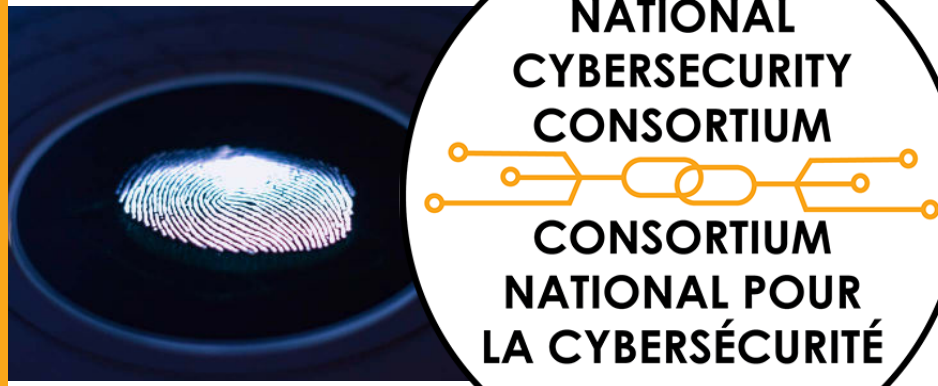


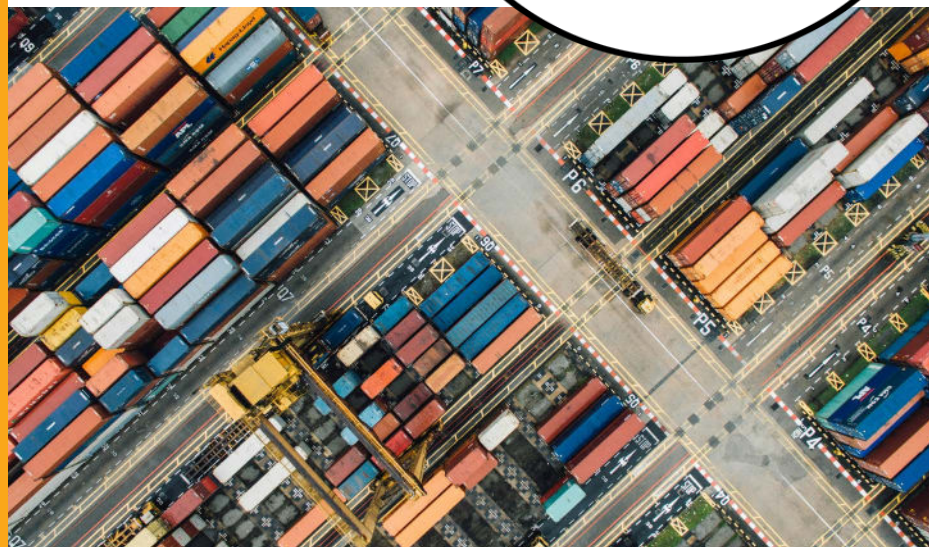




NATIONAL CYBERSECURITY CONSORTIUM

CONSORTIUM NATIONAL POUR LA CYBERSÉCURITÉ

Rapport annuel 2025-2026 du Consortium national pour la cybersécurité



Bâtir la souveraineté numérique du Canada par la

collaboration, l'innovation et le perfectionnement

Message de la présidente du conseil d'administration



Charmaine Dean, Ph.D.

Alors que le Canada assume son rôle de chef de file de confiance en cette époque marquée par l'expansion du secteur technologique, le développement de l'IA, la préparation à l'arrivée de l'informatique quantique et la surveillance, des prochaines percées exigent toutes une fondation en cybersécurité solide et pérenne. Le Consortium national pour la cybersécurité (CNC) est devenu un partenaire de premier plan pour le développement et la préparation du Canada en matière de cybersécurité.

Au cours de ses trois années d'activité, le CNC s'est montré un partenaire efficace et essentiel pour le soutien et le développement de l'écosystème de la cybersécurité au Canada ainsi qu'un membre respecté du Réseau d'innovation pour la cybersécurité (RIC). À ce jour, le CNC a engagé plus de 55 millions $ pour financer des programmes de recherche, de développement, de formation et de commercialisation en cybertechnologie de partout au pays.

Ces investissements, tout comme le développement actif de l'écosystème de la cybersécurité au Canada, ont fait partie intégrante de l'établissement d'un cadre de travail pour des solutions de cybersécurité souveraines au Canada.

Le CNC et son équipe se positionnent activement comme l'un des acteurs les plus indispensables et les plus dynamiques de l'écosystème de la cybersécurité au Canada. Sous la direction de notre directeur scientifique, Ken Barker, l'équipe offre des programmes efficaces et à fort rayonnement et a bâti un réseau pancanadien de membres experts en cybersécurité.

Je tiens à remercier mes collègues membres du conseil d'administration du CNC et toute l'équipe du CNC pour leurs services rendus à cet environnement stratégique et essentiel. Je souhaite également remercier le gouvernement du Canada et les ministères de l'Industrie et de l'Intelligence artificielle et de l'Innovation numérique pour l'attention portée à ce secteur vital. Au cours de la dernière année, votre dévouement et votre créativité ont été fondamentaux pour le succès du CNC et c'est pour moi un honneur de travailler avec vous.

Sincèrement,

Charmaine Dean

Conseil d'administration



Amir Belkhelladi
associé et leader national, services liés aux cyberrisques, Deloitte



Tim Evans, Ph.D.,
vice-recteur à la recherche, à l'innovation et au rayonnement, Université Concordia



William Ghali, Ph.D.,
vice-recteur à la recherche, Université de Calgary



Antoine Guilmain, Ph.D.,
co-chef, cybersécurité et protection des données, Gowling WLG



Elaine Hum
directrice, partenariats de cybersécurité, Scotiabank



Marc Kneppers
président et directeur général, Goldenrod Consulting

Conseil d'administration (cont.)



Emily Laidlaw, Ph.D.,
professeure agrégée et titulaire de la Chaire de recherche du Canada en droit de la cybersécurité, Faculté de droit, Université de Calgary



Steven N. Liss, Ph.D.,
vice-recteur à la recherche et à l'innovation, Université métropolitaine de Toronto



David MaGee, Ph.D.,
vice-recteur à la recherche, Université du Nouveau-Brunswick



Leon « Lee » Morris
Gestionnaire des projets de TI et chargé de cours principal pour la Joint Economic Development Initiative, Collège communautaire du Nouveau-Brunswick (CCNB)



Greg Murray
vice-président principal à la cybersécurité, à la vie privée et aux réseaux, Les Compagnies Loblaw Limitée



Olivera Zatezalo
responsable de la sécurité de l'information et vice-présidente à la cybersécurité et à la sécurité des TI, Ontario Power Generation

Message du directeur scientifique

du Consortium national pour la cybersécurité



Ken Barker, Ph.D

Le CNC a eu une année très productive! Nous avons tenu trois appels à proposition et noué des partenariats clés partout au pays qui continuent de faire avancer l'écosystème canadien de la cybersécurité.

Nous avons engagé 55 millions $ en financement dans 81 projets par l'entremise du Réseau d'innovation pour la cybersécurité (RIC). La communauté de la cybersécurité canadienne s'est engagée à verser une contribution équivalente à ce montant, ce qui nous permettra d'offrir un financement total de plus de 134 millions $ au cours des prochaines années. Ces projets continueront de soutenir le Canada et de protéger les Canadiens et les Canadiennes.

