Rapport de la Section canadienne de l'Association parlementaire du Commonwealth

Atelier sur l'intelligence artificielle dans le domaine de la sécurité

Londres, Royaume Uni

Du 27 au 30 janvier 2025

Rapport

L'honorable Rosemary Moodie, sénatrice, vice-présidente de la Section canadienne de l'Association parlementaire du Commonwealth (APC), et l'honorable David Wells, sénateur, membre du comité exécutif, ont assisté à l'atelier sur l'intelligence artificielle (IA) dans le secteur de la sécurité en 2025, organisé par la Section du Royaume Uni (R. U.) de l'APC à Londres, au R. U., du 27 au 30 janvier 2025.

JOUR 1 – Groupe des cinq

La première journée de la conférence a été consacrée à des réunions entre les délégués des pays membres du Groupe des cinq présents. Les sénateurs Moodie et Wells ont ainsi eu l'occasion de discuter de questions importantes en matière de sécurité avec des parlementaires britanniques et néo-zélandais au cours de deux séances de travail.

Séance 1 : Stratégie et innovation

La réunion a porté sur les stratégies de défense des pays du Groupe des cinq et a abordé des thèmes tels que les dépenses de défense, l'approvisionnement et les investissements futurs. Les dépenses militaires ont augmenté dans les cinq régions géographiques, en grande partie en raison des tensions géopolitiques croissantes. Les participants ont examiné l'évolution du portrait de la défense dans ce contexte, notamment de la présence accrue de l'IA dans les systèmes d'armement. La discussion a mis en évidence les priorités fondamentales des pays du Groupe des cinq et de leurs alliés en matière de collaboration et d'innovation.

Séance 2 : Coopération internationale

La réunion a permis d'examiner l'évolution du Groupe des cinq et les possibilités de collaboration offertes à ses membres. Les délégués ont discuté des défis actuels en matière de sécurité nationale et internationale et ont échangé sur des questions communes et les pratiques exemplaires, notamment les lignes directrices pour assurer la sécurité à l'ère numérique. Les participants se sont également penchés sur l'importance que revêtent encore aujourd'hui les activités du Groupe des cinq (surveillance géographique et partage de renseignements).

JOURS 2 À 4 – Atelier parlementaire

L'atelier a réuni 30 parlementaires de 15 assemblées législatives du Commonwealth, représentant l'Afrique, les Caraïbes, l'Europe, l'Asie et le Pacifique. Les délégués se sont réunis à Westminster pour discuter de l'impact de l'IA sur la sécurité et la démocratie dans le monde.

Ils ont entendu un large éventail de conférenciers experts internationaux qui ont abordé les thèmes clés de l'atelier, à savoir la désinformation fondée sur l'IA, la cybersécurité, la défense et les cadres internationaux pour une gouvernance responsable de l'IA. En échangeant leurs expériences et leurs idées, les délégués ont exploré des stratégies pour contrer les menaces émergentes et renforcer la résilience démocratique face à l'évolution rapide des technologies.

PRINCIPAUX SUJETS ABORDÉS

- **Gouvernance et collaboration en matière d'IA**

Pendant l'atelier, la sénatrice Moodie a présidé un groupe de discussion sur le portrait actuel de la gouvernance nationale et internationale de l'IA. Au cours de la séance, les participants ont examiné différentes approches de la gouvernance de l'IA dans des contextes nationaux et multinationaux, en abordant les principales caractéristiques des différentes approches réglementaires, des initiatives politiques et des cadres de conformité, et en présentant les normes mondiales et les pratiques exemplaires.

Après avoir échangé avec des experts tout au long de l'atelier, les délégués ont reconnu l'importance croissante de la réglementation de l'IA à mesure que ses avantages sont de plus en plus reconnus, tout en soulignant les complexités et les défis liés à la mise en place d'une gouvernance efficace dans ce domaine en rapide évolution. Au cours des dernières années, l'attention mondiale s'est détournée des préoccupations liées à l'IA pour s'intéresser à ses avantages potentiels. Cette évolution souligne le besoin croissant d'une réglementation efficace. Le défi réside dans la complexité que représente la gouvernance de l'IA, car il semble peu probable qu'un accord sur la réglementation puisse voir le jour à l'échelle internationale.

