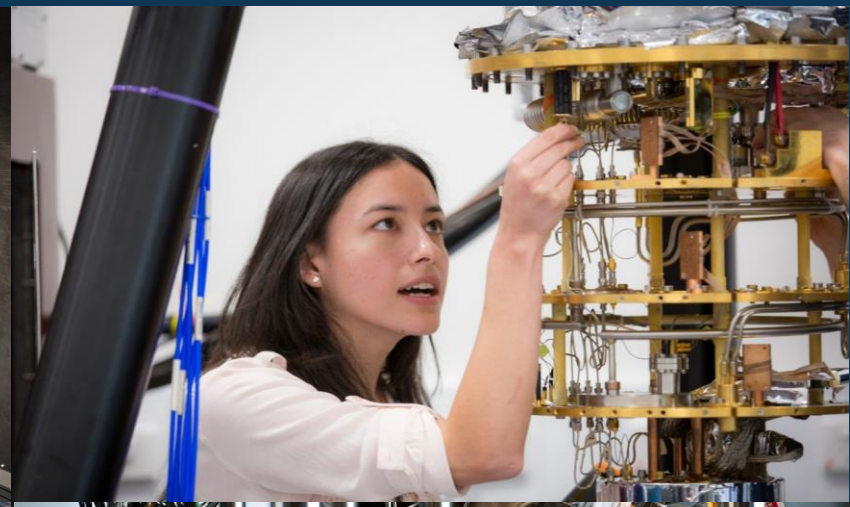
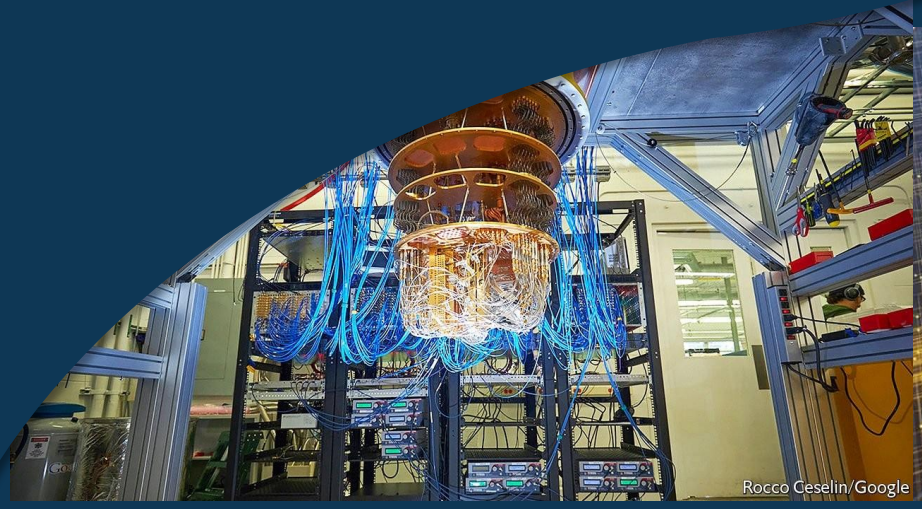
Citizen F1RST

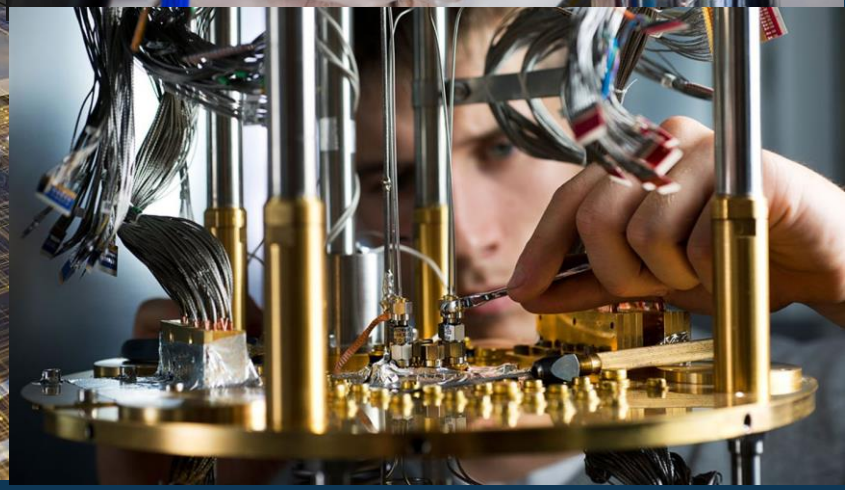
ANIMÉ PAR
l'Institut
des services axés
sur les citoyens

Informatique quantique 101

- Qu'est-ce que l'informatique quantique?
- Applicabilité pratique
- Avantages du gouvernement et de l'industrie
- Répercussions futures de l'informatique quantique







RAPPORT MENSUEL À L'INTENTION DES CADRES DES CONSEILS MIXTES

Élaboré par le Comité de recherche

Avril 2022

Images : Université de Sydney, New Scientist, India Times, Nature, IBM.com, Investable Universe.

