La menace quantique pour la cybersécurité : Danger et possibilité

Soumis à l'appui d'une présentation au Comité permanent de la sécurité publique et nationale sur la cybersécurité dans le secteur financier en tant que question de sécurité économique nationale

Michele Mosca, Brian O'Higgins et Bill Munson, Quantum-Safe Canada

22 février 2019

1. *La Stratégie nationale de cybersécurité du Canada et la menace quantique*

La stratégie de cybersécurité du Canada, *Stratégie nationale de cybersécurité : Vision du Canada pour la sécurité et la prospérité dans l'ère numérique* (juin 2018), souligne la nécessité de se préparer aux menaces de plus en plus complexes qui pèsent sur les cybersystèmes dont dépendent nos infrastructures essentielles et nos institutions démocratiques. La Stratégie engage le gouvernement (dans le présent contexte, les efforts de cybersécurité de ce dernier) à « se concentrer sur les domaines émergents d'excellence canadienne, comme l'informatique quantique ».

La plupart d'entre nous ont entendu parler de l'informatique quantique, savent qu'elle s'en vient, et sont conscients qu'elle permettra une accélération presque inimaginable de la capacité des ordinateurs à effectuer des calculs. Cela nous permettra de réaliser de grands progrès, par exemple en découvrant de nouveaux matériaux et en concevant de nouveaux médicaments qui sauveront des vies. Malheureusement, de puissants ordinateurs quantiques permettront également de pirater le chiffrement « indéchiffrable » d'aujourd'hui en quelques minutes.

Dans l'état actuel des choses, le chiffrement qui sous-tend la sécurité des infrastructures essentielles de la société risque sérieusement d'être miné par les ordinateurs quantiques au cours des huit à quinze prochaines années. Il s'agit de la menace quantique – que la sécurité nationale et la prospérité économique du Canada soient compromises alors que le gouvernement, les communications, les transports, les banques, l'énergie et d'autres systèmes critiques deviennent vulnérables aux actions hostiles parce que notre cryptographie n'est plus assez forte pour nous protéger. Même aujourd'hui, les mauvais acteurs peuvent copier et stocker des données chiffrées jusqu'à ce qu'un ordinateur quantique soit disponible pour les déchiffrer.

Nous expliquons ici comment la réalisation d'un Canada où règne la sécurité quantique est une pierre angulaire naturelle d'une stratégie canadienne visant à protéger les Canadiens et notre économie contre les cyberattaques, tout en récoltant les avantages économiques de ces efforts.

1. La menace quantique pour la cybersécurité

On reconnaît de plus en plus la nécessité pour la société de se préparer à faire face aux menaces de plus en plus complexes qui pèsent sur les cybersystèmes dont

dépendent nos infrastructures essentielles et nos institutions démocratiques. Cela nécessitera des investissements importants dans les outils, les services et les compétences en cybersécurité, y compris ceux nécessaires pour contrer la menace quantique.

En même temps, la cybersécurité n'est pas seulement un moyen de protection, mais aussi une importante source d'innovation qui contribuera à assurer la compétitivité. On demande aux gouvernements de concentrer leurs efforts sur le soutien des domaines émergents d'excellence locale, régionale ou provinciale; et au Canada, cela comprend de toute évidence l'informatique quantique.

2. Contrer la menace quantique

Le Canada doit réagir de façon proactive à la menace quantique en mettant en œuvre les éléments qui permettront une transition ordonnée et rapide vers la cryptographie résistant à l'informatique quantique. Si nous ne le faisons pas, notre sécurité et notre prospérité économique seront menacées alors que le gouvernement, les banques, l'énergie, l'intelligence artificielle et d'autres systèmes d'infrastructures essentielles deviendront vulnérables à des actions hostiles en raison de la faiblesse de la cryptographie.

La forme la plus courante de cryptographie, utilisée dans l'infrastructure à clé publique, est également la plus vulnérable. Il s'agit d'une source de grande préoccupation, car ses utilisations ont une importance universelle : validation des clés (de sorte que seules les parties visées ont accès à une communication ou à une opération particulière) et authentification par clé (de sorte que chaque partie à une transaction sache que les autres sont bien celles qu'elles disent être et que les messages sont légitimes). Sans de telles assurances, il n'y aura pas de confiance en ligne et peu de transactions, qu'elles soient effectuées par des êtres humains ou les appareils qui composent l'Internet des objets.

Le défi, c'est qu'une suite de rechange d'algorithmes cryptographiques évolués et testés contre l'informatique quantique n'est pas encore disponible. Les outils fondés sur ces derniers non plus. Il en va de même pour les experts en cybersécurité possédant des compétences en sécurité quantique qui utiliseront les outils pour diagnostiquer et réparer chaque système séparément. Sans une forte incitation à concentrer les efforts sur une campagne à long terme pour contrer la menace quantique, le Canada perdra du terrain à mesure que les vulnérabilités seront exploitées et que le potentiel de leadership mondial sera miné.