Il a été souligné que l'IA offre de grandes possibilités pour l'innovation commerciale et la croissance économique; toutefois, il est essentiel qu'une réglementation soit mise en place pour garantir la protection des données et les droits d'auteur. Cela dit, il est tout aussi important que la réglementation ne freine pas la croissance et ne limite pas l'innovation.

Pour qu'un système soit bien réglementé, l'IA nécessite une approche de gouvernance polycentrique, combinant des instruments juridiques non contraignants, des accords contraignants et des normes de l'industrie. Il existe déjà un certain nombre d'instruments à caractère non contraignant axés sur l'IA comme les principes de l'OCDE sur l'IA, le processus de Hiroshima sur l'IA du G7 et la stratégie continentale africaine sur l'IA, qui permettent aux États de s'entendre plus rapidement. Toutefois, en raison du caractère non contraignant des instruments, de plus en plus de voix s'élèvent pour réclamer des obligations juridiques exécutoires afin de garantir le respect des règles et la reddition de compte.

Un autre défi réside dans la réglementation des puissantes entreprises technologiques, dont certaines exercent désormais une influence considérable sur les gouvernements nationaux et dont la valeur dépasse le produit intérieur brut de certains pays. Les États ont l'obligation de réglementer les entreprises relevant de leur juridiction et de veiller à ce qu'elles ne causent pas de préjudice. Toutefois, à mesure que les grandes entreprises technologiques continuent de gagner en influence, la probabilité que la réglementation s'améliore de manière significative peut varier d'une région à l'autre.

Certaines régions du Commonwealth sont confrontées à des défis supplémentaires en matière de gouvernance de l'IA, en particulier les pays qui ont une capacité limitée à renforcer leur expertise dans ce domaine. Dans bon nombre de ces pays, même lorsque les compétences sont perfectionnées, il y a souvent un exode des cerveaux, ce qui prive les pays d'une main-d'œuvre capable d'assurer la gouvernance. Par ailleurs, les contraintes financières peuvent entraver le développement de l'IA, ce qui pourrait conduire certains pays à se soumettre à des réglementations qui ne sont pas les adaptées à leur contexte.

La coopération internationale a été établie comme un mécanisme essentiel pour soutenir l'applicabilité et le respect des règles. Le bureau européen de l'IA, le bureau de l'IA des Nations Unies, le groupe de travail sur l'AI du Brésil, de la Russie, de l'Inde, de la Chine et de l'Afrique du Sud, le sommet sur la sécurité de l'IA du Royaume Unis, et le pacte numérique mondiale représentent tous des moyens utiles pour favoriser la collaboration et promouvoir le dialogue international. Même si un traité mondial général pourrait être difficile à faire accepter par tous les pays ou risquerait fort d'être affaibli, les initiatives mondiales et les lois régionales et nationales sont toutes essentielles, et le Commonwealth a un rôle important à jouer à cet égard.

Reconnaissant la nécessité d'un apprentissage continu à mesure que l'IA évolue, le Secrétariat du Commonwealth poursuit son travail approfondi dans le domaine, après avoir créé en 2023 un consortium du Commonwealth sur l'IA ainsi que quatre groupes de travail sur l'IA. Un incubateur d'IA ainsi qu'un mégafonds dédié à l'IA ont été établis afin d'encourager l'innovation et de mettre en place des infrastructures.

Si la voie vers une réglementation efficace de l'IA est semée d'embûches, il sera essentiel d'encourager la collaboration et l'apprentissage continu, ainsi que la mise en place de cadres adaptables afin de garantir que les pays soient en mesure de trouver un équilibre entre l'innovation et la protection des intérêts nationaux et mondiaux.

- **L'IA dans le domaine de la cybersécurité et de l'armée**

Les délégués ont entendu plusieurs conférenciers s'exprimer sur l'utilisation croissante de l'IA dans les domaines de la sécurité et de la défense, ainsi que sur les risques et les avantages que cela présente. À mesure que la technologie continue de se développer à un rythme effréné, l'IA devient une nouvelle composante de la défense, et de plus en plus de pays l'utilisent pour obtenir un avantage stratégique sur le champ de bataille. La guerre est de plus en plus influencée par les technologies numériques. Il est donc essentiel que les ministères de la Défense restent souples et prompts à s'adapter aux nouvelles technologies. Cependant, cette évolution s'accompagne également de vulnérabilités et de risques importants.

