COGNITIVE SECURITY
SÉCURITÉ COGNITIVE
CANADA

Perceive • Percevoir | Analyze • Analyser | Integrate • Intégrer

RAPPORT DE RECHERCHE

La sécurité cognitive au Canada

Analyse des systèmes humains, résilience civique, confiance publique et environnement informationnel numérique

Numéro du rapport	COGSECCAN RR-002-FR
Date de publication	Mai 2026
Préparé par	Sécurité Cognitive Canada
Classe d'information	Recherche d'intérêt public

Perceive / Percevoir • Analyze / Analyser • Integrate / Intégrer

Contrôle du document

Type de document	Rapport de recherche
Numéro du rapport	COGSECCAN RR-002-FR
Titre	La sécurité cognitive au Canada : analyse des systèmes humains, résilience civique, confiance publique et environnement informationnel numérique
Statut de publication	Diffusion publique
Préparé par	Sécurité Cognitive Canada
Version	v1.0-FR
Notes	Modèle maître de rapport de recherche

Résumé exécutif

L'environnement informationnel numérique du Canada est désormais une infrastructure civique. Il influence la façon dont les résidents reçoivent les alertes publiques, interprètent les conflits politiques, comprennent les conseils de santé et de sécurité, accèdent aux services, évaluent les preuves et décident à qui faire confiance. La sécurité cognitive désigne la pratique d'intérêt public qui vise à protéger les conditions permettant aux personnes et aux institutions de percevoir, d'analyser et d'intégrer l'information avec intégrité. Elle ne remplace pas la cybersécurité, la sécurité publique, l'éducation aux médias, le droit de la vie privée ou la sécurité nationale. Elle offre plutôt un cadre de systèmes humains qui relie ces domaines autour d'une même question : comment les systèmes d'information influencent-ils l'attention, l'interprétation, le jugement, le comportement et la confiance publique?

La nécessité d'un cadre national de sécurité cognitive est visible partout au Canada. L'Évaluation des cybermenaces nationales 2025-2026 du Centre canadien pour la cybersécurité indique que le Canada fait face à un paysage de cybermenaces de plus en plus vaste et complexe, incluant des acteurs étatiques et non étatiques qui ciblent les infrastructures essentielles et la sécurité nationale. La même évaluation souligne que des cyberopérations combinées à des campagnes d'information en ligne peuvent servir à perturber, diviser, intimider et orienter l'opinion publique [1]. La couche cognitive devient donc centrale pour la sécurité : l'effet recherché n'est pas seulement le vol de données ou la perturbation d'un système, mais aussi une transformation de la confiance, de la perception et du comportement collectif.

L'ingérence étrangère, la polarisation intérieure, l'IA générative, les médias synthétiques, les systèmes de recommandation, la publicité ciblée, les interfaces trompeuses, la cybercriminalité et les défaillances de communication institutionnelle influencent toutes la manière dont les Canadiennes et les Canadiens interprètent la réalité. La Commission sur l'ingérence étrangère a conclu que les institutions démocratiques canadiennes demeurent robustes, tout en avertissant que la désinformation représente l'une des menaces les plus sérieuses pour la démocratie et la confiance du public [2]. Cette conclusion révèle un écart pratique : le Canada dispose d'institutions pour la cyberdéfense, les élections, la vie privée, l'application de la loi, la protection des consommateurs, le renseignement et les communications publiques, mais il ne possède pas encore de vocabulaire civique largement partagé pour décrire les effets interprétatifs humains qui relient ces domaines.

Le présent rapport propose la sécurité cognitive comme cadre canadien calme, non partisan, civique et analytique. Son objet n'est ni la censure, ni la surveillance, ni le contrôle des croyances. Son objet est la

conscience situationnelle, l'intégrité décisionnelle, la transparence institutionnelle et la résilience face à la manipulation. Une approche canadienne mûre devrait protéger la liberté d'expression et le désaccord démocratique tout en améliorant la capacité du public à identifier la source, l'intention, l'authenticité, la qualité des preuves, la conception manipulatrice et les pressions exercées par les systèmes d'information.