Cette année fut marquée par de nombreux changements pour le pays. On peut citer les investissements majeurs dans le secteur de la défense dans le cadre de la Stratégie industrielle de défense (SID) ainsi qu'un important engagement envers les technologies émergentes en intelligence artificielle et en informatique quantique du ministre de l'Intelligence artificielle et de l'Innovation numérique. La SID aura besoin de financement supplémentaire en cybersécurité pour protéger les systèmes de défense lorsque des troupes seront déployées ou pour protéger l'Arctique dans le cadre de nos efforts d'affirmation de la souveraineté nationale et pour devenir un chef de file mondial dans les domaines de la cybersécurité susceptibles de neutraliser les menaces pour le Canada. Les parties prenantes du CNC sont en bonne posture pour contribuer à cette dimension essentielle de notre sécurité nationale.

L'intelligence artificielle est une menace existentielle émergente pour les organisations des secteurs public et privé, notamment en ce qui a trait aux modèles d'intelligence artificielle et aux grands modèles de langage de pointe capables de découvrir des vulnérabilités encore inconnues dans divers systèmes. Cette menace a toujours constitué un défi pour la cybersécurité. Ce qui a changé, c'est la rapidité à laquelle des vulnérabilités peuvent être découvertes et les ressources pour y remédier rapidement afin de protéger les infrastructures critiques et les chaînes d'approvisionnement. Les modèles d'IA de pointe continueront à menacer la protection de la vie privée. À mesure que les modèles pionniers assimilent d'énormes quantités de données, nous devrons trouver des moyens de protéger le Canada et sa souveraineté numérique.

Les membres du CNC et leurs collaborateurs des secteurs privé et public sont impatients d'élargir leurs travaux pour répondre aux défis associés à ces deux nouveaux domaines prioritaires. Plus de 140 établissements d'enseignement supérieur et 200 organisations privées et à but non lucratif travaillent sur des projets financés par le CNC, sont motivés à relever ces nouveaux défis et possèdent l'expertise nécessaire pour obtenir des résultats très rapidement. Le CNC se réjouit à l'idée de collaborer avec ces parties prenantes dans le cadre de l'appel à proposition de 2027, qui ciblera ces défis émergents.

Le CNC est très reconnaissant de l'appui important du gouvernement fédéral, qui nous a permis d'atteindre nos objectifs et nous a aidés maintes et maintes fois à trouver des solutions pour que les choses se fassent. De même, je tiens à remercier l'ensemble de la communauté des experts en informatique de tous les secteurs pour leurs contributions au CNC, notamment pour leurs conseils, leurs examens des projets, leur appui aux demandes de financement et leur soutien moral alors que nous mettions sur pied le CNC.

Je souhaite également remercier notre conseil d'administration pour son engagement inébranlable à l'égard du CNC, pour ses objectifs et sa vision, ainsi que notre personnel qui continue de travailler dur pour établir une approche véritablement visionnaire pour répondre à un besoin fondamental au Canada. Votre vision, votre engagement et votre expertise permettront au CNC de prospérer et de diversifier sa proposition de valeur à l'intention de ses membres alors que nous entamons notre troisième année complète d'activité.

Sincèrement,

Ken Barker

APPEL À PROPOSITIONS
VUE D'ENSEMBLE

Réseau d'innovation pour la cybersécurité (RIC)

Années d'activité 2023 2024 2025

86 Projets financés

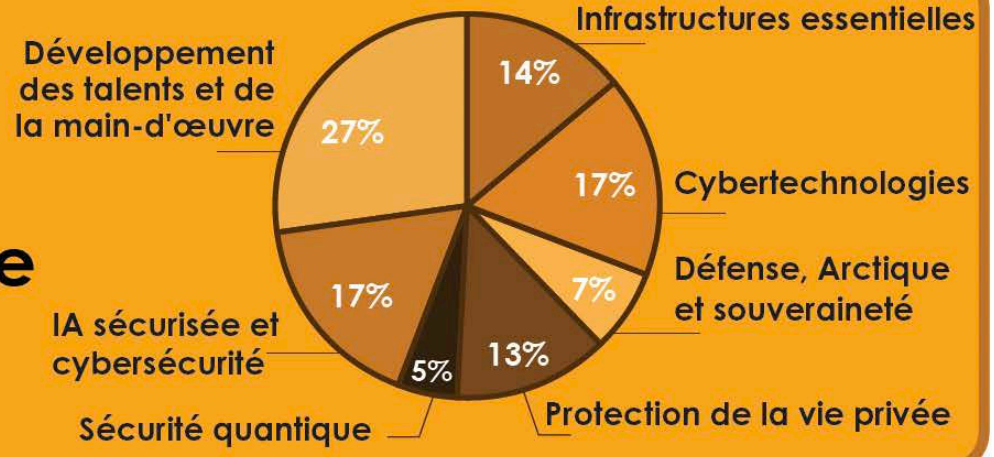
42 Bénéficiaires

453 Organisations partenaires

53,2 M$ Fonds distribués par le RIC

79 M$ Investissements des collaborateurs

Projets financés par thème



Projets financés par volet

63 Recherche

19 Formation

4 Commercialisation

Projets financés par secteur

70 Académique

3 Organismes à but non lucratif

13 Secteur privé

Projets financés et collaborateurs

Projets financés		Collaborateurs des projets	
Alb.	16	Alb.	70
C.-B.	10	C.-B.	33
Man.	0	Man.	4
N.-B.	5	N.-B.	18
T.-N.-L.	2	T.-N.-L.	4
N.-É.	2	N.-É.	11
T.N.-O.	0	T.N.-O.	0
Nt	0	Nt	1
Ont.	34	Ont.	175
Î.-P.-É.	0	Î.-P.-É.	0
Qc	16	Qc	102
Sask.	1	Sask.	9
Yn	0	Yn	1
		International	25

Appel à propositions

2025

En 2025, le CNC a engagé 20 998 698 $ en financement dans 31 nouveaux projets et en financement additionnel pour des projets déjà financés issus des appels à propositions de 2023 et de 2024. Ce montant porte le total des sommes investies à plus de 135 millions $ dans des projets de cybersécurité visant à soutenir l'innovation et l'amélioration des compétences dans le secteur de la cybersécurité au Canada.

Protéger l'avenir numérique du Canada

Le programme de financement du CNC a pour but de stimuler un écosystème national solide de cybersécurité et de positionner le Canada comme chef de file mondial en matière de cybersécurité. Depuis 2023, le CNC a financé trois catégories de projets du domaine de la cybersécurité : **commercialisation, recherche et développement et formation**. Ces projets s'inscrivent dans des secteurs variés qui correspondent aux cinq priorités du CNC : la protection des infrastructures essentielles, la cybersécurité centrée sur l'humain, la sécurité des réseaux, les technologies de protection de la vie privée et de renforcement de la confidentialité et la sécurité logicielle.

Le CNC a mis à profit l'appel à propositions de 2025 pour évaluer les besoins de financement de différents types de projets issus de l'écosystème de la cybersécurité au Canada. L'appel à propositions de cette année prévoit trois catégories :

Catégorie 1, projets accélérés : destinée à faire avancer rapidement des projets très ciblés et associés à un budget important;

Catégorie 2, nouveaux projets en 2025 : un appel à propositions pour des initiatives axées sur la cybersécurité et la protection de la vie privée;

Catégorie 3, financement additionnel pour les projets de 2023 et de 2024 : destinée à renforcer les résultats des projets déjà approuvés par le CNC en leur permettant d'intégrer de nouvelles idées ou de remédier aux lacunes identifiées lors des travaux menés jusqu'à présent.

Les projets ont été soumis à l'évaluation de plus de 35 experts sectoriels de l'écosystème canadien de la cybersécurité, répartis en huit sous-comités, puis à l'approbation du conseil d'administration du CNC.