1. Introduction et applicabilité

Un ordinateur quantique est un ordinateur qui utilise la physique quantique pour exécuter des calculs plus rapidement qu'un ordinateur traditionnel. Les qubits, qui sont des unités d'information, sont utilisés dans les ordinateurs quantiques pour effectuer des tâches. Contrairement aux « bits » traditionnels des ordinateurs, qui sont soit des 1 ou des 0, les qubits peuvent être l'un – ou les deux – en même temps. Ceci est crucial pour des vitesses de traitement beaucoup plus rapides, qui sont nécessaires pour modéliser la physique quantique au niveau moléculaire. **Comparée aux ordinateurs classiques, l'informatique quantique va faire un changement fondamental dans la vitesse, l'efficacité et la qualité de toutes sortes de calculs.** À l'heure actuelle, les ordinateurs quantiques commencent à être utilisés par :

- **IBM :** prévisions météorologiques en analysant une myriade de variables.
- **JPMorgan Chase :** calcul des contrats à options de prix et évaluation des risques dans le secteur bancaire et financier.
- **Microsoft :** calcul des processus chimiques et bactériologiques pour économiser l'énergie et réduire les émissions de CO2.
- **Daimler AG :** stimulation de la chimie cellulaire pour améliorer la longévité et la résilience des batteries dans les véhicules électriques.
- **ProteinQure :** découverte de médicaments par des molécules stimulantes et des processus moléculaires.
- **Post-Quantique :** amélioration ou piratage des algorithmes de cybersécurité.

L'informatique quantique a un énorme potentiel pour permettre une transformation massive du système. Il semble que la transition de l'informatique classique à l'informatique quantique sera plus importante que la transition de l'abaque à l'ordinateur standard. C'est l'une des raisons pour lesquelles les gouvernements du monde entier, y compris le Canada, continuent d'investir dans la recherche et le développement en informatique quantique. Ces efforts s'intensifient maintenant que la recherche quantique passe du domaine théorique au domaine pratique, comme le développement de l'intelligence artificielle (IA) il y a dix ans.

Depuis la fin des années 2010, les États-Unis et la Chine sont à l'avant-garde des investissements publics dans l'informatique quantique.

Pourquoi ce rapport est-il important?

- L'informatique quantique, qui est plus puissante que les ordinateurs classiques, a le potentiel de révolutionner le monde. Elle a le pouvoir de remodeler les services numériques, d'accélérer le traitement des données et d'ouvrir une nouvelle ère de communications et d'intelligence artificielle. Des entreprises comme IBM, Microsoft et Google rivalisent pour élaborer des ordinateurs quantiques fiables. La Stratégie quantique nationale, d'une valeur de 360 millions de dollars, a été lancée en 2021 par le gouvernement canadien pour stimuler l'innovation nationale.
- L'informatique quantique peut servir à relever les défis liés au changement climatique, aux soins de santé et aux résultats politiques axés sur les citoyens. L'informatique quantique fait encore l'objet d'essais sur son applicabilité et sa pertinence exactes à divers calculs que les gouvernements pourraient exiger. À l'heure actuelle, l'intérêt pour l'informatique quantique est partagé entre la technologie, le milieu universitaire, l'industrie et le gouvernement, créant des lieux de collaboration et de coopération.

Qu'est-ce qui est abordé dans ce rapport à l'intention des cadres?

Ce rapport comprend les suivants :

- Introduction et applicabilité
- Caractéristiques uniques des ordinateurs quantiques
- Avantages du quantum pour le gouvernement
- Répercussions futures de l'informatique quantique

Sources : « How Quantum Computing Could Change Financial Services. »; Quantum Computing 101; What Is Quantum Computing?

2. Caractéristiques uniques de l’informatique quantique

Dans les calculs effectués par un ordinateur quantique, toutes les possibilités sont réalisables, et il peut les traiter tous à la fois plutôt qu’en parallèle.

