC ou au CST, doit être prise rapidement et sans effort excessif. Toute confusion ou ambiguïté concernant la détermination des incidents de cybersécurité peut entraîner des retards susceptibles de mettre le réseau en péril.

Recommandation : Supprimer les références aux périodes de conformité.

Les exigences en matière de cybersécurité, en particulier celles relatives à la notification des incidents, ne doivent pas détourner les opérateurs d'infrastructures critiques de leurs efforts d'intervention et de rétablissement à la suite d'un incident. Les exigences en matière d'établissement de rapports doivent être bien définies, cohérentes et assorties d'un délai suffisamment flexible pour permettre l'utilisation efficace de ressources limitées lors de l'intervention et du rétablissement.

Le délai de déclaration des incidents liés à la cybersécurité repose sur le moment où il est déterminé qu'un incident doit être déclaré, et non sur le moment de l'incident. Toute référence au délai de déclaration des incidents de cybersécurité devrait être laissée à la réglementation. Donc, le mot « immédiatement » devrait être supprimé de l'article 17.

De même, les mots « sans délai » devraient également être supprimés de l'article 14.

Recommandation : Ajouter des dispositions accordant une protection juridique aux opérateurs en ce qui concerne les renseignements communiqués au Centre de la sécurité des télécommunications en vertu de la présente loi.

À moins que le projet de loi comprenne des dispositions accordant une protection juridique aux opérateurs d'infrastructures critiques qui communiquent des renseignements au CST, les opérateurs seront réticents à partager des renseignements supplémentaires et à fournir des rapports volontaires sur des incidents qui pourraient ne pas entrer dans le champ d'application de la réglementation. Comme l'a entendu le Comité permanent de la sécurité publique et nationale lors de son *évaluation de la posture de sécurité du Canada par rapport à la Russie* l'année dernière, des dispositions ou mesures « d'exonération » sont un élément important de la promotion de l'échange de renseignements entre l'industrie et le gouvernement. Il sera donc crucial d'ajouter des dispositions qui réduisent les risques juridiques des opérateurs d'infrastructures critiques pour garantir la mise en œuvre réussie des nouvelles exigences en matière de rapports et la réalisation des objectifs généraux de la législation.

L'année dernière, les États-Unis ont adopté le *Cyber Incident Reporting for Critical Infrastructure Act 2022 (CIRCIA)*. Cette loi comprend des dispositions qui prévoient des protections en matière de responsabilité pour les entités déclarantes. Nous recommandons d'ajouter un libellé similaire dans le projet de loi C-26. Ces protections juridiques devraient également être étendues aux rapports volontaires, comme le prévoit la CIRCIA.

Recommandation : Modifier l'article 14 (1) b) et supprimer les exigences excessives en matière de rapports sur la chaîne d'approvisionnement et l'utilisation de produits et de services de tiers.

Le projet de loi exige l'élaboration d'un programme de cybersécurité pour gérer les risques associés à la chaîne d'approvisionnement de l'opérateur désigné et à l'utilisation de produits et de services de tiers. Ce programme nécessitera l'élaboration d'une liste de produits et de services de tiers qui, s'ils sont compromis, peuvent avoir des incidences sur un service ou un système critique. Le programme de cybersécurité permet de gérer en continu les risques liés à la chaîne d'approvisionnement au fur et à mesure de l'ajout et de la suppression de produits et de services.

En vertu de l'article 14 (1) (b), un opérateur désigné doit aviser l'autorité de réglementation de tout changement important dans sa chaîne d'approvisionnement ou dans son utilisation de produits et services de tiers. Nous recommandons que cette disposition soit modifiée ou remplacée par une disposition moins contraignante et plus adaptée.