Le rapport recommande un programme national de sécurité cognitive fondé sur cinq piliers : des définitions communes, l'analyse des systèmes humains, l'infrastructure de confiance publique, la résilience civique et la gouvernance numérique responsable. La mise en œuvre devrait être graduelle et passer par l'éducation publique, les protocoles de recherche, la formation institutionnelle, les normes d'approvisionnement, les pratiques de communication de crise, la transparence des plateformes et de l'IA, ainsi que des partenariats intersectoriels. L'objectif n'est pas d'éliminer l'incertitude. L'objectif est d'améliorer la capacité du Canada à reconnaître et à gérer l'incertitude sans affaiblir les droits, la confiance ou le raisonnement public.

Constat principal : Le Canada a besoin d'un cadre national de sécurité cognitive qui relie la cybersécurité, la sensibilisation à l'ingérence étrangère, la gouvernance de l'IA, les communications publiques, la résilience civique et l'intégrité décisionnelle humaine, sans transformer la sécurité cognitive en censure, en surveillance ou en communication partisane.

Carte du contenu

Définition et portée

Aux fins du présent rapport, la sécurité cognitive désigne la protection et le renforcement de la perception, de l'interprétation, du jugement et de la prise de décision humaine dans des environnements informationnels complexes. Elle s'intéresse à la manière dont les personnes et les institutions comprennent les signaux, attribuent du sens, évaluent la confiance et agissent dans l'incertitude. Le concept comprend la protection contre la manipulation, mais il comprend aussi le renforcement positif des capacités : meilleures explications publiques, communication institutionnelle plus claire, habitudes de preuve plus solides et compréhension civique plus résiliente.

Un cadre canadien de sécurité cognitive devrait être centré sur l'humain. Il devrait considérer les résidents, les fonctionnaires, les leaders communautaires, les journalistes, les chercheurs et les décideurs comme des personnes intégrées à des systèmes d'attention, d'incitatifs, de conception, d'émotion, de culture, de langue, de confiance, d'histoire et de pouvoir institutionnel. L'individu n'est pas le maillon faible. L'individu est le point où les systèmes deviennent une expérience vécue. Une approche de systèmes humains étudie

donc la relation entre les personnes et les systèmes qui façonnent ce qu'elles voient, ce qu'elles ignorent, ce qu'elles considèrent normal, ce qu'elles craignent et ce qu'elles sont en mesure de décider.

Le présent rapport a une portée nationale. Il traite du Canada comme fédération réunissant des acteurs fédéraux, provinciaux, territoriaux, municipaux, autochtones, privés, universitaires, médiatiques et issus de la société civile. Il n'attribue pas la responsabilité de la sécurité cognitive à un seul ministère ou à une seule profession. Le champ se situe entre plusieurs domaines existants : cybersécurité, sécurité nationale, évaluation du renseignement, résilience démocratique, gouvernance de l'IA, protection de la vie privée, protection des consommateurs, éducation, santé publique, gestion des urgences, sciences du comportement et administration publique.

Le rapport ne recommande pas de surveiller la pensée, de supprimer le désaccord ou de créer une autorité étatique sur la vérité. La vie démocratique exige débat, dissidence, plaidoyer, persuasion, satire, critique et incertitude. La préoccupation de sécurité cognitive apparaît lorsque les systèmes d'information deviennent opaques, asymétriques, manipulateurs, coercitifs ou tellement dégradés que les citoyens ne peuvent plus raisonnablement identifier la source, l'intention, la preuve, l'authenticité ou le risque. L'objectif d'intérêt public est de préserver les conditions du jugement indépendant.

