Mémoire d'Ingénieurs Canada présenté au Comité permanent de la sécurité publique et nationale

Projet de loi C-26, Loi concernant la cybersécurité, modifiant la *Loi sur les télécommunications* et apportant des modifications corrélatives à d'autres lois

Les questions relatives à la teneur de ce mémoire devraient être adressées à :

Joey Taylor
Gestionnaire, Affaires publiques et Relations gouvernementales
Ingénieurs Canada
joey.taylor@ingenieurscanada.ca
613.232.2474, poste 213

Aperçu

Le gouvernement du Canada prend des mesures proactives afin de renforcer la cybersécurité en apportant des modifications exhaustives au *Projet de loi C-26, Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois*. Les modifications proposées consistent en deux parties, chacune ayant trait à des aspects particuliers de la cybersécurité.

La partie 1 est axée sur la modification de la *Loi sur les télécommunications* afin d'accorder une priorité à la sécurité du système canadien de télécommunication et la partie 2 présente la *Loi sur la protection des cybersystèmes essentiels* qui prévoit un cadre de protection des cybersystèmes essentiels qui sont d'une importance critique pour la sécurité nationale ou la sécurité publique.

En mettant en œuvre ces changements législatifs, le gouvernement fédéral vise à renforcer la sécurité et la résilience du système canadien de télécommunication et des cybersystèmes essentiels. Ces mesures contribuent à l'objectif global de créer un cyberenvironnement plus sûr et plus sécurisé au Canada, d'atténuer les risques et d'assurer la protection des intérêts nationaux.

Lutter contre les cybermenaces : protéger le paysage numérique du Canada

La cybersécurité revêt une importance capitale dans notre monde de plus en plus numérique, où la protection des ordinateurs, des réseaux, des logiciels et des données contre les accès non autorisés et les attaques malveillantes est essentielle. La protection des infrastructures essentielles du Canada est importante pour la stabilité économique et la sécurité nationale. Les perturbations des infrastructures essentielles peuvent avoir des conséquences catastrophiques, notamment la perte de vies humaines, des effets économiques négatifs et une atteinte à la confiance du public. À mesure que la technologie évolue et que les systèmes numériques deviennent plus complexes, les compétences des personnes qui cherchent à exploiter les vulnérabilités évoluent également. Les cyberattaques et les violations de données sont de plus en plus fréquentes, ce qui souligne la nécessité de mettre en place des mesures de cybersécurité solides.

Le Sondage de CIRA sur la cybersécurité a mis en lumière les défis en constante augmentation auxquels font face les organisations canadiennes en matière de protection contre les cybermenaces. Le sondage révèle une augmentation importante de la difficulté de se défendre contre les attaques par rapport aux niveaux prépandémiques. Près de 30 % des organisations ont été victimes d'une violation de données, tandis que 15 % ont subi une atteinte à leur réputation et une perte de clients à la suite d'une attaque. Ces statistiques soulignent le besoin urgent de prendre des mesures proactives en matière de cybersécurité.

Les avantages d'intégrer les ingénieurs dans la législation sur la cybersécurité

La participation d'ingénieurs titulaires, en particulier ceux qui travaillent dans le domaine de la cybersécurité, est importante pour relever efficacement ces défis. Les ingénieurs possèdent une expertise qui les rend tout particulièrement qualifiés pour contribuer à la conception, à la mise en œuvre et au maintien de mesures de cybersécurité. Leurs connaissances spécialisées, leur approche systémique, leur responsabilité éthique, leur respect de normes rigoureuses et leur engagement à l'égard du développement professionnel continu profitent grandement aux initiatives en matière de cybersécurité.

Responsabilité éthique et professionnelle

Les ingénieurs qui exercent dans des disciplines spécialisées possèdent les mêmes compétences que d'autres professionnels des TI, mais ils sont tenus professionnellement et éthiquement responsables à un niveau plus élevé en vertu des lois provinciales et territoriales en vigueur au Canada. Opérant dans un environnement réglementaire, les ingénieurs assurent la responsabilité de leur travail. Ils adhèrent à des normes éthiques et professionnelles strictes imposées par les organismes de réglementation, en privilégiant les pratiques exemplaires et la sécurité publique. En intégrant les ingénieurs dans la législation fédérale, la responsabilité éthique de ces derniers profite aux initiatives de cybersécurité. Cette intégration garantit le développement, la mise en œuvre et le maintien de mesures de cybersécurité avec un engagement fort à l'égard de la conduite éthique, de la responsabilité et de la protection du public et de l'environnement naturel.