3. Solutions de sécurité quantique

Pour réagir efficacement à la menace quantique, il faudra nécessairement qu'un éventail d'intervenants travaillent ensemble pour trouver des occasions de traduire leurs recherches en produits innovateurs sans danger quantique. Une infusion de soutien financier ciblé pour les infrastructures et le personnel est nécessaire pour accélérer les

travaux de découverte, de mise à l'essai et de déploiement de solutions de sécurité quantique dans deux domaines : la cryptographie post-quantique et la distribution de clés quantiques.

3.1 Cryptographie post-quantique

La préparation à l'informatique quantique exige que de nouveaux algorithmes et outils cryptographiques résistants à l'informatique quantique soient découverts et développés pour remplacer ceux qui sont maintenant en place. En 2016, le *National Institute for Standards AMD Technology* (NIST) des États-Unis a lancé un projet pluriannuel visant à identifier un ensemble normalisé de systèmes cryptographiques viables et résistants aux ordinateurs quantiques d'ici 2024. L'annonce des normes du NIST pour la cryptographie post-quantique devrait permettre de réoutiller l'infrastructure des technologies de l'information et des communications dans le monde entier.

Les chercheurs canadiens participent activement à l'effort du NIST et ont contribué un certain nombre de candidats actuellement à l'étude. Ce sera à l'avantage économique à long terme du Canada si nos chercheurs participent de façon centrale à toutes les étapes du processus du NIST et au-delà, et leurs efforts devraient être encouragés et soutenus.

Les chercheurs et les technologues du Canada sont également à l'avant-garde du développement de logiciels et de services de cryptographie post-quantique, y compris des logiciels ouverts, des logiciels commerciaux et des services d'experts-conseils. En réponse aux progrès réalisés dans l'informatique quantique, les chercheurs devront poursuivre leurs travaux au fur et à mesure que des générations successives de cryptographie quantique sécurisée de plus en plus efficace seront déployées.

3.2 Distribution des clés quantiques

La recherche et le développement d'une distribution pratique de clés quantiques (DCQ) exigent des investissements importants dans les composantes physiques essentielles, comme les satellites et les stations au sol, ainsi que dans le personnel qualifié. L'objectif est un outil de DCQ évolutif et à l'épreuve de l'altération qui utilise les propriétés de la science quantique pour protéger l'importante validation des clés qui commence les transactions numériques.

Il est de toute évidence nécessaire que la DCQ soit intégrée dans un réseau réel d'ici trois à cinq ans. Cela permettrait de mettre à l'essai la DCQ avec un réseau national par satellite reliant des centres de collaboration individuels. Des travaux préliminaires sont déjà en cours dans des universités canadiennes. Non seulement certains des éléments physiques clés sont en place, mais des chercheurs clés se sont déjà regroupés et peuvent se mobiliser rapidement.

Ces chercheurs continueront d'innover pour rendre la DCQ plus efficace et moins coûteuse. Ce dont ils ont besoin, c'est d'un soutien financier supplémentaire pour

pouvoir accélérer ce travail afin de faire face à la menace imminente. Cela suppose probablement d'abord l'établissement de plusieurs centres de collaboration sur des réseaux distincts, les centres les plus probables étant :

- Calgary (près du secteur de l'énergie; à améliorer)
- Waterloo / Toronto (près du secteur financier et du gouvernement; à développer)
- Ottawa (près du gouvernement; à terminer)
- Québec (lié, par exemple, au secteur de l'aérospatiale ou de l'intelligence artificielle; à développer).

Les réseaux distincts seraient ensuite intégrés dans un seul réseau canadien fonctionnel de DCQ, qui pourrait éventuellement être relié à un réseau mondial de DCQ.

4. Élargir la base de compétences en sécurité quantique

La Stratégie nationale de cybersécurité reconnaît la nécessité d'accroître la capacité du Canada d'entreprendre les activités de recherche et de commercialisation nécessaires. Il faut prendre des mesures sérieuses pour renforcer et élargir la base de compétences du Canada, sans laquelle les aspects souhaités de la cybersécurité, soit la protection et le développement économique, ne peuvent être atteints.

Il faudra mettre en place des programmes et des cours de formation professionnelle pour que le Canada dispose du cadre nécessaire d'experts en cybersécurité possédant des compétences supérieures en matière de sécurité quantique. Ces experts exécuteraient des tâches telles que l'évaluation des risques cybernétiques et l'intégration des systèmes afin de s'assurer que les solutions de sécurité quantique appropriées ont été correctement installées et intégrées aux systèmes existants complexes.