Les ordinateurs quantiques seraient si puissants pour certaines sortes de calculs complexes et massifs qu’un grand nombre d’ordinateurs traditionnels seraient autrement obligés de faire un travail équivalent.

« Si vous essayez de sortir d’un labyrinthe, vous arriverez à votre première porte, et vous pouvez aller à droite ou à gauche. Nous devons faire un choix, mais pas un ordinateur quantique. Il peut aller à droite et à gauche en même temps. »

Rebecca Krauthamer, PDG, Quantum Thought

"Les ordinateurs numériques utilisent la logique booléenne, le langage des 0 et des 1. Un ordinateur quantique le remplace par la loi quantique, ce qui accélère les opérations. Cela nous permet de faire certaines tâches avec moins d’étapes."

Hartmut Neven, fondateur du laboratoire quantique Google

« Une machine quantique est une sorte de calculatrice analogique qui calcule en encodant les renseignements dans les ondes éphémères qui comprennent la lumière et la matière à l’échelle nanométrique. »

David Reilly, Chercheur Microsoft

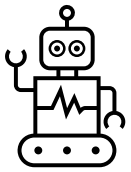
Sources : Quantum Computing : Everything You Need to Know; 20 Mind-Boggling Facts About Quantum Computing Everyone Should Read; More Possibilities Than There Are Particles In The Universe

Voici quelques-uns des faits et des chiffres les plus importants sur l’informatique quantique.

Le calcul quantique nécessite des températures extrêmement basses, car les particules subatomiques doivent être aussi proches d'un état stationnaire que possible pour être mesurées. Les coeurs des ordinateurs quantiques D-Wave fonctionnent à -460 degrés F, ou -273 degrés C, ce qui est juste 0,02 degrés au-dessus du zéro absolu.

La science-fiction semble devenir réalité à un niveau quantique. Les particules peuvent se téléporter (tunnellisation quantique) entre deux sites en se déplaçant vers l'arrière ou vers l'avant dans le temps.

Les univers parallèles pourraient être une explication au fonctionnement des ordinateurs quantiques. Parce que nous observons des qubits dans plusieurs univers en même temps, on a émis l'hypothèse qu'ils peuvent exister dans deux états en même temps.



D'ici 2028, des machines intelligentes pourraient émerger, capables d'accomplir n'importe quelle tâche que les humains pourraient accomplir. Les ordinateurs quantiques pourraient aider au développement d'une intelligence entièrement nouvelle.

3. Avantages du quantum pour le gouvernement

Même si l'utilisation de l'informatique quantique est limitée aujourd'hui, elle sera à l'avenir en mesure d'améliorer de manière significative tous les domaines d'activités gouvernementales où les ordinateurs actuels sont impliqués. Une collection de données qui prend des jours ou des mois à analyser maintenant, pourrait fournir des réponses en quelques secondes, accélérant les processus d'élaboration des politiques.

Les ordinateurs quantiques peuvent gérer un grand nombre de résultats possibles en même temps en raison de leur nature technique et de leur méthode de fonctionnement. Ces résultats dépassent ce qui est faisable avec la version la plus rapide d'un ordinateur classique.

Un ordinateur quantique peut résoudre une variété de problèmes, y compris les réactions chimiques dans les molécules et une meilleure compréhension de certains des questions entourant le changement climatique. Cela comprend des calculs budgétaires et une variété de conséquences politiques de tous les niveaux de complexité.

Sources : Quantum Computing Holds Promise for the Public Sector; What Is Quantum Computing and How Can It Help Feds?; Quantum Computing and Communications

Exemples d'applications possibles dans le secteur public

Efficiences

En renforçant le système dans son ensemble, la technologie quantique permettra aux gouvernements provinciaux et municipaux de tout améliorer, de l'affectation des ressources aux calculs budgétaires, en passant par une gamme d'autres opérations provinciales et locales. Le quantum est particulièrement efficace pour les problèmes liés à l'acheminement, à la logistique et à l'optimisation des ressources.

Les exemples locaux varient de l'acheminement le plus efficace des opérations d'urgence à l'orientation des ambulanciers jusqu'au lieu de l'accident. Il y a aussi les optimisations sophistiquées pour la sécurité publique au niveau fédéral avec des calculs complexes.