Questions de recherche et méthode

Ce document d'orientation est guidé par cinq questions de recherche :

• Que signifie la sécurité cognitive dans un contexte civique et institutionnel canadien?
• Comment les systèmes d'information numériques influencent-ils la perception, l'interprétation, la confiance et la prise de décision?
• Quels risques émergent lorsque les cyberopérations, la désinformation, les contenus générés par l'IA, la conception des plateformes et les défaillances de communication institutionnelle interagissent?
• Quels domaines de gouvernance canadienne traitent déjà des éléments de la sécurité cognitive, et où se situent les lacunes?
• Quelles mesures pratiques le Canada pourrait-il prendre pour renforcer la résilience civique sans affaiblir les droits, le pluralisme et le débat ouvert?

La méthode est une synthèse analytique. Le rapport s'appuie sur des documents publics du gouvernement du Canada relatifs aux cybermenaces, sur la Commission sur l'ingérence étrangère, sur des documents canadiens concernant la vie privée et la protection des consommateurs, sur des documents de gouvernance de l'IA, sur la littérature relative à la résilience démocratique, ainsi que sur certains travaux internationaux et universitaires portant sur l'intégrité de l'information et les risques liés aux systèmes humains. Le rapport utilise uniquement des sources publiques et ne formule aucune conclusion classifiée, investigative, médicale, psychologique ou juridique.

L'analyse est volontairement prudente. Elle distingue l'influence de la manipulation, le désaccord de la désinformation, et la vulnérabilité de l'incapacité. Elle reconnaît aussi que la confiance ne peut pas être exigée par les institutions. Elle doit être gagnée par l'exactitude, l'humilité, la réactivité, la transparence et la responsabilité. La sécurité cognitive n'est donc pas seulement un cadre de menace. Elle est aussi un cadre de qualité de gouvernance.

Pourquoi la sécurité cognitive est importante au Canada

L'environnement de sécurité du Canada devient de plus en plus cognitif parce que de nombreux préjudices opèrent désormais par l'interprétation. Une attaque par rançongiciel contre un hôpital, une atteinte aux données, une campagne d'influence étrangère, un hypertrucage ou un message d'urgence confus peuvent produire simultanément des effets techniques, opérationnels et psychologiques. Le public peut se demander : l'information est-elle réelle? Qui est responsable? Puis-je faire confiance à l'institution? Suis-je en sécurité? Que dois-je faire maintenant? Ces questions ne sont pas secondaires à la sécurité; elles font partie de la sécurité.

Le Centre pour la cybersécurité note que les plateformes en ligne et les technologies numériques servent d'intermédiaires dans la manière dont les Canadiens travaillent, magasinent, voyagent, socialisent, s'informent et accèdent aux services essentiels [1]. Cela signifie que les Canadiens ne rencontrent pas l'information dans un espace neutre. Ils la rencontrent à travers des fils d'actualité, des résultats de recherche, des applications de messagerie, des moteurs de recommandation, des publicités ciblées, des incitatifs de plateforme, des systèmes de travail, des portails de services, des influenceurs et des outils automatisés. Ces systèmes peuvent améliorer l'accès et l'efficacité, mais ils peuvent aussi déformer l'attention, amplifier les contenus émotionnels, segmenter les publics et rendre la vérification difficile.

L'ingérence étrangère ajoute une dimension de sécurité nationale. La Commission sur l'ingérence étrangère a conclu que des acteurs étrangers ont tenté d'interférer dans les processus démocratiques canadiens et que la désinformation peut nuire à la confiance démocratique même lorsque les résultats électoraux ne sont pas modifiés [2]. Cette conclusion est importante parce que la cible stratégique peut être la confiance publique elle-même. Un acteur hostile n'a pas besoin de convaincre tout le monde d'une fausseté. Il peut suffire d'épuiser les gens, de brouiller les normes de preuve, d'intimider des communautés, d'approfondir la suspicion ou de faire paraître les institutions démocratiques comme étant durablement compromises.