Chaque nouvelle capacité de l'IA comporte des risques pour la sécurité, d'autant plus que les développements deviennent plus complexes et plus vulnérables aux menaces. L'IA augmentera également le volume des cyberattaques à court terme, les acteurs malveillants agissant souvent de manière plus innovante que les gouvernements, en utilisant l'IA pour automatiser et intensifier les cybermenaces. L'IA augmente considérablement le risque d'attaques par rançonciel et par hameçonnage, en particulier après l'essor des cryptomonnaies, qui constituent une monnaie non retraçable.

L'IA est utilisée à la fois dans les cyberopérations offensives et défensives. Du côté offensif, elle peut faciliter la désinformation, l'hameçonnage et la création de codes malveillants. Dans le domaine de la défense, l'IA peut aider à repérer et à corriger les vulnérabilités, à analyser plus rapidement les données et les menaces, ainsi qu'à réduire la charge de travail des experts qualifiés en cybernétique, leur permettant ainsi de se concentrer sur des tâches plus complexes.

Les acteurs non étatiques, en particulier ceux qui ne disposent pas d'une expertise technologique avancée, ont de plus en plus recours à l'IA, ce qui donne lieu à des campagnes de désinformation et à des cybermenaces plus sophistiquées.

Ces problèmes ne se limitent pas aux États avancés sur le plan technologique; les pays du Commonwealth sont également confrontés à des défis pour faire face aux menaces en matière de cybersécurité. Si certains disposent déjà de lois connexes, beaucoup doivent se mettre à niveau et élaborer des lois. Par ailleurs, la question de savoir qui devrait être chargé de faire respecter les normes de cybersécurité, d'appliquer des mécanismes de reddition de compte et d'apporter un soutien aux victimes de cyberattaques reste à régler.

Du point de vue militaire, l'IA est en train de transformer la nature des conflits. Ne pas adopter l'IA présente un désavantage stratégique, mais des préoccupations éthiques subsistent. Même si l'IA peut être déployée, cela ne signifie pas nécessairement qu'elle doit l'être, et les pays devraient se demander si les systèmes et les armes reposant sur l'IA sont en mesure d'offrir la sécurité et la fiabilité requises sur le champ de bataille. Aussi, malgré les progrès technologiques constants, la surveillance humaine demeure essentielle. Même si l'IA peut améliorer la prise de décision, le personnel sur le terrain restera indispensable.

Un autre enjeu majeur lié à l'utilisation de l'IA dans le domaine de la défense concerne son rôle dans le traitement des données classifiées et du renseignement militaire. L'IA est un outil précieux pour dégager des tendances et analyser de grandes quantités de données, ce qui la rend très utile pour la collecte de renseignements. Toutefois, l'intégration de l'IA dans les espaces de données classifiées pourrait poser d'importants enjeux en matière de sécurité de l'information.

À l'échelle mondiale, il n'existe pas encore de processus établi par les Nations Unies régissant l'IA dans le domaine militaire. Bien qu'il y ait des discussions sur les armes autonomes, la cyberguerre et la guerre cognitive, les approches en matière de politique d'IA varient considérablement d'une région à l'autre, les petits États ayant particulièrement du mal à suivre la course à l'armement dans ce domaine en raison de leurs ressources limitées.

Pour relever ces défis, il faut adopter une approche proactive et collaborative afin de garantir que les pays non seulement atténuent les risques, mais exploitent également le potentiel de l'IA de manière responsable et efficace. Tout d'abord, les pays pourraient privilégier les investissements dans l'IA plutôt que de se contenter de réagir aux nouveaux développements. Le fait de courir après le progrès peut rendre les pays vulnérables face à des acteurs plus avancés en matière de technologies d'IA. De plus, en tant que problème mondial, la lutte contre les cybermenaces nécessite une réponse globale coordonnée. Les pays du Commonwealth aussi pourraient continuer à explorer les moyens de partager leurs recherches et leurs pratiques exemplaires afin d'améliorer la collaboration et la résilience en matière de cybersécurité. Enfin, les pays devraient continuer à reconnaître l'importance de la surveillance humaine. De nombreuses défaillances de sécurité sont dues à de simples erreurs, ce qui souligne la nécessité de disposer d'un personnel bien formé et de stratégies d'intervention efficaces. Les petites entreprises et le grand public doivent également être équipés pour se protéger, être

capables d'identifier les acteurs malveillants et d'atténuer les menaces. La culture numérique est essentielle, et les gouvernements devraient envisager de mettre en place des initiatives et des programmes visant à sensibiliser le public.