Cybersécurité

Les techniques de chiffrement seront obligées de changer à la suite des ordinateurs quantiques. Sur les superordinateurs les plus puissants, les méthodes actuelles sont fondées sur des méthodologies dont la résolution peut prendre des millénaires. Ce genre de problème peut être résolu en quelques heures ou jours sur un ordinateur quantique.

Le quantum peut aider les gouvernements à promouvoir la recherche de tactiques de chiffrement nouvelles et plus diversifiées pour défendre la sécurité nationale, puisque les ordinateurs quantiques peuvent être en mesure de casser tous les types de systèmes de chiffrement.

Science et technologie

Le quantum sera une force motrice dans tout, des prévisions météorologiques et l'analyse du changement climatique à l'amélioration des choix de traitement pour les pandémies comme la Covid-19 et la découverte de perspectives de recherche nouvelles et passionnantes.

Pour tous les ordres de gouvernement, les laboratoires, les instituts spéciaux pour l'innovation en soins de santé, et plus encore, les possibilités sont infinis.

Services financiers

Il sera plus facile d'évaluer les collections de données volumineuses ou non structurées pour les acteurs financiers. Une meilleure compréhension de ces domaines pourrait améliorer la prise de décision, le service à la clientèle et l'analyse des politiques. Les marchés des capitaux, la finance nationale, la gestion de portefeuille et les opérations liées au chiffrement sont tous des cas d'application convaincants.
Les ordinateurs quantiques sont particulièrement utiles lorsque les algorithmes sont alimentés par des flux de données en direct avec une grande quantité de bruit aléatoire, comme les prix des actions en temps réel.

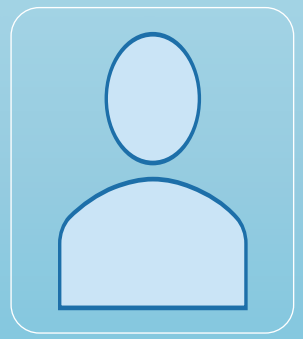
4. Limites actuelles de l'informatique quantique

La nature fragile des renseignements quantiques nécessite des installations compliquées et coûteuses pour héberger les ordinateurs quantiques. La plupart des systèmes quantiques ne peuvent fonctionner que dans des environnements de type vide plus froids que l'espace profond. Cela nécessite l'installation de réfrigérateurs spécialisés et énergivores dans les laboratoires. Certains systèmes quantiques sont créés avec des matériaux rares, posant des problèmes éthiques et environnementaux.

Les chercheurs du monde entier avancent dans la résolution de certains des obstacles techniques les plus persistants de l'informatique quantique, aussi intimidants qu'ils puissent paraître. Les processeurs quantiques pourraient bientôt fonctionner à des températures plus normales, grâce à des recherches récentes, et des codes de correction d'erreurs quantiques sont déjà en cours de création.

Le paysage du développement quantique est très diversifié, avec de nombreuses parties prenantes, des nations et même des disciplines qui contribuent à des solutions uniques.

Sources : Quantum Computers : Limits, Options, and Applications; The Limits of Quantum; Limitations in Quantum Computing from Resource Constraints; Quantum Computing: What It Is, Why We Want It, and How We're Trying to Get It



Difficultés techniques

Même si le potentiel de l'informatique quantique simple a été identifié pour la première fois dans les années 1980, il n'a pas encore été réalisé. L'ingénierie, la construction et la programmation des ordinateurs quantiques sont des questions complexes. Par conséquent, il y a des défauts comme le bruit, les dysfonctionnements et la perte de cohérence quantique, ce qui provoque la panne des ordinateurs quantiques.

Qualité des qubits

Les ordinateurs quantiques fondés sur le nuage d'aujourd'hui, avec leurs quelques qubits, sont insuffisants pour les systèmes à grande échelle. Lorsqu'ils effectuent des opérations entre deux qubits à un rythme beaucoup plus élevé que ce dont nous aurions besoin pour réussir le calcul, ils produisent néanmoins des erreurs. Il faut faire davantage de recherches pour déterminer les meilleures conditions requises pour obtenir des réponses correctes.

Correction d'erreurs

Des algorithmes de correction d'erreurs sont nécessaires pour vérifier et corriger les erreurs de qubit aléatoires au fur et à mesure qu'elles surviennent, car les qubits ne sont pas assez bons pour l'échelle nécessaire à leur fonctionnement. Même si la correction des erreurs dans l'informatique quantique n'a pas encore été présentée comme une image complète, elle reste un domaine de recherche prioritaire pour de nombreux pays.