Prochains appels à propositions

Le CNC et Innovation, Sciences et Développement économique Canada (ISDE) ont poursuivi leurs discussions au sujet de la continuité du soutien à l'écosystème de la cybersécurité, notamment en ce qui concerne un éventuel appel à proposition en 2027. Toutefois, en raison des changements apportés aux priorités du gouvernement, le renouvellement du programme du RIC demeure incertain.

Nous sommes extrêmement fiers des résultats obtenus par les projets que nous avons financés et nous nous engageons à continuer de travailler pour fournir un soutien pérenne aux talents futurs et à l'innovation.

Soutien et suivi après le financement

Nous fournissons aux bénéficiaires d'un financement des séances de soutien et d'information de manière trimestrielle pour les aider à produire leurs rapports. Nous continuons de rationaliser nos processus et de chercher des gains en efficience pour satisfaire aux obligations d'ISDE.

Projets financés en 2025

Projets accélérés

Commercialisation

Mise en marché de CYBERDEFENSE AI 2025-2027

Bénéficiaire : CYBERDEFENSE AI, Montréal, Qc

Collaborateurs : Cybereco

Fonds engagés : 142 250 $

Recherche et de développement

Fédération sécurisée des données de santé grâce au contrôle d'accès génératif

Bénéficiaire : Otekha Health Corporation, Kitchener, Ont.

Collaborateurs : Université de Toronto, Université de Calgary, Université de Waterloo, Université du Nouveau-Brunswick

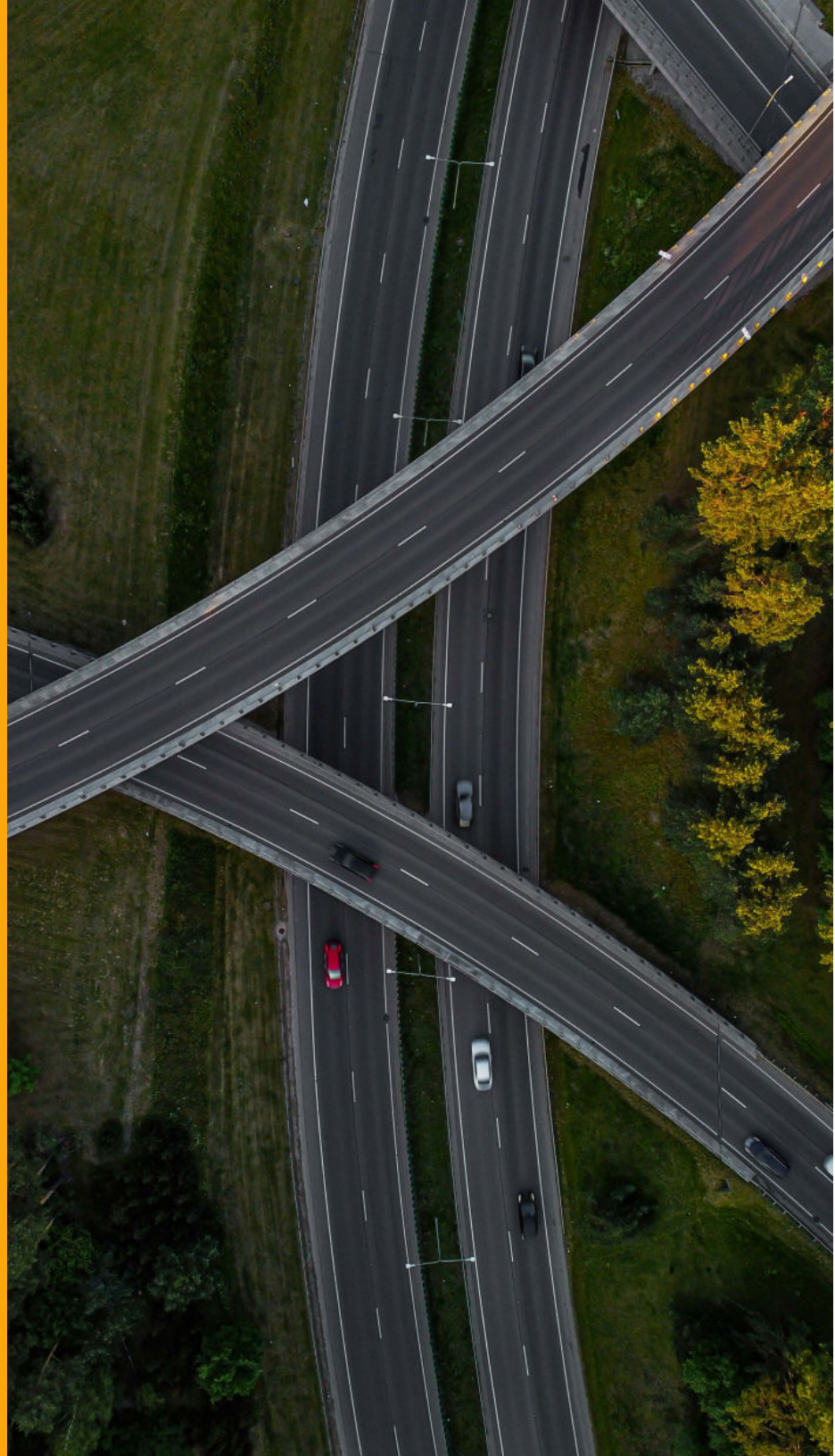
Fonds engagés : 2 384 650 $

Protection en enseignement supérieur en Alberta et au Nunavut avec des partenariats internationaux

Bénéficiaire : Cybera Inc., Calgary, Alb.

Collaborateurs : AARNet, Université de Calgary, Université de l'Alberta, Collège de l'Arctique du Nunavut

Fonds engagés : 2 500 000 $



Nouveaux projets

Recherche et de développement – de pointe

Votre attention s'il vous plaît : comment l'attention des employés influence le comportement en matière de cybersécurité

Bénéficiaire : Université de Waterloo, Waterloo, Ont.

Collaborateurs : Université du Delaware, TU Darmstadt

Fonds engagés : 223 529 $

Guerrier numérique

Bénéficiaire : Humber Polytechnic, Etobicoke, Ont.

Collaborateurs : White Bear Education Complex

Fonds engagés : 482 375 $

Risque cybersynthétique : une approche générative multiagent pour la prédiction de l'impact des cyberattaques avancées sur les écosystèmes d'entreprise

Bénéficiaire : Université de Guelph, Guelph, Ont.

Collaborateurs : Fortinet Canada, InCloud Security Inc., RiskView Inc, Toronto Community Housing Corporation, Université de Toronto, École de technologie supérieure Engineering, Université du Nouveau-Brunswick, Université de Brandon

Fonds engagés : 159 850 $

Sécurité de l'IA par auto-réparation à travers la génération autonome de correctifs et l'autovaccination des grands modèles de langage

Bénéficiaire : Université de Guelph, Guelph, Ont.

Collaborateurs : 3Tenets Consulting, eSentire Corp, ISACybersecurity Ltd, Wellington-Dufferin-Guelph Public Health, Université McGill, Université de la Saskatchewan, Université Dalhousie

Fonds engagés : 182 671 $


Canada
611
130611
ARC



Renseignements pilotés par l'IA sur les menaces l'IdO : sécurité des environnements intelligents travers les réseaux Zigbee, Z-Wave, Bluetooth et Wi-Fi

Bénéficiaire : Université Dalhousie, Halifax, N-É.

Collaborateurs : Université York, Solana Networks

Fonds engagés : 499 100 $

Système de gestion de batterie cyberrésilient avec flux d'énergie bidirectionnel sécurisé pour les véhicules connectés

Bénéficiaire : Institut universitaire de technologie de l'Ontario, Oshawa, Ont.

Collaborateurs : Université métropolitaine de Toronto

Fonds engagés : 500 000 $

Programmation différentielle et chiffrement totalement homomorphe sur les appareils périphériques connectés

Bénéficiaire : Université Simon Fraser, Burnaby, C.-B.