Expertise spécialisée

Les ingénieurs possèdent des connaissances et des compétences spécialisées qui sont très pertinentes pour la cybersécurité. Leur expertise dans des domaines tels que les communications, la conception de systèmes, et le développement de matériel et de logiciels leur permet de comprendre en profondeur les aspects techniques de la cybersécurité. En impliquant les ingénieurs dans le processus législatif, leurs connaissances spécialisées sont mises à profit dans l'élaboration et la mise en œuvre des politiques et des réglementations en matière de cybersécurité, ce qui se traduit par des mesures de cybersécurité plus efficaces et plus complètes.

Pensée systémique et évaluation des risques

Les ingénieurs sont formés pour aborder les problèmes sous un angle systémique, en tenant compte des interdépendances et des risques entre les différentes composantes. Cette approche holistique est très utile lorsqu'il s'agit de relever les défis de la cybersécurité, car elle permet aux ingénieurs d'évaluer les vulnérabilités, de repérer les vecteurs d'attaque potentiels et de concevoir des stratégies d'atténuation qui tiennent compte de l'ensemble du système. En intégrant les ingénieurs dans le processus législatif, les responsables de l'élaboration des politiques peuvent tirer parti de leurs capacités de pensée

systémique pour élaborer des cadres de cybersécurité complets qui tiennent compte de la complexité des infrastructures critiques.

Développement professionnel continu

Les ingénieurs sont tenus de participer à des activités de développement professionnel continu afin de rester au fait des dernières tendances, technologies et pratiques exemplaires de l'industrie. En incluant les ingénieurs dans la législation fédérale, leur engagement en matière de formation continue et d'acquisition de connaissances profite aux initiatives de cybersécurité. En effet, les ingénieurs sont en mesure de faire face efficacement aux nouvelles cybermenaces et d'intégrer les stratégies et technologies défensives les plus récentes dans les cadres de cybersécurité.

Recommandations

Ingénieurs Canada recommande les modifications suivantes à la *Loi sur les télécommunications* afin de s'assurer que les ingénieurs soient sollicités :

1. Modification du paragraphe 71(2) de l'article 4(1) Désignation des inspecteurs :
    - « (2) Le ministre peut désigner au titre d'inspecteur une personne qualifiée, telle qu'un ingénieur titulaire, pour vérifier le respect ou prévenir le non-respect des dispositions de la présente loi qu'il est chargé de faire appliquer. Cela inclut les arrêtés visés aux articles 15.1 et 15.2 ou les règlements visés à l'alinéa 15.8(1)(a). »

Cette modification proposée vise à élargir le pouvoir du ministre de désigner des inspecteurs qui sont des personnes qualifiées, comme les ingénieurs, dans le but précis d'assurer le respect des dispositions de la loi. Elle améliore l'efficacité des mécanismes d'application de la loi et renforce le cadre réglementaire en habilitant les inspecteurs qualifiés à prendre les mesures appropriées pour vérifier le respect ou prévenir la non-respect.

2. Modification du texte actuel du paragraphe 71(2) de l'article 4(1) :
    - « (2) Le ministre peut désigner au titre d'inspecteur une personne qualifiée, telle qu'un ingénieur titulaire, pour vérifier le respect ou prévenir le non-respect des dispositions de la présente loi qu'il est chargé de faire appliquer. »
    - La modification proposée, qui prévoit l'ajout d'ingénieurs titulaires en tant qu'inspecteurs, reconnaît l'expertise spécialisée que possèdent les ingénieurs et qui est d'une grande utilité pour assurer le respect de la loi et prévenir efficacement les cas de non-respect. En accordant au ministre le pouvoir de désigner des ingénieurs à titre d'inspecteurs, la modification vise à améliorer l'efficacité des inspections et des activités de mise en application de la loi en tirant parti des connaissances et compétences techniques des ingénieurs. Cette reconnaissance de l'expertise des ingénieurs contribuera à l'efficacité et l'efficience globales des inspections, renforçant ainsi l'objectif d'assurer le respect de la loi.

Conclusion

La collaboration du Comité avec des parties prenantes importantes, en particulier la profession d'ingénieur, est essentielle au soutien de la cybersécurité de même qu'au maintien de l'intérêt public et de la sécurité publique. En intégrant les ingénieurs au processus législatif, nous pouvons tirer parti de leur expertise et assurer l'élaboration de mesures de cybersécurité robustes et résilientes. Ingénieurs Canada se réjouit à l'idée de contribuer à ces efforts et est reconnaissant au Comité d'examiner les recommandations.

À propos d'Ingénieurs Canada

Ingénieurs Canada est l'organisme national constitué des 12 organismes provinciaux et territoriaux de réglementation du génie qui sont chargés de délivrer les permis d'exercice aux ingénieurs du pays, dont le nombre s'élève actuellement à plus de 300 000. Étant le seul porte-parole national de la profession d'ingénieur, notre organisme collabore depuis longtemps avec le gouvernement fédéral pour l'aider à élaborer les lois, les règlements et les politiques publiques qui touchent la profession.