5. Considérations futures pour l'utilisation de l'informatique quantique

Une main-d'œuvre instruite aura besoin de talents pour maintenir la croissance et éviter un déficit de compétences si le Canada veut tirer parti des avantages économiques et politiques que peut procurer le quantum. L'éducation en mécanique quantique et en apprentissage automatique est indispensable pour encourager les étudiants du secondaire, du collège et des cycles supérieurs à exercer des professions dans ce domaine.

Il faudrait promouvoir davantage l'informatique quantique afin d'obtenir le soutien bipartisan de tous les ordres de gouvernement. Il faudrait plus que de simples dépenses matérielles pour donner vie à l'informatique quantique afin de répondre aux besoins en temps réel.

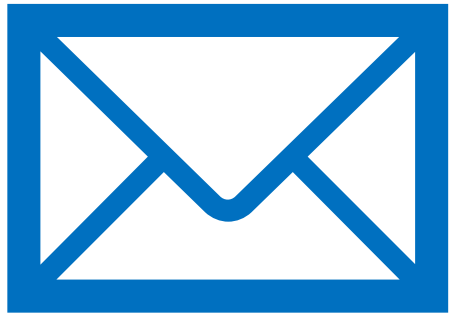
Tous les ordres de gouvernement peuvent promouvoir l'informatique quantique de diverses façons, non seulement pour améliorer la façon dont les villes et les provinces fonctionnent, et les percées en matière de sécurité des citoyens, mais aussi pour la croissance économique et l'efficacité qui profiteront à tous à long terme. Certains d'entre eux sont difficiles à comprendre maintenant.

Voilà toutes les raisons pour lesquelles la gouvernance quantique est importante pour l'avenir du secteur publique.

Étapes organisationnelles pour se préparer à l'ère quantique

Sensibiliser aux risques de sécurité du quantum.	L'informatique quantique constitue une menace pour les méthodes de cryptographie et de chiffrement existantes. Pour obtenir un vaste soutien pour investir dans une infrastructure de cryptographie à sécurité quantique, il est recommandé de transmettre ces renseignements à d'autres dirigeants d'entreprise au niveau du conseil d'administration, de la haute direction et des opérations.
Adopter une nouvelle approche de la gouvernance cryptographique.	Une difficulté technique majeure est la préparation des systèmes de cryptographie pour l'ère de l'informatique quantique. Une approche plus agile de la gouvernance cryptographique peut permettre de construire des entreprises plus flexibles qui peuvent rapidement pivoter et redéfinir les priorités en réponse à de nouvelles préoccupations en matière de sécurité, tout comme les principes de livraison de logiciels Agile contribuent à créer des équipes technologiques plus adaptables. Ce changement de mentalité peut conduire à une infrastructure cryptographique plus flexible et plus dynamique, capable de s'adapter aux défis et exigences changeants en matière de sécurité dans l'entreprise, l'industrie et la technologie.
Évaluer l'état de préparation de l'entreprise à devenir agile en matière de cryptographique.	Un organisme plus agile en cryptographie – capable de mettre à jour efficacement les algorithmes, les paramètres, les processus et les technologies cryptographiques pour mieux répondre aux nouveaux protocoles, normes et menaces de sécurité, y compris ceux qui utilisent des méthodes informatiques quantiques – peut être favorisé par une approche actualisée de la cryptographie.
Pratiquer une bonne hygiène cybernétique.	Être proactif dans le contrôle et l'élimination des risques de cybersécurité, comme toujours. Établir et maintenir de solides concepts et pratiques de base en matière de cybersécurité, ainsi que la connaissance de la situation des données, des infrastructures et d'autres actifs.

Sources : 5 Steps to Prepare Security for the Quantum Era; What Businesses Need to Consider Today for the Quantum Era



Lectures complémentaires

- Qu’est-ce que l’informatique quantique?
- What Makes Quantum Computing So Hard to Explain?
- Quantum computers and quantum supremacy, explained
- Quantum Computing: What It Is, Why We Want It, and How We're Trying to Get It
- Race Not Over Between Classical and Quantum Computers
- The Basics of Quantum Computing
- The Quantum Computing Era Is Here. Why It Matters—And How It May Change Our World.