L'article 14 (1) b) ajoute des exigences supplémentaires en matière d'établissement de rapports sans apporter de gain supplémentaire en matière de cybersécurité. Cela risque de retarder le processus d'achat et d'acquisition des logiciels et services nécessaires, dans un environnement de marché où les chaînes d'approvisionnements éprouvent déjà des difficultés. Si l'on considère tous les systèmes de contrôle susceptibles d'avoir une incidence sur un service essentiel, y compris les centres de contrôle

centraux, grand nombre de logiciels peuvent être utilisés sur des centaines de systèmes informatiques. Cela rend l'exercice d'établissement de rapports difficile.

Cette disposition crée également des risques supplémentaires pour la sécurité du système essentiel en créant une liste centrale de produits et de services de tiers susceptibles d'avoir une incidence sur les systèmes essentiels en cas de compromission. Cette liste serait ensuite transmise et visible par des parties qui n'ont pas besoin de ces renseignements.

En revanche, nous proposons que l'opérateur puisse gérer les risques liés à la chaîne d'approvisionnement sans devoir déclarer les logiciels et services utilisés. Au lieu d'exiger des opérateurs qu'ils avisent l'autorité de réglementation de « changements importants », les documents relatifs au processus de gestion des risques de la chaîne d'approvisionnement devraient rester chez l'opérateur désigné et être disponibles pour analyse en vertu des dispositions permettant à l'autorité de réglementation de faire la vérification du programme de cybersécurité de l'opérateur désigné. Cela permettrait à l'autorité de réglementation de vérifier le processus de gestion des risques de la chaîne d'approvisionnement de l'opérateur, sans ajouter d'exigences excessives en matière de rapports ni créer de risques supplémentaires pour la sécurité.

Protéger la collaboration existante

Dans sa forme actuelle, nous craignons que le projet de loi C-26 n'ait des conséquences imprévues sur la collaboration existante au sein de l'industrie, ainsi qu'avec les gouvernements et les organismes de réglementation nord-américains. Nous demandons au Comité de prendre en considération ces recommandations afin de s'assurer que la collaboration existante, qui contribue à assurer la sécurité de nos infrastructures critiques, ne soit pas affectée négativement par ce projet de loi.

Recommandation : Exempter le Centre canadien pour la cybersécurité de l'obligation de communiquer à d'autres entités les renseignements obtenus en vertu de la présente loi.

Depuis la création du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) en 2018, l'industrie et le gouvernement ont collaboré étroitement sur les problèmes liés à la cybersécurité. Cela a permis de renforcer la posture de sécurité globale du Canada. Cette collaboration entre l'industrie et le Centre pour la cybersécurité repose sur la confiance. La confiance dans le fait que les renseignements partagés avec le Centre pour la cybersécurité ne sont pas communiqués aux organismes de réglementation ou d'application de la loi. Le projet de loi C-26 met en péril cette collaboration.

Afin de protéger la collaboration existante et positive entre les opérateurs d'infrastructures critiques et le Centre pour la cybersécurité, nous recommandons que le projet de loi isole celui-ci de toute obligation de partage de renseignements prévu par la législation.

Bien que les rôles de ces organisations soient différents, la relation entre la NERC, les régulateurs provinciaux et l'E-ISAC est un exemple de la manière dont une agence peut gagner la confiance des

exploitants d'infrastructures critiques et favoriser le partage de renseignements. Bien que l'E-ISAC soit géré par la NERC, il est isolé, sur le plan organisationnel, des processus d'application de la NERC. Cela signifie que les renseignements que les opérateurs communiquent à l'E-ISAC ne seront pas partagés avec la NERC.

Recommandation : Modifier les sections « Communication et utilisation des renseignements » pour permettre le partage de renseignements avec la NERC.

Le projet de loi prévoit des restrictions en ce qui concerne les organisations avec lesquelles les autorités fédérales peuvent conclure des accords en vue de partager des renseignements : le gouvernement d'une province ou l'une de ses institutions, un État étranger ou une organisation internationale créée par les gouvernements de plusieurs États. Cependant, il n'est pas certain que la NERC réponde à la définition d'une « organisation internationale », étant donné qu'il s'agit d'une organisation nord-américaine sans but lucratif placée sous la surveillance de la FERC.