Fonds engagés : 494 115 $

Vulnérabilités et défenses des forums de discussion interactifs en ligne face aux interférences de l'IA générative

Bénéficiaire : Université de la Colombie-Britannique, Vancouver, C.-B.

Fonds engagés : 500 000 $

Sécurité de la chaîne d'approvisionnement des logiciels du Canada

Bénéficiaire : Université de Calgary, Calgary, Alb.

Collaborateurs : BoostSecurity.io

Fonds engagés : 470 588 $

Sécurisation des agents LLM contre les outils malveillants ou les vulnérabilités

Bénéficiaire : Université de Waterloo, Waterloo, Ont.

Fonds engagés : 254 116 $

Sécurisation des systèmes d'IA agentive tout au long du cycle de développement et d'exploitation

Bénéficiaire : École polytechnique de Montréal, Montréal, Qc

Collaborateurs : Université de Waterloo

Fonds engagés : 500 000 $

Détection des menaces à divulgation nulle de connaissance et évaluation des risques pour les infrastructures aérospatiales et orbitales

Bénéficiaire : Université McGill, Montréal, Qc

Collaborateurs : CAE Inc, Collège militaire royal du Canada, Université Queen's

Fonds engagés : 500 000 $

Modélisation des menaces et atténuation des vulnérabilités dépendant de facteurs humains dans les systèmes d'aide à la conduite avancés

Bénéficiaire : Université Western Ontario, London, Ont.

Collaborateurs : Acerta

Fonds engagés : 481 850 $

Efficacité et sécurité de la cryptographie à groupe d'ordre inconnu

Bénéficiaire : Université de Calgary, Calgary, Alb.

Collaborateurs : Pacific Institute for the Mathematical Sciences

Fonds engagés : 499 411 $

Détection fiable et explicable des logiciels malveillants

Bénéficiaire : Université de la Colombie-Britannique, Vancouver, C.-B.

Fonds engagés : 262 200 $

Surveillance de la géolocalisation

Bénéficiaire : Université de Calgary, Calgary, Alb.

Collaborateurs : Université York

Fonds engagés : 450 000 $

Cyberdéfense de pointe en IA quantique : des mesures de sécurité sans précédent pour les infrastructures essentielles

Bénéficiaire : Université de Calgary, Calgary, Alb.

Collaborateurs : IoTech Lab, Quantum City, Axiam Technology, Université Dalhousie, Pauli Group Inc

Fonds engagés : 500 000 $

Résilience post-quantique des systèmes électriques cyberphysiques

Bénéficiaire : Université métropolitaine de Toronto, Toronto, Ont.

Collaborateurs : ABB Canada, Hydro Québec – IREQ

Fonds engagés : 500 000 $

Recherche et de développement – standard

Cybersécurité, résilience et fiabilité des infrastructures essentielles et des actifs de mobilité aérienne avancée (AAM) en réseau en cas de cyberattaque malicieuse par un adversaire

Bénéficiaire : Université Concordia, Montréal, Qc

Collaborateurs : Université de Windsor, Université de l'Alberta, Université du Manitoba, VOZWIN Inc., HUMANITAS Inc.

Fonds engagés : 1 997 550 $

Plateforme jumeau numérique pour la modélisation et l'évaluation de la cybersécurité des infrastructures essentielles

Bénéficiaire : Institut de technologie de la Colombie-Britannique, Burnaby, C.-B.

Collaborateurs : BC Hydro, Siemens Canada, Awesense, Islay Power, EdgeTune Power, Fuse Power, EVECTRIX, Hydron Energy, Université polytechnique Kwantlen

Fonds engagés : 900 000 $

Analyse prescriptive et solutions agentives en matière de désinformation et d'attaques numériques

Bénéficiaire : Koat.ai Incorporated, Calgary, Alb.

Collaborateurs : FORESIGHT REPORTS, Alberta Innovates, ALTAML

Fonds engagés : 625 000 $

SECMAT : cybersécurité fondée sur les matériaux dans le secteur de l'électronique

Bénéficiaire : Université de Waterloo, Waterloo, Ont.

Collaborateurs : Palitronica, Wade Antenna

Fonds engagés : 2 000 000 $

Formation

Levez les boucliers : une plus grande cyberrésilience pour les petites entreprises

Bénéficiaire : Protexxa Inc., Aurora, Ont.

Collaborateurs : Institut universitaire de technologie de l'Ontario

Fonds engagés : 1 000 000 $

Programme de formation expérientiel en cybersécurité des infrastructures essentielles

Bénéficiaire : Institut de technologie de la Colombie-Britannique, Burnaby, C.-B.

Collaborateurs : BC Hydro, EdgeTune Power Inc., Fortis BC

Fonds engagés : 310 000 $

Programme de formation complet en cybersécurité avancée des réseaux 5G, des SCI/SCP et plus

Bénéficiaire : Université Concordia, Montréal, Qc

Collaborateurs : Institut universitaire de technologie de l'Ontario, Ericsson

Fonds engagés : 500 000 $

Promotion de l'excellence en matière de cybersécurité : des passerelles pour réduire les manques de main-d'œuvre et les écarts de compétences

Bénéficiaire : Digital Nova Scotia, Halifax, N-É.

Collaborateurs : Université de Waterloo, Université Saint-Francis-Xavier, Gouvernement de la Nouvelle-Écosse

Fonds engagés : 498 943 $

Première intervention contre les cybermenaces : une initiative collaborative de formation à la cybersécurité

Bénéficiaire : Université de Windsor, Windsor, Ont.

Collaborateurs : Sterling Information Technology, WE-Tech Alliance

Fonds engagés : 350 000 $

Préparation de la main-d'œuvre canadienne pour l'avenir de la cybersécurité à travers des parcours de formation et d'études

Bénéficiaire : Université Concordia d'Edmonton, Edmonton, Alb.

Fonds engagés : 330 500 $



Financement additionnel pour les projets de 2023-2024

PASCAL

Bénéficiaire : Palitronica, Waterloo, Ont.

Collaborateurs : Partenaires internes

Fonds engagés : 500 000 $

Mise en place de réseaux 5G cyberrésilients et sécurisés grâce à l'automatisation et à l'IA

Bénéficiaire : Université Concordia, Montréal, Qc

Collaborateurs : Ericsson

Fonds engagés : 500 000 $

Renforcer la cybersécurité : méthodes de détection précoce et d'atténuation des rançongiciels

Bénéficiaire : Université du Nouveau-Brunswick, Fredericton, N.-B.

Collaborateurs : Research NB Emerging fund – 2025

Fonds engagés : 25 000 $







Conférence inaugurale du CNC

25 au 27 juin 2025,

Centre des arts de Banff, Banff (Alberta)

La conférence 2025 du NCC a joué un rôle de point de convergence pour les experts et les leaders canadiens du secteur de la cybersécurité, lors de laquelle ceux-ci ont pu se réunir, échanger des idées, élargir leurs réseaux professionnels et cocréer des stratégies pour faire progresser l'écosystème de la cybersécurité au pays.

Cet événement, principalement sur invitation, s'adressait aux pionniers, aux chercheurs chevronnés et en début de carrière ainsi qu'aux partisans des technologies de pointe partageant une même volonté de faire progresser le domaine au Canada. Plus de 130 participants ont assisté à ces deux journées de tables rondes, de débats et d'ateliers. Le CNC a aussi organisé, avec le soutien de Mastercard, une compétition de capture du drapeau pour les étudiants d'établissements postsecondaires issus des programmes de cybersécurité ou de domaines connexes.