La dimension intérieure est tout aussi importante. L'insécurité cognitive peut apparaître sans acteur étranger. Elle peut découler de la manipulation commerciale, de l'amplification algorithmique, d'une mauvaise communication institutionnelle, d'une faible littératie médiatique, d'écosystèmes d'escroquerie, de conflits identitaires polarisés, de systèmes d'IA opaques ou de pratiques de conception qui orientent les choix. Le Bureau de la consommation du gouvernement du Canada décrit les interfaces truquées comme des techniques de conception qui peuvent induire en erreur ou exercer une pression sur les consommateurs en ligne [4]. Ces enjeux de conception montrent que la sécurité cognitive est aussi une question de vie quotidienne, et pas seulement une question de sécurité nationale.

Pour le Canada, la sécurité cognitive est importante parce qu'elle relie la confiance publique à la gouvernance pratique. Une population qui ne peut pas distinguer les preuves crédibles de la manipulation synthétique est plus vulnérable pendant les urgences. Les institutions qui communiquent mal créent des vides informationnels. Les plateformes qui optimisent uniquement l'engagement peuvent récompenser l'indignation. Les organismes publics qui déploient l'IA sans explicabilité peuvent affaiblir la confiance même lorsque les outils sont techniquement exacts. La sécurité cognitive aide à relier ces problèmes dans un même cadre de systèmes humains.

Analyse des systèmes humains

L'analyse des systèmes humains commence par une prémisse simple : les personnes n'interprètent pas l'information isolément. Elles l'interprètent à travers la mémoire, l'émotion, l'identité, l'expérience antérieure, la confiance sociale, la langue, la fatigue, la peur, les normes communautaires, la crédibilité institutionnelle et la conception des systèmes qui présentent l'information. Une approche de sécurité cognitive ne demande donc pas seulement quelle information a été fournie, mais comment l'environnement qui l'entoure a façonné l'interprétation.

Dans un environnement numérique, le système n'est pas seulement le message. Il comprend le fil d'actualité, le moment de diffusion, la répétition, le classement, l'indice visuel, la notification, la preuve sociale, le contexte absent, la friction nécessaire pour vérifier et l'état émotionnel créé par l'interface. Une personne peut croire qu'elle choisit librement parmi des options visibles alors qu'un système a déjà limité ce qu'elle voit, rendu une option plus facile, une autre plus difficile, et associé des indices sociaux ou émotionnels au choix.

L'analyse des systèmes humains ne devrait pas servir à excuser toutes les décisions ni à retirer l'agentivité. Elle améliore plutôt la responsabilité en montrant où le choix individuel rencontre la pression environnementale. Cet aspect est particulièrement important pour les politiques publiques. Si une communication publique échoue parce qu'elle suppose une attention parfaite, un haut niveau de littératie, une confiance stable et un temps illimité, l'échec est en partie systémique. Si la conception d'une

plateforme récompense le sensationnalisme, la confusion publique qui en résulte n'est pas simplement une faiblesse de l'utilisateur. Si un outil d'IA produit des explications confiantes mais erronées, le risque comprend à la fois l'erreur technique et la dépendance humaine excessive.

Un modèle utile de systèmes humains pour la sécurité cognitive peut être organisé autour de six questions : Qu'est-ce qui a été rendu visible? Qu'est-ce qui a été caché ou rendu difficile d'accès? Quels indices émotionnels ont façonné l'interprétation? Quels indices sociaux ont façonné la légitimité perçue? Quels choix étaient réellement disponibles? Quelles preuves permettraient une révision ultérieure? Ces questions peuvent être utilisées par les chercheurs, les communicateurs publics, les enquêteurs, les agents d'approvisionnement, les éducateurs et les analystes de politiques.