- **Désinformation et résilience démocratique**

Au cours des discussions avec les experts et les participants des groupes de discussion, les délégués ont reconnu la menace croissante que représente la désinformation générée par l'IA et ses conséquences profondes, tout en examinant les stratégies potentielles pour renforcer la résilience et la reddition de compte. L'essor de l'IA générative a rendu encore plus facile la diffusion d'informations trompeuses, telles que les hypertrucages et les médias manipulés, qui ont été et continuent d'être utilisés pour cibler des personnes dans le monde entier, en particulier les femmes. La hausse de la désinformation générée par l'IA entraîne une érosion de la confiance dans l'information, le public devenant de plus en plus sceptique à l'égard du contenu. Il est préoccupant de constater que ce scepticisme ne se limite pas au contenu généré par l'IA; le public se montre également de plus en plus sceptique à l'égard du contenu en ligne légitime, ce qui illustre la complexité croissante de la vérification de la crédibilité des informations et des médias.

La désinformation générée par l'IA peut nuire à la résilience démocratique en ciblant des personnalités clés et des groupes vulnérables, tels que les politiciennes, et en diffusant de faux discours qui influencent l'opinion publique. Les lois actuelles ne traitent souvent pas du rôle de l'IA dans la désinformation, et les stratégies des politiciens sur les réseaux sociaux s'avèrent souvent inadéquates, car elles ont été conçues avant l'essor de l'IA générative. L'absence de codes de conduite des partis politiques sur l'utilisation, le partage et la rediffusion de contenu généré par l'IA complique encore davantage la question de la reddition de compte.

Pour faire face à l'enjeu urgent et immédiat que représente la désinformation fondée sur l'IA, les parlementaires pourraient envisager une réforme législative visant à lutter contre le contenu préjudiciable généré par l'IA comme les hypertrucages. De même, afin de promouvoir la reddition de compte parmi les entreprises technologiques, les pays pourraient envisager de s'accorder sur des exigences uniformes obligeant les entreprises technologiques à lutter efficacement contre la désinformation.

Le renforcement des capacités des organismes de réglementation est également essentiel pour garantir leur capacité à lutter efficacement contre la désinformation. Les pays devraient donc veiller à ce que les organismes de réglementation disposent de ressources, d'expertise et de financement suffisants. Enfin, afin de promouvoir la résilience démocratique, les pays devraient veiller à ce que les commissions électorales et les partis politiques fournissent des directives claires aux membres et aux politiciens sur l'utilisation responsable des réseaux sociaux.

Pour répondre efficacement aux enjeux liés à la désinformation fondée sur l'IA, les décideurs politiques peuvent envisager toute une série de mesures stratégiques, notamment des réformes législatives, des cadres réglementaires plus stricts et des mesures de protection démocratique renforcées.

Parmi les principales approches, on compte les suivantes :

- **Réforme législative :** Adopter des lois pour lutter contre le contenu préjudiciable généré par l'IA comme les hypertrucages.
- **Réglementation technologique unifiée :** Les pays pourraient collaborer à l'élaboration d'exigences communes afin d'assurer la reddition de compte des entreprises technologiques en ce qui concerne la lutte contre la désinformation.
- **Renforcement des organismes de réglementation :** Veiller à ce que les organismes de réglementation disposent de ressources, d'expertise et de financement suffisants pour lutter efficacement contre la désinformation.
- **Engagement politique responsable :** Les commissions électorales et les partis politiques pourraient fournir des directives claires sur l'utilisation responsable des médias sociaux aux membres et aux politiciens.