Les bénéficiaires de financement du CNC ont présenté des affiches portant sur leurs projets en cybersécurité et en protection de la vie privée. Cet événement fut une occasion unique pour les participants de découvrir les recherches récentes et en cours, les initiatives de formation et les projets de commercialisation menés au Canada. Le CNC a également tenu un événement de capture du drapeau destiné aux étudiants d'établissements postsecondaires canadiens.

CAPTURE DE DRAPEAU 2025

événement étudiant rendu possible par Mastercard

25 juin 2025, à distance et en présentiel au Centre des arts de Banff, à Banff (Alberta)

Le CNC a tenu sa première compétition de capture du drapeau, propulsée par la plateforme ENFOCOM Cyber et rendue possible par Mastercard. Cet événement hybride, qui a eu lieu au Centre des arts de Banff en Alberta, a rassemblé 25 équipes composées d'un total de 78 étudiants.

Les équipes participantes, formées d'étudiants issus d'établissements postsecondaires canadiens, se sont affrontées pour des prix et pour décrocher les premières places du classement. Trois équipes issues d'écoles secondaires de l'Alberta ont participé dans une catégorie non compétitive et ont tenu tête avec brio aux étudiants postsecondaires tant sur le plan des compétences que des connaissances.

Compétitions de capture de drapeau Mastercard

présentées par le Consortium national pour la cybersécurité

En 2026, le CNC et Mastercard se sont unis à nouveau, cette fois pour organiser une série de compétitions de capture du drapeau aux quatre coins du pays. Ces compétitions offraient aux étudiants inscrits à un établissement postsecondaire canadien la possibilité de participer en personne ou à distance. Les défis au programme se voulaient une occasion pratique d'apprendre la cybersécurité pour les participants de tous les niveaux.

Région du Centre

samedi 7 février 2026

Équipes du Manitoba, du Nunavut, de l'Ontario et du Québec

Région de l'Est

samedi 28 février 2026

Équipes du Nouveau-Brunswick, de Terre-Neuve-et-Labrador, de la Nouvelle-Écosse, et de l'Île-du-Prince-Édouard

Région de l'Ouest

samedi 17 janvier 2026

Équipes de l'Alberta, de la Colombie-Britannique, de la Saskatchewan, des Territoires du Nord-Ouest et du Yukon

Finale nationale

mercredi 17 juin 2026

Équipes de partout au Canada

Événements à venir

L'écosystème canadien de la cybersécurité est diversifié et géographiquement diffus, ce qui rend difficile la constitution d'une masse critique suffisante pour tirer pleinement parti des résultats de la recherche. Le CNC a notamment constaté ces défis au vu du nombre limité de projets financés dans le volet « commercialisation » et du manque de fonds disponibles pour faire progresser des projets prometteurs à travers les différents niveaux de maturité technologique jusqu'à ce qu'ils soient prêts à être commercialisés.

La participation active aux activités du CNC offre aux parties prenantes l'occasion d'atténuer ces lacunes, de renforcer les liens au sein de l'écosystème et de créer de l'engouement autour des initiatives de commercialisation de la recherche et de l'innovation en cybersécurité et en protection de la vie privée au Canada. L'élargissement et la mobilisation de notre réseau de parties prenantes sont des objectifs clés pour atteindre la masse critique nécessaire à l'avancement des projets et pour multiplier les occasions de faire progresser les résultats de la recherche vers la commercialisation.





Rayonnement

Le CNC continue de développer sa stratégie de communication afin d'élargir son rayonnement et de renforcer son engagement au sein de l'écosystème canadien de la cybersécurité. Un nouveau site web, en cours de développement, fournira une vitrine améliorée pour faire connaître les programmes, les activités et l'incidence du CNC. Le CNC a également adopté une plateforme de marketing par courriel hébergée au Canada pour ses infolettres. Cette transition lui permet de se conformer à la législation canadienne en matière de protection de la vie privée et de lutte contre les pourriels, en plus de conserver les données des abonnés au Canada. Pour l'avenir, le CNC prévoit d'établir une présence sur la plateforme Gander Social dès son lancement afin d'accroître le nombre de canaux de communication avec les parties prenantes et pour diffuser de l'information au sein de l'écosystème.

Rapport sur la propriété intellectuelle et les partenariats

L'équipe de la propriété intellectuelle et des partenariats (PIP) fait le pont entre le CNC et les activités de cybersécurité au Canada et les principaux acteurs régionaux, sectoriels et institutionnels essentiels pour renforcer la résilience en matière de cybersécurité et de protection de la vie privée au Canada. Plus particulièrement, le travail de l'équipe PIP consiste à développer et à préserver la propriété intellectuelle canadienne. L'équipe PIP a également le mandat d'élaborer et de mettre en place des plans de renforcement des capacités qui s'inscrivent dans la mission du CNC, en collaboration avec le directeur scientifique du CNC, le Comité consultatif scientifique et de l'écosystème (CCSE), les membres du CNC et d'autres intervenants stratégiques. Quelques réalisations clés de l'équipe PIP en 2025-2026 :

- L'équipe PIP a mené des activités de recherche et de promotion dans le cadre d'événements consacrés à la cybersécurité, à la protection de la vie privée et à d'autres thèmes du secteur (par exemple : InCyber, CPSC, qConnect, webinaires, etc.). L'analyse résultante a mis en évidence un lien entre l'engagement de l'équipe PIP et les milieux de la recherche, de la politique et des affaires, lors d'ateliers, de conférences et d'actions de promotion stratégiques. Ces travaux ont également permis de mieux comprendre l'incidence de l'intelligence artificielle et de la défense sur la propriété intellectuelle, notamment en ce qui concerne les systèmes émergents et les technologies à double usage.

- Un des exemples illustrant les efforts déployés par l'équipe PIP est sa collaboration avec le Bureau d'assurance du Canada, qui visait à approfondir la compréhension et à explorer les possibilités de collaboration dans les domaines suivants : les marchés de la cyberassurance, la gestion des incidents de cybersécurité, la cyberagilité des PME et les nouvelles catégories de cyberrisques.

L'équipe PIP a donné deux ateliers :

- un atelier consacré à l'accélération de la cyberagilité des PME canadiennes a permis d'examiner les lacunes relatives à l'accès, à l'adoption et à l'utilisation des outils et des services de cybersécurité par les PME;

- un atelier consacré au capital-risque et à la commercialisation dans le domaine de la cybersécurité ayant pour but d'examiner comment le Canada pourrait mieux valider, financer et développer les entreprises de cybersécurité (par exemple : cadres de validation pour les technologies de pointe; occasions d'investissement de capital-risque en cybersécurité dans les milieux de recherche; l'investissement dans la cybersécurité dans le cadre d'une stratégie économique régionale).



Comité consultatif scientifique et de l'écosystème

Au cours de l'exercice 2025-2026, le CNC a élargi les compétences et le rôle stratégique du Comité consultatif scientifique et de l'écosystème (CCSE), afin de renforcer sa capacité à fournir des analyses sur les nouvelles tendances en cybersécurité, les défis liés à l'écosystème et les orientations futures de la recherche pour le Canada. Les domaines d'intérêt ciblés comprennent les défis posés par la cybersécurité renforcée par l'IA, la cybersécurité et les systèmes d'IA, la souveraineté numérique et les avenues d'innovation en lien avec la participation du ministère de la Défense nationale et des Forces armées canadiennes.

Le CCSE a été créé en 2025 et rassemble des experts en cybersécurité et en protection de la vie privée et des leaders issus du monde académique, du secteur privé, d'organisations à but non lucratif et des gouvernements. Le comité formule au CNC des conseils portant sur les besoins émergents de l'écosystème, les lacunes en matière de capacités, l'évolution des priorités en recherche et les domaines stratégiques de risque ou d'opportunité pour le Canada. Le CCSE aide également le CNC à comprendre l'évolution de la recherche, du bassin de talent, de l'innovation et des besoins opérationnels dans les différents secteurs de la cybersécurité au Canada. Le CCSE se rencontre deux fois par année, dont une lors de la conférence annuelle du CNC.