Couche analytique	Question centrale	Pertinence pour la sécurité cognitive
Perception	Quelle information la personne a-t-elle réellement rencontrée?	Détermine l'environnement de preuve visible.
Interprétation	Quel sens a été encouragé par le cadrage, l'émotion, la répétition ou les indices identitaires?	Identifie comment la compréhension a été façonnée.
Architecture du choix	Quelles actions étaient faciles, difficiles, cachées ou décourageées?	Montre si les décisions étaient réellement disponibles.
Environnement de confiance	Quelles institutions, messagers ou communautés ont été traités comme crédibles ou suspects?	Relie la confiance publique au comportement informationnel.
Trace de preuve	L'exposition, la conception, la source et le chemin décisionnel peuvent-ils être révisés?	Permet la responsabilité et l'apprentissage.

Environnement informationnel numérique du Canada

L'environnement informationnel numérique du Canada se caractérise par une forte connectivité, une dépendance aux plateformes, la collecte de données, la création de contenus médiée par l'IA, la cybercriminalité et la vitesse des controverses publiques. L'Évaluation du Centre pour la cybersécurité indique que les adversaires étatiques du Canada deviennent plus agressifs dans le cyberespace et que des acteurs parrainés par des États combinent très probablement des attaques perturbatrices contre des réseaux informatiques avec des campagnes d'information en ligne afin d'intimider et d'influencer l'opinion publique [1]. Il s'agit d'un lien direct entre la cybersécurité et la sécurité cognitive.

L'IA générative intensifie cet environnement en réduisant le coût de production de textes, d'images, d'audios et de vidéos persuasifs. Les contenus synthétiques peuvent servir la créativité, l'accessibilité, la traduction et l'éducation publique, mais ils peuvent aussi soutenir l'usurpation d'identité, la fraude, le harcèlement, les fausses preuves et la manipulation à grande échelle. L'IA ne crée pas à elle seule le besoin de sécurité cognitive; elle accélère des vulnérabilités déjà présentes dans l'attention, l'authentification, la vérification des sources et la confiance.

L'architecture des plateformes importe également. Les systèmes de recommandation peuvent rendre la vie publique apparemment personnalisée tout en masquant les raisons pour lesquelles certains contenus apparaissent. Les utilisateurs peuvent interpréter une exposition répétée comme une réalité sociale, une popularité ou une preuve, même lorsqu'elle reflète l'optimisation de l'engagement ou une distribution ciblée. L'enjeu d'intérêt public n'est pas l'existence du classement. Le classement est inévitable dans les grands espaces informationnels. L'enjeu est de savoir si les utilisateurs, les chercheurs, les régulateurs et les institutions peuvent comprendre et contester les systèmes de classement à fort impact lorsqu'ils touchent la

participation démocratique, la sécurité publique, les comportements de santé ou les communautés vulnérables.

Le ciblage fondé sur les données ajoute une autre couche. Les données personnelles, les préférences inférées, les signaux émotionnels, les habitudes de localisation et les informations du graphe social peuvent être utilisés pour adapter les messages. Dans des contextes ordinaires, la personnalisation peut être utile. Dans des contextes à fort impact, elle peut exploiter la vulnérabilité ou fragmenter le dossier public. Des groupes différents peuvent recevoir des messages différents, des niveaux de peur différents, des promesses différentes et des explications différentes. Cela rend plus difficile le maintien d'une compréhension civique commune.

L'insécurité numérique est aussi vécue à travers les escroqueries ordinaires, la fraude, les rançongiciels, l'hameçonnage et le vol d'identité. Le Centre pour la cybersécurité identifie la cybercriminalité comme une menace persistante et perturbatrice, et note que la cybercriminalité comme service soutient un écosystème mondial résilient [1]. Ces crimes sont cognitifs autant que techniques : ils utilisent l'urgence, l'autorité, la peur, la confiance, la honte, la confusion et l'ingénierie sociale pour contourner le jugement. Une approche canadienne de sécurité cognitive devrait donc relier l'hygiène cybernétique à l'hygiène du jugement.