La NERC n'a été créée par aucun gouvernement. Elle a été créée à la suite d'un accord conclu le 1er juin 1968 entre 12 organisations régionales gérant les réseaux électriques américains et des parties des réseaux de l'Ontario, de la Colombie-Britannique et du Manitoba. L'E-ISAC, qui est géré par la NERC, mais distinct d'un point de vue organisationnel, n'est pas considéré comme une organisation internationale. Cela dit, les autorités fédérales ne seraient pas autorisées à conclure un accord avec la NERC et l'E-ISAC concernant la divulgation de renseignements, qu'ils soient confidentiels ou non.

Des craintes légitimes existent quant à la possibilité de faire coexister les mécanismes établis par la loi et ceux qui sont actuellement en place. Les deux mécanismes nécessitent le partage de renseignements dont la plupart sont confidentiels au sens de la loi. Bien que la divulgation de renseignements confidentiels soit autorisée lorsqu'elle est nécessaire pour protéger les systèmes vitaux et les cybersystèmes critiques (article 26 (1) d)), il n'est pas certain que les opérateurs puissent continuer à s'adresser à la NERC pour les problèmes liés à la cybersécurité et à signaler les incidents de cybersécurité à l'E-ISAC.

Par ailleurs, à moins qu'un accord puisse être conclu entre l'autorité fédérale et la NERC, les opérateurs ne seraient pas autorisés à divulguer directement à la NERC l'existence d'une directive et les mesures que le gouvernement fédéral leur ordonne de prendre en vertu de cette directive. Il est important de rappeler que le contenu et l'existence d'une directive constituent des renseignements qui ne peuvent être divulgués (art. 24 et 25).

Il faut préciser que, dans les normes CIP adoptées (p. ex., CIP-008-5), les régulateurs provinciaux peuvent se référer aux normes de la NERC ainsi qu'aux mécanismes de l'E-ISAC pour le signalement des incidents liés à la cybersécurité. La *Régie de l'énergie du Québec*, par exemple, a également conclu un accord concernant le Programme de surveillance de la conformité et d'application des normes de fiabilité au Québec (PSCAQ) en vertu duquel elle retient les services de la NERC et du *Northeast Power Coordinating Council* (NPCC) pour « contrôler et évaluer la conformité des entités soumises aux normes de fiabilité au Québec » (clause 3). En vertu de cet accord, la NERC et le NPCC peuvent accéder à distance à un entrepôt de données contenant des renseignements qui ne sont pas publiques.

Pour protéger la collaboration existante qui rend notre réseau plus sûr, le projet de loi devrait être modifié pour permettre le partage de renseignements avec la NERC ou avec toute entité régionale avec laquelle les régulateurs provinciaux ont conclu un accord. Il devrait également garantir que tout accord ou arrangement conclu entre l'autorité fédérale et les régulateurs provinciaux permette la reconnaissance de l'accord entre eux, la NERC et les entités régionales.

Recommandation : Modifier l'article 25 (1) pour permettre aux opérateurs désignés de divulguer à des partenaires industriels de confiance qu'une directive a été émise.

Le secteur de l'électricité a une tradition d'assistance mutuelle aux autres services publics en cas de besoin. Les responsables de la sécurité du secteur se réunissent régulièrement pour discuter des défis, des menaces et des meilleures pratiques qu'ils partagent. En temps de crise, il est primordial de maintenir la capacité du secteur à se mobiliser et à demander de l'aide.

Le secteur est confronté à d'importantes pénuries de main-d'œuvre et de compétences dans le domaine de la cybersécurité. Par conséquent, le partage de l'expertise entre les opérateurs d'infrastructures critiques contribue à renforcer le dispositif de sécurité de notre secteur.