Les recommandations du CCSE se sont progressivement concentrées sur la manière dont le CNC peut renforcer le développement de l'écosystème après l'octroi de financement, améliorer la collaboration avec les acteurs opérationnels et favoriser des approches mieux coordonnées en ce qui concerne les priorités nationales en matière de cybersécurité. Une attention particulière était accordée aux liens de plus en plus étroits entre l'intelligence artificielle, la résilience en matière de cybersécurité, la sécurité nationale et la souveraineté numérique ainsi qu'à la manière dont ces tendances redéfinissent les capacités dont le Canada a besoin.

Pour soutenir ces objectifs, le CNC a élargi sa série d'ateliers réunissant des chercheurs, des professionnels, des représentants du gouvernement et des acteurs opérationnels afin de faire émerger des idées concrètes, de clarifier les priorités et de définir les pistes d'action. Ces ateliers sont destinés à renforcer les capacités du CCSE en soutenant une participation mieux structurée de l'écosystème et en traduisant les discussions stratégiques en actions concrètes.

Le CCSE continue d'agir à titre de conseiller stratégique pour le CNC en ciblant des collaborations à forte valeur ajoutée, des prochaines priorités de financement et des occasions d'améliorer la coordination de la recherche, des talents et de l'innovation créant de la valeur pour les Canadiens et les Canadiennes. De plus, le comité œuvre à établir des liens solides entre le CNC et des secteurs clés, tels que les gouvernements, les institutions publiques, les communautés responsables de la sécurité nationale et de l'application de la loi, le monde académique et le secteur privé.

Le CNC accorde une grande importance à la contribution des membres du CCSE et continuera, au cours de la prochaine année, à renforcer l'engagement du comité et à étendre son rayonnement au sein de l'écosystème afin de maximiser sa valeur stratégique tant pour le CNC que pour l'ensemble de l'écosystème canadien de la cybersécurité.

Équité, diversité, inclusion et accessibilité

Le CNC a pour conviction que c'est en s'appuyant sur la diversité des compétences, des points de vue, des expériences et des parcours des acteurs de l'écosystème qu'il pourra mener à bien sa mission et concrétiser sa vision. En 2025-2026, le CNC a fait une priorité de l'intégration des principes d'équité, de diversité, d'inclusion et d'accessibilité dans différents domaines de ses activités :

- Toutes les communications externes sont fournies dans les deux langues officielles et écrites dans une langue claire et accessible.
- Les déclarations de reconnaissance territoriale font l'objet d'une révision régulière et sont rédigées en concertation avec des experts locaux afin de garantir que le contexte, les points de vue et les considérations locaux soient dûment pris en compte et respectés.
- Les intervenants et les animateurs invités à participer aux conférences du CNC sont, dans la mesure du possible, choisis afin de représenter une diversité de profils.
- La compétition étudiante de capture du drapeau organisée par le CNC a été pensée avec un souci pour l'accessibilité, en offrant des possibilités de participation en présentiel et à distance. Les prochains événements seront également en modalité hybride. Des lieux seront prévus partout au Canada pour la participation en présentiel.

Membres

Le CNC a le privilège de pouvoir compter sur un noyau de membres qui font partie de l'organisation depuis ses débuts. Le nombre de ses membres a augmenté de manière importante pour atteindre 71 organisations membres pour l'année 2025-2026. L'adhésion de base au CNC est ouverte aux organisations du monde académique, du secteur privé et du secteur des organisations à but non lucratif.

Le CNC est reconnaissant de pouvoir compter sur un groupe de membres solide. Les organisations membres de base du CNC nous aident à soutenir le développement de l'écosystème canadien de la cybersécurité.

Le CNC tient à exprimer sa profonde gratitude à tous les membres adhérents pour l'année 2025-2026 pour leur soutien indéfectible :

Actua
Alacrity Foundation of B.C.
BAAR Technologies Inc.
CharliAI Inc.
Collège militaire royal du Canada
Cyber PNM Inc
Cybera Inc
Cyberdefense AI
Cybereco
DeepCode
Deloitte
Digital Moment
Digital Nova Scotia
École Polytechnique de Montréal
ENFOCOM International Corporation
Envisioning Labs eQualitie Inc
Ericsson Canada Inc.
ezSec Inc
Field Effect Software
Fields Institute
Flare Systems Inc.
Humber College
Institut de technologie de la Colombie-Britannique
Institut national de la recherche scientifique
Institut universaire de technologie de l'Ontario
Koat.ai Incorporated
Magnificus Software Inc
Manitoba Research Network
Mycroft Technologies Inc.
Otekha Health Corporation
Palitronica
Portage Cybertech Inc.
Protexxa Inc.
Quantized Technologies Inc.
Quantum Algorithms Institute
Redeemer College
Réseau d'expertise en éthique de données
RESTIV Technology Inc.
RISQ
Sheridan College
Skills for Change
Solsys Corporation
Southern Alberta Institute of Technology
Université de Calgary
Université Carleton
Université de la Colombie-Britannique
Université Concordia
Université Concordia d'Edmonton
Université Dalhousie
Université de Guelph
Université Laval
Université McGill
Université McMaster
Université Memorial de Terre-Neuve
Université métropolitaine de Toronto
Université du Nouveau-Brunswick
Université d'Ottawa
UQAM
Université Queen's
Université Québec Outaouais
Université de Regina, Faculté de génie
Université de la Saskatchewan
Université de Sherbrooke
Université de Waterloo
Université Western Ontario
Université de Windsor
Université Simon Fraser
Université York
West Island College Society of Alberta



Les bonnes personnes, les bonnes discussions, au bon moment.

Situation financière

L'exercice 2025-2026 marquait la deuxième année de mise en œuvre dans le cadre de l'accord de financement conclu avec ISDE. L'organisation a maintenant tout le personnel et les ressources requis pour prendre en charge la livraison des projets. Le montant des dépenses pour le personnel administratif du CNC s'élève à 3 161 948 $. Le CNC a octroyé 16 909 945 $ en financement issus des contributions d'ISDE à des projets approuvés dans le cadre des appels à propositions de 2023, 2024, et 2025. Toutes les contributions reçues d'ISDE en 2025-2026 ont été affectées et dépensées durant l'exercice en cours.

Les sommes recueillies en frais d'adhésion pour l'année s'élèvent à un montant de 1 007 486 $, duquel 834 384 $ a été déclaré à titre de revenu.

Le CNC fait l'objet d'un audit financier annuel réalisé par un auditeur indépendant. Le rapport a été approuvé par le conseil d'administration, après examen par le comité de vérification et des finances. L'audit financier pour l'exercice 2025-2026 a été réalisé en juin 2026 par BDO Canada S.E.N.C.R.L, qui a exprimé une opinion sans réserve. Les états financiers audités se retrouvent à l'annexe 1.

En outre, le CNC s'est conformé à toutes les obligations légales de déclaration et de paiement. Notre dévouement envers la transparence et la conformité témoigne de notre engagement à souscrire aux plus hautes normes de reddition de compte et de gouvernance.