Résilience civique et confiance publique

La résilience civique est la capacité des personnes et des institutions à absorber des chocs informationnels, à maintenir un désaccord démocratique légal, à corriger les erreurs et à continuer de prendre des décisions dans l'incertitude. Elle n'est pas l'absence de conflit. Les sociétés démocratiques doivent contenir le désaccord. La question de résilience consiste à savoir si le désaccord demeure ancré dans la preuve, la proportionnalité, la dignité humaine et des voies institutionnelles de correction.

La confiance publique n'est pas un produit de communication. C'est une relation. Les institutions tentent souvent de rétablir la confiance en publiant davantage de déclarations, mais la sécurité cognitive exige de prêter attention aux conditions dans lesquelles ces déclarations sont reçues. Si des communautés ont vécu de la négligence, de la discrimination, du secret, des contradictions ou des torts administratifs, les messages institutionnels peuvent être interprétés à travers ces histoires. Une communication efficace doit donc être exacte, opportune, humble, transparente quant à l'incertitude et sensible aux questions du public.

La Commission sur l'ingérence étrangère est instructive parce qu'elle met en lumière la relation entre la communication des menaces et la confiance démocratique. Les avertissements publics peuvent informer les citoyens, mais des avertissements vagues peuvent aussi créer de la suspicion, de la stigmatisation ou de la panique. L'exagération peut nuire à la confiance; la sous-estimation peut laisser les gens vulnérables. La sécurité cognitive exige une communication calibrée qui aide le public à comprendre le risque sans fabriquer un sentiment d'impuissance.

La résilience civique exige aussi une capacité locale. Les institutions nationales ne peuvent pas interpréter chaque contexte local. Les administrations municipales, les gouvernements et organisations autochtones, les écoles, les bibliothèques, les organismes d'établissement, les médias communautaires, les associations professionnelles et les groupes de la société civile aident tous les personnes à interpréter les événements. Une stratégie nationale de sécurité cognitive devrait donc soutenir les intermédiaires de confiance plutôt que centraliser toute interprétation.

La littératie médiatique demeure importante, mais elle ne suffit pas à elle seule. Demander aux individus de tout vérifier dans un environnement de médias synthétiques à grande vitesse peut devenir irréaliste. La sécurité cognitive devrait combiner les compétences individuelles avec la responsabilité des plateformes, la transparence institutionnelle, les normes professionnelles, les données publiques accessibles et la conception des communications de crise. Le fardeau ne peut pas reposer uniquement sur l'utilisateur.

Analyse des menaces et des risques

Un risque de sécurité cognitive est le plus élevé lorsqu'un mécanisme informationnel est opaque, répété, émotionnellement intense, lié à l'identité, difficile à vérifier, difficile à refuser et associé à une décision à fort impact. Le tableau ci-dessous résume des risques récurrents pour le Canada.

Mécanisme de risque	Indicateurs observables	Préjudice potentiel d'intérêt public	Préoccupation de gouvernance
Opérations informationnelles cyberactivées	Fuites de données accompagnées de récits; activités de piratage-divulgation; amplification coordonnée.	Confusion, intimidation, méfiance et pression sur les institutions publiques.	Relier cybersécurité, communication publique et résilience démocratique.
Médias synthétiques et usurpation	Hypertrucages audio ou vidéo, voix clonées, captures d'écran fabriquées, faux documents.	Fraude, atteinte à la réputation, fausses preuves et confusion en situation de crise.	Authentification, provenance, correction rapide et éducation publique.
Amplification algorithmique	Viralité soudaine, contenus d'indignation répétés, recommandations inexpliquées.	Perception déformée de l'opinion publique et polarisation accrue.	Transparence des plateformes et accès pour la recherche.
Interfaces truquées	Options de retrait obscurcies, fausse urgence, consentement confus, renouvellement forcé.	Autonomie et consentement dégradés dans la vie numérique quotidienne.	Protection des consommateurs et responsabilité de conception.
Défaillance de communication institutionnelle	Messages publics tardifs, vagues, défensifs ou contradictoires.	Vides informationnels et baisse de confiance.	Normes de communication de crise et examen après action.
Harcèlement ciblé ou répression transnationale	Intimidation de diasporas, divulgation malveillante de renseignements, surveillance, abus coordonné.	Silence imposé à des communautés et réduction de la participation démocratique.	Protection, voies de signalement et confiance communautaire.

