engineerscanada
ingénieurscanada

EXERCICE PROFESSIONNEL DANS LE DOMAINE DE LA CYBERSÉCURITÉ

POSITION DE LA PROFESSION

- Les lois relatives à la cybersécurité doivent tenir compte de la nécessité d'avoir recours à des ingénieurs pour le développement et la maintenance des logiciels, du matériel, des systèmes et des infrastructures essentielles de cybersécurité.
- Peu importe que cela soit prévu dans une loi fédérale ou provinciale, la cybersécurité exige la participation d'un ingénieur inscrit auprès d'un organisme de réglementation provincial.
- En intégrant la responsabilité d'un ingénieur dans la législation fédérale et provinciale liée aux infrastructures et systèmes de cybersécurité, on inscrit le processus de réglementation du génie dans les pratiques gouvernementales, ce qui assure la sécurité de la population canadienne.
- Les organismes canadiens de réglementation du génie ont pour mission de protéger l'intérêt public. Ils établissent des normes professionnelles et déontologiques élevées, instaurent et tiennent à jour des codes de conduite et administrent les processus réglementaires pour les ingénieurs afin d'assurer la protection de l'intérêt public et de l'environnement naturel.

Enjeu

La cybersécurité est décrite comme l'ensemble des techniques de protection des ordinateurs, des réseaux, des matériels, des logiciels, des programmes et des données contre les accès non autorisés ou les attaques qui visent à les exploiter.[1] Dans un monde de plus en plus numérique, les Canadiens s'attendent à ce que les systèmes technologiques soient protégés contre les menaces et les vulnérabilités en matière de cybersécurité. La sécurité nationale et la stabilité économique du Canada dépendent de la résilience des infrastructures essentielles. On entend par infrastructures essentielles l'ensemble des processus, des systèmes, des installations, des technologies, des réseaux, des biens et des services nécessaires pour assurer la santé, la sûreté, la sécurité et le bien-être économique de la population canadienne ainsi que l'efficacité du gouvernement. Il peut s'agir d'infrastructures autonomes ou caractérisées par des interdépendances au sein d'une province ou d'un territoire, entre eux ou au-delà des frontière du pays. La perturbation de ces infrastructures essentielles pourrait se traduire en pertes de vie et en effets économiques néfastes, et pourrait considérablement ébranler la confiance du grand public[2]. Alors que les systèmes d'infrastructure essentiels deviennent de plus en plus interconnectés, en particulier avec le développement de systèmes d'intelligence artificielle, et que les services essentiels sont petit à petit gérés en ligne, les vulnérabilités, les incidents et les attaques préméditées visant des infrastructures indispensables peuvent compromettre gravement la sécurité du pays et de la population.

À mesure que la technologie se développe et que les systèmes numériques deviennent plus complexes et sophistiqués, les compétences des personnes qui tentent de les affaiblir le deviennent aussi. Les cyberattaques et les violations de données sont aujourd'hui monnaie courante. Selon une étude réalisée par Statistique Canada en 2017, environ 21 % des entreprises canadiennes ont déclaré avoir été touchées par un incident de cybersécurité qui a eu des répercussions sur leurs activités quotidiennes. L'étude révélait aussi que 41 % des grandes entreprises étaient plus de deux fois plus susceptibles que les petites entreprises d'avoir décelé un incident ayant des répercussions.[3]

Compte tenu de la demande croissante de professionnels de la cybersécurité et de la nécessité immédiate de se prémunir contre de futures cyberattaques, il importe que le gouvernement fédéral demeure vigilant pour s'assurer que des ingénieurs inscrits auprès d'un organisme de réglementation provincial, plus précisément les ingénieurs travaillant dans le domaine de la cybersécurité et qui sont des experts en communication et en sécurité, participent à la conception, à la mise en œuvre et à la maintenance des logiciels, matériels et systèmes de cybersécurité et des cyberinfrastructures essentielles.

Les ingénieurs qui exercent dans des disciplines spécialisées possèdent, au minimum, les mêmes compétences que d'autres professionnels des TI, mais ils sont tenus responsables de leur travail, sur le plan professionnel comme sur le plan déontologique, par les organismes canadiens de réglementation du génie en vertu de la législation provinciale et territoriale dans tout le Canada. Les autres professionnels des TI ne sont pas assujettis à un cadre réglementaire. S'ils participent au développement et à la maintenance des logiciels, des matériels, des systèmes et des infrastructures essentielles, ces ingénieurs seront tenus personnellement responsables de leur travail dans le cadre des processus d'application de la loi, d'enquête et de discipline. Si les ingénieurs ne participent pas au processus de développement et de maintenance, la responsabilité sera limitée au recours au système judiciaire.