NATIONAL CYBERSECURITY CONSORTIUM

CONSORTIUM NATIONAL POUR LA CYBERSÉCURITÉ

www.ncc-cnc.ca

Suivez-nous sur LinkedIn

Inscrivez-vous à notre liste d'envoi

Financé par le gouvernement du Canada

Canada

Annexe 1

Consortium national pour la cybersécurité

États financiers

Pour l'exercice terminé le 31 mars 2026

Table des matières

Rapport de l'auditeur indépendant	2 - 3
États financiers	
État de la situation financière	4
État de l'évolution de l'actif net (insuffisance)	5
État des résultats	6
État des flux de trésorerie	7
Notes complémentaires	8 - 10

Tél./Tel: 613-237-9331
Téléc./Fax: 613-237-9779
www.bdo.ca

BDO Canada s.r.l./S.E.N.C.R.L./LLP
180 Kent Street
Suite 1700
Ottawa ON K1P 0B6 Canada

Rapport de l'auditeur indépendant

Aux membres du
Consortium national pour la cybersécurité

Opinion

Nous avons effectué l'audit des états financiers du Consortium national pour la cybersécurité (le « consortium »), qui comprennent l'état de la situation financière au 31 mars 2026, et les états des résultats, de l'évolution de l'actif net (insuffisance) et des flux de trésorerie pour l'exercice terminé à cette date, ainsi que les notes, y compris le résumé des principales méthodes comptables.

À notre avis, les états financiers ci-joints donnent, dans tous leurs aspects significatifs, une image fidèle de la situation financière du consortium au 31 mars 2026, ainsi que de sa performance financière et de ses flux de trésorerie pour l'exercice terminé à cette date, conformément aux Normes comptables canadiennes pour les organismes sans but lucratif.

Fondement de l'opinion

Nous avons effectué notre audit conformément aux normes d'audit généralement reconnues du Canada. Les responsabilités qui nous incombent en vertu de ces normes sont plus amplement décrites dans la section *Responsabilités de l'auditeur à l'égard de l'audit des états financiers* du présent rapport. Nous sommes indépendants du consortium conformément aux règles de déontologie qui s'appliquent à notre audit des états financiers au Canada et nous nous sommes acquittés des autres responsabilités déontologiques qui nous incombent selon ces règles. Nous estimons que les éléments probants que nous avons obtenus sont suffisants et appropriés pour fonder notre opinion d'audit.

Responsabilités de la direction et des responsables de la gouvernance à l'égard des états financiers

La direction est responsable de la préparation et de la présentation fidèle des états financiers conformément aux Normes comptables canadiennes pour les organismes sans but lucratif, ainsi que du contrôle interne qu'elle considère comme nécessaire pour permettre la préparation d'états financiers exempts d'anomalies significatives, que celles-ci résultent de fraudes ou d'erreurs.

Lors de la préparation des états financiers, c'est à la direction qu'il incombe d'évaluer la capacité du consortium à poursuivre son exploitation, de communiquer, le cas échéant, les questions relatives à la continuité de l'exploitation et d'appliquer le principe comptable de continuité d'exploitation, sauf si la direction a l'intention de liquider le consortium ou de cesser son activité ou si aucune solution réaliste ne s'offre à elle.

Il incombe aux responsables de la gouvernance de surveiller le processus d'information financière du consortium.

BDO Canada s.r.l./S.E.N.C.R.L./LLP, une société canadienne à responsabilité limitée/société en nom collectif à responsabilité limitée, est membre de BDO International Limited, société de droit anglais, et fait partie du réseau international de sociétés membres indépendantes BDO.

BDO Canada LLP, a Canadian limited liability partnership, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms.

Responsabilités de l'auditeur à l'égard de l'audit des états financiers

Nos objectifs sont d'obtenir l'assurance raisonnable que les états financiers pris dans leur ensemble sont exempts d'anomalies significatives, que celles-ci résultent de fraudes ou d'erreurs, et de délivrer un rapport de l'auditeur contenant notre opinion. L'assurance raisonnable correspond à un niveau élevé d'assurance, qui ne garantit toutefois pas qu'un audit réalisé conformément aux normes d'audit généralement reconnues du Canada permettra toujours de détecter toute anomalie significative qui pourrait exister. Les anomalies peuvent résulter de fraudes ou d'erreurs et elles sont considérées comme significatives lorsqu'il est raisonnable de s'attendre à ce que, individuellement ou collectivement, elles puissent influer sur les décisions économiques que les utilisateurs des états financiers prennent en se fondant sur ceux-ci.

Dans le cadre d'un audit réalisé conformément aux normes d'audit généralement reconnues du Canada, nous exerçons notre jugement professionnel et faisons preuve d'esprit critique tout au long de cet audit. En outre :

- Nous identifions et évaluons les risques que les états financiers comportent des anomalies significatives, que celles-ci résultent de fraudes ou d'erreurs, concevons et mettons en œuvre des procédures d'audit en réponse à ces risques, et réunissons des éléments probants suffisants et appropriés pour fonder notre opinion. Le risque de non-détection d'une anomalie significative résultant d'une fraude est plus élevé que celui d'une anomalie significative résultant d'une erreur, car la fraude peut impliquer la collusion, la falsification, les omissions volontaires, les fausses déclarations ou le contournement du contrôle interne;
- Nous acquérons une compréhension des éléments du contrôle interne pertinents pour l'audit afin de concevoir des procédures d'audit appropriées aux circonstances, et non dans le but d'exprimer une opinion sur l'efficacité du contrôle interne du consortium;
- nous apprécions le caractère approprié des méthodes comptables retenues et le caractère raisonnable des estimations comptables faites par la direction, de même que des informations y afférentes fournies par cette dernière;
- Nous tirons une conclusion quant au caractère approprié de l'utilisation par la direction du principe comptable de continuité d'exploitation et, selon les éléments probants obtenus, quant à l'existence ou non d'une incertitude significative liée à des événements ou situations susceptibles de jeter un doute important sur la capacité du consortium à poursuivre son exploitation. Si nous concluons à l'existence d'une incertitude significative, nous sommes tenus d'attirer l'attention des lecteurs de notre rapport sur les informations fournies dans les états financiers au sujet de cette incertitude ou, si ces informations ne sont pas adéquates, d'exprimer une opinion modifiée. Nos conclusions s'appuient sur les éléments probants obtenus jusqu'à la date de notre rapport. Des événements ou situations futurs pourraient par ailleurs amener le consortium à cesser son exploitation;
- Nous évaluons la présentation d'ensemble, la structure et le contenu des états financiers, y compris les informations fournies dans les notes, et apprécions si les états financiers représentent les opérations et événements sous-jacents d'une manière propre à donner une image fidèle.

Nous communiquons aux responsables de la gouvernance notamment l'étendue et le calendrier prévus des travaux d'audit et nos constatations importantes, y compris toute déficience importante du contrôle interne que nous aurions relevée au cours de notre audit.

BDO Canada s.r.l./LLP
Comptables professionnels agréés
Ottawa (Ontario)
La 28 juillet 2026

Docusign Envelope ID: B081962B-1EF1-831F-80AE-AF883CCDF740

Consortium national pour la cybersécurité
État de la situation financière

31 mars	2026	2025
Actif		
Court terme		
Encaisse	**1 603 898 $**	1 516 381 $
Comptes à recevoir	**543 753**	191 492
Autres créances	**30 815**	76 710
Frais payés d'avance	**182 813**	100 375
Avances de projets	**7 785 647**	3 994 276
	10 146 926 $	5 879 234 $
Passif et actif net		
Court terme		
Créditeurs et frais courus (Note 2)	**351 435 $**	292 149 $
Subventions à payer - remboursements	**772 965**	1 303 926
Subventions à payer - bénéficiaires finaux	**76 684**	952 266
Subventions et adhésions reportées (Note 3)	**8 078 354**	2 999 526
Dû aux membres fondateurs	**115 000**	115 000
	9 394 438	5 662 867
Actif net		
Non affecté	**752 488**	216 367
	10 146 926 $	5 879 234 $

Au nom du Conseil d'administration :

Signed by: Dave MaGee 9C036B809005435... Directeur

Signed by: Charmaine B. Dean 41D0855C03A4474... Directeur

Les notes complémentaires font partie intégrante des états financiers.