L'analyse des risques doit éviter de traiter toute influence comme hostile. Les conseils de santé publique, les alertes d'urgence, les campagnes d'éducation, le journalisme, le plaidoyer politique et l'organisation communautaire cherchent tous à influencer le comportement. La différence tient à la légitimité, à la transparence, à la preuve, au consentement, à la responsabilité et à la proportionnalité. La sécurité cognitive s'intéresse à l'influence qui est cachée, coercitive, exploitante, trompeuse ou structurellement nuisible au jugement autonome.

Le défi le plus difficile est celui de la preuve. Les préjudices de sécurité cognitive découlent souvent d'une exposition cumulative plutôt que d'un seul événement. Une personne peut être influencée par des centaines de publications, messages, indices de conception et pressions sociales. Les systèmes juridiques et de politiques publiques ont besoin de protocoles de preuve qui préservent le contenu, le moment, les indicateurs de source, la conception d'interface, les interactions de l'utilisateur, les réponses des plateformes et les décisions institutionnelles.

Sans preuve, les allégations de sécurité cognitive peuvent devenir soit impossibles à démontrer, soit trop faciles à exagérer. Une approche canadienne devrait donc combiner humilité et documentation. Toute manipulation perçue ne sera pas démontrable. Toute affirmation fausse ne sera pas stratégique. Toute

opération d'influence stratégique ne réussira pas. Mais l'observation systématique peut révéler des tendances : récits répétés, comptes coordonnés, communautés ciblées, pression de conception, artefacts synthétiques et défaillances de réponse institutionnelle.

Paysage de gouvernance

Le Canada dispose déjà de plusieurs outils de gouvernance pertinents pour la sécurité cognitive. Les institutions de cybersécurité traitent les activités cybernétiques malveillantes et la résilience. Les institutions électorales protègent l'administration des élections et la confiance du public. Les organismes de protection de la vie privée traitent les renseignements personnels et le consentement. Les organismes de protection des consommateurs et de concurrence peuvent agir contre les pratiques trompeuses et la conception manipulatrice. Les organismes de Sécurité publique et de sécurité nationale traitent l'ingérence étrangère. Les outils d'ISDE et du Secrétariat du Conseil du Trésor traitent l'IA et le gouvernement numérique. La lacune n'est pas une absence complète de gouvernance; elle réside dans la fragmentation.

Le document d'accompagnement de la Loi sur l'intelligence artificielle et les données décrivait une approche fédérale proposée pour les systèmes d'IA à incidence élevée, y compris des obligations de réduction des risques, de surveillance, de transparence et de tenue de dossiers [3]. Peu importe l'état législatif, ces catégories de politiques sont pertinentes pour la sécurité cognitive, car l'IA à incidence élevée peut influencer la manière dont les personnes sont évaluées, informées, persuadées, servies ou exclues. L'analyse de sécurité cognitive devrait être incluse partout où les systèmes d'IA façonnent le jugement humain ou les décisions institutionnelles.

La protection des consommateurs est également pertinente. Les directives publiques du Bureau de la consommation sur les interfaces truquées décrivent des pratiques de conception qui peuvent orienter, presser ou induire en erreur les utilisateurs [4]. Il s'agit d'un exemple pratique de sécurité cognitive dans la vie quotidienne. Un processus d'annulation confus, une invite de confidentialité manipulatrice ou un compte à rebours de fausse urgence peut ne pas ressembler à de la sécurité nationale, mais il normalise un consentement dégradé et affaiblit les attentes publiques envers une conception numérique transparente.