EXERCICE PROFESSIONNEL DANS LE DOMAINE DE LA CYBERSÉCURITÉ

Contribution d'Ingénieurs Canada à cet enjeu

Ingénieurs Canada participe activement aux consultations fédérales sur les lois et les règlements qui ont une incidence sur le travail des ingénieurs et qui portent sur des activités pouvant nécessiter l'expertise d'un ingénieur.

Par ailleurs, les organismes canadiens de réglementation du génie ont pour mission de protéger et d'améliorer le bien-être public. Ils établissent des normes professionnelles et déontologiques élevées, instaurent et tiennent à jour des codes de conduite et administrent les processus réglementaires pour les ingénieurs afin d'assurer la protection du public et de l'environnement naturel.

Recommandations à l'intention du gouvernement fédéral

Ingénieurs Canada a été encouragé de voir que le gouvernement fédéral s'est engagé, dans le Budget de 2019, à protéger les cybersystèmes essentiels qui soutiennent l'infrastructure et les services qui font partie intégrante de la vie quotidienne de la population canadienne.

Ingénieurs Canada appuie les initiatives fédérales en matière de cybersécurité, plus précisément le travail du Centre canadien pour la cybersécurité, qui visent à assurer un cyberespace sûr et sécurisé, chose importante pour la sécurité, la stabilité et la prospérité du Canada. Pour mieux protéger les Canadiens contre de futures cyberattaques, le gouvernement fédéral devrait :

- S'assurer que les lois et les règlements qui font mention de travaux d'ingénierie sont élaborés en collaboration avec des ingénieurs, conformément aux lois sur les ingénieurs en vigueur dans les provinces et territoires;
- Utiliser les lois en lien avec la profession pour faire en sorte que les travaux d'ingénierie soient effectués par des professionnels titulaires d'un permis d'exercice, encourageant ainsi la conformité aux lois régissant la profession.
- Développer davantage, clarifier et faire appliquer les règlements, les règles, les lignes directrices relatives à la cybersécurité et les normes de développement et de maintenance des infrastructures essentielles, afin d'exiger que des praticiens titulaires d'un permis d'exercice réalisent les travaux touchant la protection publique quand la gestion de la sécurité et la conformité à la réglementation sont déléguées à des industries sous réglementation fédérale.

Contribution future d'Ingénieurs Canada

Ingénieurs Canada continuera de :

- Faire un suivi du programme, des initiatives législatives et des propositions de réglementation sur la cybersécurité du gouvernement pour porter à l'attention de celui-ci des recommandations sur les lois en lien avec la profession.
- Demander que les décideurs veillent à ce que les lois sur la cybersécurité conservent des mentions explicites des ingénieurs et du génie, dans l'intérêt de la sécurité du public dans l'ensemble du pays.
- S'efforcer activement de déterminer les possibilités d'exiger la participation des ingénieurs dans le cadre des lois et des règlements fédéraux lorsque cela est dans l'intérêt du public;
- Appuyer le travail effectué par les organismes de réglementation provinciaux et territoriaux pour faire appliquer les lois régissant la profession dans le cadre de l'exercice des disciplines qui ont un impact sur la sécurité publique.
- Par l'intermédiaire du Bureau canadien d'agrément des programmes de génie, conseiller les responsables des programmes de premier cycle en génie axés sur la cybersécurité quant à la façon de répondre aux normes d'agrément.

[1] The Economic Times (2019). "Definition of 'Cyber Security'." Consulté le 3 octobre 2019 à : https://economictimes.indiatimes.com/definition/cyber-security

[2] Sécurité publique Canada (2018). "Stratégie nationale sur les infrastructures essentielles". Consulté le 29 mai 2020 à https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-fr.aspx

[3] Statistique Canada (2018). L'incidence du cybercrime sur les entreprises canadiennes, 2017. Consulté le 8 juillet 2019 à https://www150.statcan.gc.ca/n1/daily-quotidien/181015/dq181015a-fra.htm.

55, rue Metcalfe, bureau 300, Ottawa (Ontario) K1P 6L5 (613) 232-2474 | government.relations@engineerscanada.ca | www.engineerscanada.ca