Consortium national pour la cybersécurité
État de l'évolution de l'actif net (insuffisance)

Pour l'exercice terminé le 31 mars	2026	2025
Solde, début de l'exercice	**216 367 $**	(20 311)$
Excédent des produits sur les charges	**536 121**	236 678
Solde, fin de l'exercice	**752 488 $**	216 367 $

Les notes complémentaires font partie intégrante des états financiers.

Consortium national pour la cybersécurité
État des résultats

Pour l'exercice terminé le 31 mars	2026	2025
Produits		
Subventions (Note 3)	**14 449 040 $**	5 010 800 $
Adhésions (Note 3)	**834 384**	309 862
Intérêts et autres revenus	**78 270**	24 434
	15 361 694	5 345 096
Charges		
Programmes	**11 849 056**	2 573 147
Développement, prestation et administration de programmes	**2 958 296**	2 524 935
TVH non réclamante	**18 221**	10 336
	14 825 573	5 108 418
Excédent des produits sur les charges	**536 121 $**	236 678 $

Les notes complémentaires font partie intégrante des états financiers.

Consortium national pour la cybersécurité
État des flux de trésorerie

Pour l'exercice terminé le 31 mars	2026	2025
Flux de trésorerie liés aux activités de fonctionnement		
Excédent des produits sur les charges	**536 121 $**	236 678 $
Variations des éléments hors caisse du fonds de roulement:		
Comptes à recevoir	**(352 261)**	(117 410)
Autres créances	**45 906**	46 200
Frais payés d'avance	**(82 439)**	(74 029)
Créditeurs et frais courus	**59 276**	154 693
Subventions et adhésions reportées	**5 078 828**	1 485 534
Avances de projets	**(3 791 371)**	(3 994 276)
Subventions à payer – récipiendaires finaux	**(875 582)**	952 266
Subventions à payer – remboursements	**(530 961)**	1 303 926
	87 517	(6 418)
Flux de trésorerie liés aux activités d'investissement		
Changement au dû aux membres fondateurs	**-**	2 500
Augmentation (diminution) nette de la trésorerie	**87 517**	(3 918)
Encaisse, début de l'exercice	**1 516 381**	1 520 299
Encaisse, fin de l'exercice	**1 603 898 $**	1 516 381 $

Les notes complémentaires font partie intégrante des états financiers.

Consortium national pour la cybersécurité
Notes complémentaires

31 mars 2026

1. Méthodes comptables

Statut et objectif de l'organisme

Consortium national pour la cybersécurité (le « consortium ») est un organisme sans but lucratif constitué sans capital-actions en vertu de la Loi canadienne sur les organisations sans but lucratif le 3 mars 2020, en tant qu'organisation fondée par les membres avec une entente entre Innovation, Sciences et Développement économique Canada (ISDE) et le Consortium national pour la cybersécurité. Le consortium est un organisme sans but lucratif au sens de la Loi de l'impôt sur le revenu et, à ce titre, il est exonéré d'impôt.

Le mandat du Consortium est de faire progresser l'écosystème de la cybersécurité du Canada par la recherche et le développement, la commercialisation et la formation.

Référentiel comptable

Le consortium applique les Normes comptables canadiennes pour les organismes sans but lucratif.

Utilisation d'estimations

La préparation des états financiers exige que la direction procède à des estimations et pose des hypothèses qui ont une incidence sur les montants présentés au titre des actifs et des passifs et sur les montants comptabilisés au titre des produits et des charges pour l'exercice visé.

Comptabilisation des produits

Le consortium applique la méthode du report pour comptabiliser les apports. Les apports affectés sont comptabilisés à titre de produits de l'exercice au cours duquel les charges connexes sont engagées. Les apports non affectés sont comptabilisés à titre de produits lorsqu'ils sont reçus ou à recevoir si le montant à recevoir peut faire l'objet d'une estimation raisonnable et que sa réception est raisonnablement assurée.

Les adhésions sont comptabilisées à titre de produits au prorata dans l'exercice auquel elles se rapportent. Les montants recus d'avance relativement aux exercices ultérieurs sont comptabilisés à titre de produits reportés.

1. Méthodes comptables (suite)

Instruments financiers

Les instruments financiers dans des conditions de pleine concurrence sont comptabilisés à la juste valeur lors de la comptabilisation initiale.

Tous les autres instruments financiers sont comptabilisés au coût ou au coût amorti, déduction faite de toute perte de valeur. Les coûts de transaction liés à l'acquisition, a la cession ou à l'émission des instrument financiers sont passés en charges pour les instruments évalués à la juste valeur et sont inclus dans la valeur comptable des instruments évalués au coût amorti.

Les actifs financiers font l'objet d'un test de dépréciation lorsqu'il y a des indicateurs d'une perte de valeur. Lorsqu'un changement important dans le calendrier ou les flux de trésorerie futurs de l'actif financier est identifié, la valeur comptable de cet actif est réduite et le montant est constaté à titre de dépréciation dans le résultat net. La moins-value déjà comptabilisée peut faire l'objet d'une reprise dans la mesure de l'amélioration, pourvu qu'elle ne dépasse pas le montant qui aurait été constaté à la date de la reprise si la moins-value n'avait jamais été comptabilisée, et le montant de la reprise de valeur est comptabilisé en résultat net.

2. Créditeurs et frais courus

Le poste créditeurs et frais courus comprend des sommes à remettre à l'État de 33 299 $ (2025 - 49 344 $).

31 mars 2026

3. Subventions et adhésions reportées

	2026	2025
Subventions d'ISED reportées	**7 683 846 $**	2 740 844 $
Adhésions reportées	**394 508**	258 682
Solde, à la fin de l'exercice	**8 078 354 $**	2 999 526 $

	2026	2025
Solde, au début de l'exercice	**2 999 526 $**	1 513 992 $
Plus: subventions d'ISED reçues pendant l'année	**19 392 042**	6 438 316
Plus: adhésions reçues pendant l'année	**970 210**	367 880
Moins: subventions d'ISED constatées à titre de produits de l'exercice	**(14 449 040)**	(5 010 800)
Moins: adhésions constatées à titre de produits de l'exercice	**(834 384)**	(309 862)
Solde, à la fin de l'exercice	**8 078 354 $**	2 999 526 $

4. Dépendance économique

Le consortium a reçu 94% (2025 - 94%) de ses produits d'ISED. Si ce financement ne continue pas ou si le consortium ne peut pas le remplacer, le consortium ne pourrait pas continuer ses opérations au niveau actuel.

5. Instruments financiers

Risque de liquidité

Le risque de liquidité est le risque que le Consortium puisse rencontrer des difficultés à respecter ses obligations financières à leur échéance. Cela inclut le risque que, en raison de contraintes de liquidité opérationnelle, le Consortium n'a pas suffisamment de fonds pour régler les transactions à leurs dates d'échéance, soit contraint de vendre des actifs financiers à des prix défavorables, ou soit incapable de récupérer la pleine valeur des actifs financiers. Le Consortium est principalement exposé au risque de liquidité par ses créditeurs, les subventions à payer et les charges à payer. Ce risque a diminué par rapport à l'exercice précédent, puisque les soldes des comptes fournisseurs, des subventions à payer et des charges à payer ont diminué.

Risque de crédit

Le consortium est exposé au risque de crédit puisque tous ses comptes bancaires sont détenus auprès d'une seule institution financière. Il n'y a pas eu de variation dans le risque comparativement à l'année précédente.