Autres articles dignes de mention :

- "Quantum computing: how to address the national security risk“
- The Commercial Prospects for Quantum Computing
- Industry quantum computing applications
- Quantum Computing and the Ultimate Limits of Computation: The Case for a National Investment
- The road to quantum computing

Référentiel de recherche

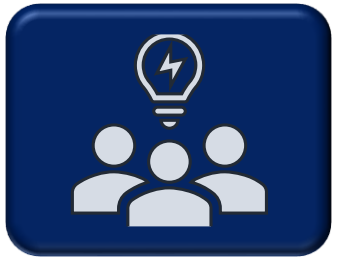
Accédez au référentiel de recherche de Citoyens en tête.

Entrées récentes dans le référentiel de recherche :

L’avenir du milieu de travail au gouvernement – Rapport exécutif du Conseil mixte de Mars 2022

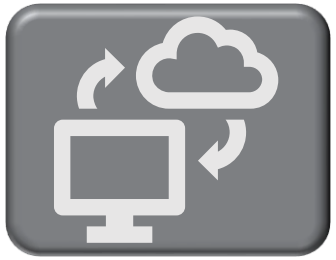
Le présent rapport comprend les éléments suivants : Tendances générales; Modèle de travail à partir de n’importe où; Principales considérations; Stratégies de préparation au milieu de travail de l’avenir.

Tendances dans le bulletin quotidien

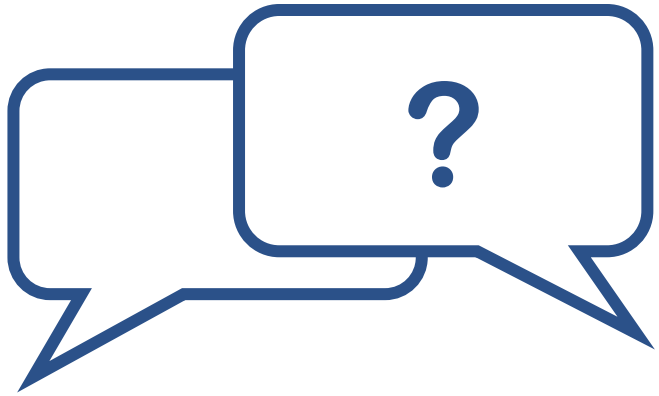


L'expérience des citoyens continue de représenter un intérêt majeur pour les organismes gouvernementaux afin d'améliorer leur propre efficacité. Les citoyens interagissent de plus en plus avec le monde par le biais de canaux numériques, ce qui implique de traiter les agences de la même manière. Ayant vu à quel point les choses peuvent être bonnes dans le monde commercial, leurs attentes ont augmenté en conséquence. Et lorsqu'ils constatent que les organismes rencontrent des défis en ce qui concerne les données qui les décrivent, leur confiance dans l'agence et le gouvernement en général peut diminuer.

Des initiatives d'identification numérique sont envisagées et élaborées par un éventail d'acteurs internationaux. Le gouvernement britannique, par exemple, a mené des efforts pour créer un système d'identification numérique qui peut permettre d'accéder aux services publics. Le nouveau programme représente un changement dans l'approche du gouvernement britannique. Il permettra aux utilisateurs de créer un compte gouvernemental pour accéder aux services en ligne. Cette initiative s'appuie sur une gamme de propositions antérieures et d'expériences internationales, et elle pourrait représenter une expérience d'apprentissage utile pour d'autres administrations.



Le Canada, le Mexique et les États-Unis ont l'occasion de forger un programme régional pour faire de l'Amérique du Nord un chef de file mondial dans le domaine des services gouvernementaux numériques. Ayant déjà établi une base solide pour la coopération, ces pays sont aujourd'hui encouragés à l'exploiter. Le gouvernement fédéral du Canada a rapidement mis au point un service de notification d'exposition à la COVID-19 sécurisé et a lancé le site Web « Trouver de l'aide financière pendant la COVID-19 », utilisé par des millions de Canadiens. Les gouvernements américain et mexicain ont lancé des initiatives similaires, qui peuvent toutes rapprocher l'Amérique du Nord d'une plus grande portée de l'intégration numérique.



Nous serons ravis d'entendre votre avis!

Connaissez-vous quelqu'un qui souhaite consulter le rapport exécutif des conseils mixtes? Veuillez partager une copie de ce rapport. Si vous n'êtes pas déjà abonné, vous pouvez maintenant vous inscrire pour recevoir le rapport. Veuillez faire parvenir vos questions à info@iccs-isac.org.

Suivre :