Il faudra plusieurs années pour développer le vaste bassin nécessaire d'intégrateurs de systèmes et de consultants en cybersécurité possédant de solides compétences en matière de sécurité quantique. Un certain nombre de collèges canadiens ont manifesté leur intérêt à accroître leurs programmes de cybersécurité grâce à des cours axés sur la migration vers la cryptographie post-quantique. Idéalement, ils collaboreront à un module standard de sécurité quantique qui sera intégré aux programmes de cybersécurité existants.

En outre, il faudrait explorer les possibilités de sensibilisation auprès de l'industrie. Il est probable qu'il y ait un intérêt pour des cours de formation visant à familiariser le personnel technique avec les technologies de sécurité quantique et la meilleure façon de travailler avec des experts externes de la sécurité quantique. Il faudra également mettre en place des systèmes de certification permettant d'évaluer la qualité de la formation et l'expertise du stagiaire.

Bien que l'éducation soit une responsabilité provinciale, le gouvernement fédéral doit jouer des rôles stratégique et financier pour s'assurer que les provinces et les territoires (ainsi que les organismes et les organismes de réglementation qu'ils contrôlent) agissent avec un sentiment d'urgence.

5. Utilisation des leviers de la politique gouvernementale

Les gouvernements ont accès à de nombreux pouvoirs politiques qui peuvent être utiles pour encourager et même assurer la conception, la construction et l'installation d'infrastructures numériques, comme les routes intelligentes, les ponts intelligents et les villes intelligentes, axées sur la sécurité quantique. Ces leviers comprennent les pouvoirs d'approbation, de planification, d'approvisionnement et de financement, dont aucun n'a besoin d'être coûteux.

Un exemple simple serait une politique fédérale selon laquelle toute proposition de soutien fédéral à un projet d'infrastructure doit être accompagnée d'une stratégie de cybersécurité. Cela comprendrait nécessairement une stratégie de sécurité quantique pour les infrastructures qui devraient être en service pendant des décennies.

6. Profiter des possibilités de leadership canadien

Comme il a été mentionné précédemment, la Stratégie nationale de cybersécurité insiste sur la nécessité de se préparer à faire face aux menaces de plus en plus complexes qui pèsent sur les cybersystèmes. En même temps, elle souligne que la cybersécurité n'est pas seulement un moyen de protection, mais aussi une importante source d'innovation qui aidera à assurer la compétitivité du Canada. Les deux côtés de la médaille sont en jeu lorsqu'il s'agit de la menace quantique.

Le fait que le Canada est à l'avant-garde mondiale en matière de cryptographie et de science de l'information quantique, et fort en cybersécurité, joue en notre faveur. Il y a une longue tradition de collaboration entre ces domaines, alors nous devrions être en mesure de mettre de l'ordre dans nos affaires avant les autres pays, puis d'exporter nos produits et notre expertise sans danger quantique. La sécurité nationale et les perspectives économiques du Canada seront toutes deux améliorées si nous profitons de cette occasion.

La mise en œuvre des éléments clés susmentionnés permettra au Canada de tirer parti des possibilités d'innovation, de prospérité et de compétitivité qui sont inhérentes à une intervention rapide pour contrer la menace quantique. Un certain nombre de mesures complémentaires devraient également être prises à l'appui des éléments fondamentaux :

- Nommer un comité consultatif de scientifiques de haut niveau en cryptographie et en cybersécurité pour fournir des conseils d'expert sur les priorités et les paramètres de recherche pour les projets et les propositions.

- Déterminer l'expertise technique nécessaire pour surveiller les travaux d'élaboration de normes internationales pertinents et participer au besoin.

- Déterminer l'expertise en gestion de programme pour faire progresser les activités d'innovation et de commercialisation, effectuer des études de marché pour quantifier les exigences nationales et mondiales en matière d'expertise en sécurité quantique, et lancer des initiatives de développement des exportations liées à la technologie, à l'expertise et à la formation en matière de sécurité quantique.

Sans une forte volonté de concentrer les efforts sur une campagne à long terme pour contrer la menace quantique, le leadership mondial est miné. Nous ne pouvons pas nous permettre d'être des suiveurs, de faire face à des vulnérabilités de sécurité massives et à des coûts de mise à niveau prohibitifs simplement parce que nous avons tardé à agir. En même temps, nous ne devrions pas fermer les yeux sur les avantages économiques de la cybersécurité dynamique et des industries de sécurité quantique ni sur le danger de perdre notre avantage actuel si nous retardons l'action.

7. Liste de recommandations

- Que le Comité exhorte le gouvernement à insister sur la nécessité de répondre vigoureusement à la menace quantique. Sinon, notre sécurité, notre compétitivité et notre prospérité économique seront compromises lorsque le gouvernement, les banques, l'énergie, l'intelligence artificielle et d'autres systèmes d'infrastructures essentielles, y compris ceux qui soutiennent nos institutions démocratiques, deviendront vulnérables à des actions hostiles en raison de la faiblesse de la cryptographie.