Colonialisme numérique et dynamique du pouvoir dans le domaine de l'IA

Les délégués ont examiné les défis importants auxquels sont confrontés les États postcolonisés en matière de partage des données, soulignant souvent que les gouvernements et les institutions ne saisissent pas toujours pleinement les implications à long terme. Les États postcoloniaux fournissent sans le savoir des données gratuitement à de grandes entreprises technologiques, souvent sans reconnaître les effets néfastes que cela pourrait avoir. Il est impossible de savoir comment ces données sont utilisées ni qui est le plus touché. Les pays du Sud et les pays en retard sur le plan technologique sont les plus exposés, et comme la technologie évolue très rapidement, il est impossible de connaître toute l'étendue des dommages. L'essor de l'IA a également un effet néfaste sur l'environnement, car les centres de données utilisent d'énormes quantités d'eau, d'énergie et de terres. Les pays à faible revenu sont touchés de manière disproportionnée, beaucoup d'entre eux devenant des dépotoirs pour les déchets électroniques. Par ailleurs, la prévalence de l'homogénéisation numérique renforce la dépendance mondiale à l'égard des grandes entreprises technologiques des pays dominants, ce qui permet à ces entreprises d'exercer une influence croissante sur les décisions gouvernementales, tout en désavantageant les petits pays en limitant leur souveraineté numérique et leur compétitivité économique.

Tout comme les données, la main-d'œuvre migre des pays à faible revenu vers les pays à revenu élevé, les plateformes numériques exploitant la main-d'œuvre des pays à faible revenu, souvent sous prétexte de promouvoir le développement. Bien que l'IA puisse créer de nouveaux emplois et stimuler les économies, ces avantages profiteront aux pays qui ont déjà mis en place les infrastructures nécessaires. À l'heure actuelle, 66 % des pays du Commonwealth n'ont pas de stratégie en matière d'IA, et la mise en place d'une stratégie nationale nécessite des fonds importants. Cependant, le temps nécessaire à l'élaboration d'une stratégie est souvent suffisant pour que la technologie ait déjà évolué.

Pour répondre à ces enjeux et les atténuer, les pays du Commonwealth pourraient tirer parti d'une collaboration accrue sur cette question, en considérant la crise de l'IA comme un enjeu mondial plutôt que d'élaborer des stratégies individuelles en matière d'IA. Grâce à cette collaboration, qui représente 2,4 milliards de personnes, ils pourraient renforcer leur pouvoir de négociation et créer des ensembles de données plus compétitifs pour rivaliser avec les leaders de l'IA et les grandes entreprises technologiques. Cependant,

pour que cette approche fonctionne, la confiance mutuelle et la transparence entre les membres du Commonwealth seront essentielles.

De plus, en raison de leur histoire commune, les pays du Commonwealth partagent souvent des fondements juridiques, institutionnels et de gouvernance similaires. Conscient de cela, le Secrétariat du Commonwealth a créé une nouvelle boîte à outils sur l'IA afin d'aider les pays à élaborer des stratégies efficaces en matière d'IA. Le nouvel outil permet d'élaborer des stratégies en matière d'IA en beaucoup moins de temps, le délai de traitement de 9 à 12 mois passant à 6 jours. En tirant parti de cadres communs et en favorisant la collaboration, les pays du Commonwealth peuvent adopter une approche unifiée de la réglementation de l'IA, garantissant ainsi leur compétitivité tout en préservant leurs intérêts collectifs.

CONCLUSION

Grâce à leur participation à l'atelier, les délégués de l'Association ont eu l'occasion de faire part de leur expérience en tant que parlementaires canadiens et de découvrir les approches adoptées dans d'autres pays du Commonwealth en matière d'IA dans le domaine de la sécurité.

La délégation tient à remercier ses hôtes de la Section britannique de l'APC d'avoir organisé un atelier passionnant sur un sujet aussi pertinent. Les délégués souhaitent également remercier la Bibliothèque du Parlement pour les documents d'information préparés en vue de leur participation.

Dépenses de déplacement

Les dépenses de déplacement associées à cette activité se retrouvent dans le rapport financier de délégation. Ce rapport est disponible dans la section de divulgation financière du site Web de la Diplomatie parlementaire.

Respectueusement soumis,

Alexandra Mendès, députée

Présidente de la Section canadienne de

l'Association parlementaire du Commonwealth (APC)