L'article 25 (1) devrait être élargi pour permettre la divulgation d'une directive de cybersécurité afin de recevoir une assistance mutuelle de la part de partenaires industriels de confiance, et pour protéger la collaboration des opérateurs avec leurs partenaires d'intervention déterminés.

Le projet de loi devrait également clarifier la capacité des opérateurs à divulguer des *directives* aux partenaires provinciaux, y compris aux régulateurs provinciaux. Ceci est particulièrement important dans les cas où une directive peut entrer en conflit avec les exigences réglementaires existantes. Dans ce cas, les exploitants qui ne sont pas en mesure de divulguer qu'une directive a été émise risquent d'être trouvés en situation de non-conformité par leurs autorités de réglementation provinciales.

Transparence

Nous comprenons que la sécurité nationale exige un certain niveau de confidentialité. Nous pensons que certaines dispositions pourraient toutefois être ajoutées à ce projet de loi afin d'offrir des niveaux de transparence raisonnables et pratiques.

Recommandation : Ajouter l'obligation pour le ministre de rendre compte annuellement du nombre de directives de cybersécurité émises ainsi que du taux de conformité à ces directives.

Bien que l'article 146 oblige le ministre à préparer, annuellement, « un rapport visant l'application de la présente loi », il n'est pas certain que cette obligation permette d'atteindre un niveau de transparence suffisant. Le Comité devrait modifier l'article 146 et ajouter des exigences spécifiques en matière de rapport pour le ministre. Bien qu'il puisse être raisonnable pour le gouvernement de ne pas rendre public le contenu des directives en matière de cybersécurité, il devrait être transparent avec les Canadiens sur la fréquence à laquelle il utilise les pouvoirs prévus par la loi. Un rapport annuel sur le

nombre de directives de cybersécurité émises ainsi que sur le taux de conformité à ces ordonnances serait un pas dans la bonne direction, permettant au public et à l'industrie de mieux comprendre dans quelle mesure les pouvoirs prévus par le projet de loi sont utilisés.

Recommandation : Ajouter des dispositions qui lèvent l'interdiction de divulguer des directives de cybersécurité après un délai raisonnable.

Pour plus de transparence, le projet de loi devrait comprendre des dispositions qui lèvent l'interdiction de divulgation après un délai raisonnable. Il est possible que l'interdiction de divulguer toutes les directives ne soit jamais levée, ce qui signifie que les Canadiens et l'industrie ne se rendront jamais compte de l'étendue de l'utilisation des nouveaux pouvoirs par le gouvernement.

Sans lever complètement l'interdiction de divulgation, des dispositions devraient au moins permettre aux agences gouvernementales et aux opérateurs d'infrastructures critiques de se rencontrer et de discuter du contenu des directives en matière de sécurité. Ce type de partage de renseignements aiderait les opérateurs à identifier les lacunes communes et à mieux défendre leurs systèmes, renforçant ainsi le dispositif de sécurité de notre secteur.

Processus d'élaboration de la réglementation

Le projet de loi C-26 est un texte législatif préparatoire, dont les détails seront élaborés au cours du processus de réglementation. Compte tenu de l'incidence significative du projet de loi sur les opérateurs d'infrastructures critiques, il convient de tirer parti des forums existants au cours du processus de consultation.

Recommandation : Tirer parti des forums existants sur les infrastructures critiques et solliciter leur contribution au cours du processus d'élaboration de la réglementation.

La communauté des infrastructures critiques est composée de membres expérimentés qui ont une grande connaissance des problèmes de sécurité auxquels leur secteur est confronté. Les opérateurs d'infrastructures critiques dans le secteur de l'électricité sont déjà mobilisés dans des processus d'élaboration de règles réglementaires au moyen de la NERC. Tirer parti de cette expérience permettrait non seulement de s'assurer que les nouvelles réglementations ne font pas inutilement double emploi avec les mesures existantes, mais aussi qu'elles ont une incidence élevée et positive sur le niveau de sécurité de notre pays et de nos infrastructures critiques.