- Que le Comité exhorte le gouvernement à réagir de façon proactive à la menace quantique, en mettant en place les éléments nécessaires pour que le Canada devienne résistant à l'informatique quantique de façon ordonnée et en temps opportun. Les principaux éléments qui demandent un soutien financier du gouvernement sont la recherche ciblée sur la cryptographie quantique sécurisée, le développement continu de la distribution de clés quantiques par satellite et la création d'un solide bassin de talents pour former le cadre nécessaire d'experts en cybersécurité possédant des compétences supérieures en matière de sécurité quantique.

- Que le Comité exhorte le gouvernement à utiliser les leviers politiques à sa disposition, y compris les pouvoirs d'approbation, de planification, d'approvisionnement et de financement, pour veiller à ce que les infrastructures numériques, comme les routes, les villes et les ponts intelligents, soient conçues et construites de manière à résister à la menace quantique.

- Que le Comité exhorte le gouvernement à fournir un financement approprié à une entité sans but lucratif qui est en mesure de lancer et de superviser les travaux à

multiples facettes nécessaires pour que le Canada mette en œuvre une stratégie robuste de sécurité quantique. Une telle stratégie doit à la fois assurer la sécurité de nos infrastructures essentielles et tirer parti des possibilités d'innovation, de compétitivité et de prospérité qui sont inhérentes à une intervention rapide pour contrer la menace quantique. Quantum-Safe Canada est disposé et capable de servir à ce titre.

Michele Mosca est un chercheur primé en cryptographie et en informatique quantique, et il a lancé de nombreuses collaborations multidisciplinaires qui ont contribué à créer l'occasion de sécurité quantique pour le Canada. Il a lancé et intensifié l'effort d'informatique quantique à Waterloo, et a fini par cofonder l'Institut d'informatique quantique (IIQ). Il a dirigé le premier réseau de recherche canadien en informatique quantique, il a piloté la création du programme d'études supérieures en informatique quantique à Waterloo et le Cours d'été en cryptographie quantique pour les jeunes étudiants (*Quantum Cryptography Summer School for Young Students*) destiné aux élèves du secondaire, a été membre fondateur de l'Institut Périmètre, a cofondé deux entreprises en démarrage et a cofondé la série d'ateliers sur la cryptographie quantique sécurisée d'ETSI-IIQ (*ETSI-IQC Quantum-Safe Cryptography Workshop*). Plus récemment, il a été cofondateur et directeur de Quantum-Safe Canada.

Brian O'Higgins est un investisseur providentiel et un membre du conseil d'administration comptant plus de 30 ans d'expérience en tant que chef de file du développement des technologies de sécurité. Il est peut-être surtout connu pour son rôle de pionnier dans l'infrastructure à clé publique et comme cofondateur et directeur de la technologie d'Entrust, une entreprise de sécurité Internet de premier plan. Il a également été cofondateur et directeur de la technologie de Third Brigade, une société de sécurité d'entreprise qui a été acquise par Trend Micro en 2009. Sa liste actuelle d'affiliations comprend des postes au sein de conseils consultatifs de Recherche et développement pour la défense Canada, des Centres d'excellence de l'Ontario et à titre de membre-cadre de Mistral Venture Partners. Il est également président du conseil d'administration de Quantum-Safe Canada.

Bill Munson est directeur, Recherche et analyse des politiques, à Quantum-Safe Canada. Avant de se joindre à Quantum-Safe Canada, cet analyste des politiques a passé plus de 20 ans à l'Association canadienne de la technologie de l'information, où il a mis sur pied et dirigé le très réputé Forum sur la cybersécurité de l'ACTI de 2000 à 2015.

Quantum-Safe Canada a été créé en 2017 pour sensibiliser la population à la menace quantique et pour aider à coordonner le développement de la recherche, de la technologie, des outils et de la formation nécessaires pour réussir la transition vers la cryptographie résistante à l'informatique quantique. Notre vision repose sur un double objectif : la sécurité et la prospérité.

Quantum-Safe Canada possède une base impressionnante de connaissances et de capacités, et s'est engagé à collaborer avec le gouvernement et d'autres intervenants pour réagir efficacement à la menace quantique imminente. Enregistré comme organisme sans but lucratif et doté d'un impressionnant conseil d'administration, d'un comité directeur universitaire et d'un conseil consultatif industrie-gouvernement déjà en place, Quantum-Safe Canada est particulièrement bien placé pour contribuer de façon significative aux efforts visant à assurer la protection des systèmes nationaux d'infrastructures essentielles et à faire en sorte que les capacités du Canada soient intégrées au leadership mondial et à l'avantage économique.