Le droit et les politiques relatifs à l'ingérence étrangère traitent une autre partie du paysage. La Loi sur la lutte contre l'ingérence étrangère a reçu la sanction royale en 2024 et comprend des mesures comme un cadre de transparence en matière d'influence étrangère [5]. Ce type d'outil peut améliorer la transparence de certaines activités liées à l'étranger, mais la sécurité cognitive demeure plus vaste. Elle comprend aussi la manipulation intérieure, la conception commerciale, la persuasion médiée par l'IA, les communications publiques et la confiance institutionnelle.

Le défi de gouvernance consiste à créer de l'interopérabilité entre ces domaines sans produire un concept trop large. La sécurité cognitive ne devrait pas devenir une étiquette appliquée à toutes les controverses de discours. Elle devrait être utilisée lorsqu'il existe une préoccupation identifiable de systèmes humains : manipulation de la perception, dégradation des conditions décisionnelles, architecture informationnelle exploitante, intimidation ciblée ou perte de capacité publique à évaluer les preuves.

Domaine	Contribution actuelle	Lacune de sécurité cognitive	Voie pratique
Cybersécurité	Évaluation des menaces, réponse aux incidents, protection des infrastructures essentielles.	Se concentre souvent davantage sur les systèmes que sur l'interprétation publique.	Intégrer les effets sur la confiance publique dans la planification des incidents cybernétiques.
Ingérence étrangère	Sensibilisation aux menaces, outils juridiques, garanties électorales.	Peut être communiquée trop étroitement comme un enjeu uniquement électoral.	Inclure la protection des diasporas, la résilience à la désinformation et des voies locales de signalement.

Vie privée	Consentement, responsabilité, protection des données.	L'utilisation des données peut être légale tout en laissant les effets d'influence opaques.	Traiter les inférences sensibles et les profils de persuasion comme des risques plus élevés.
Protection des consommateurs	Pratiques trompeuses et sensibilisation aux interfaces truquées.	La manipulation subtile n'entre pas toujours dans les catégories existantes.	Élaborer des normes applicables en matière de conception manipulatrice.
Gouvernance de l'IA	Réduction des risques, transparence, surveillance, tenue de dossiers.	Les effets sur le jugement humain peuvent être insuffisamment précisés.	Ajouter des évaluations d'impact sur l'influence et l'intégrité décisionnelle.
Administration publique	Communications, conception des services, approvisionnement.	Les effets sur la confiance sont souvent évalués après le préjudice.	Intégrer des critères de sécurité cognitive dans l'approvisionnement et l'examen des communications.

Recommandations pour le Canada

Recommandation	Acteurs responsables	Échéancier	Complexité
Adopter une définition de travail nationale de la sécurité cognitive axée sur la perception, l'interprétation, le jugement, l'intégrité décisionnelle et la confiance publique.	Sécurité publique, Patrimoine, ISDE, CST/Centre pour la cybersécurité, société civile, partenaires universitaires.	Court terme	Moyenne
Créer un guide d'évaluation des systèmes humains pour les communications publiques, les outils d'IA, les partenariats de plateformes et la réponse de crise.	Secrétariat du Conseil du Trésor, ministères fédéraux, provinces, municipalités.	Court terme	Moyenne
Ajouter des critères de sécurité cognitive à la réponse aux incidents cybernétiques, incluant l'impact sur la confiance publique, le risque de désinformation et des canaux de correction clairs.	CST/Centre pour la cybersécurité, Sécurité publique, exploitants d'infrastructures essentielles.	Court à moyen terme	Moyenne
Élaborer des protocoles de preuve pour la manipulation informationnelle, incluant la préservation des contenus, la provenance, le moment, l'amplification et l'analyse de conception.	Chercheurs, régulateurs, professionnels du droit, spécialistes de criminalistique numérique.	Moyen terme	Élevée
Renforcer l'éducation	Écoles, bibliothèques,	Court à moyen terme	Moyenne

publique sur la source, l'intention, l'authenticité, la preuve, l'incertitude et la conception manipulatrice.	organismes civiques, médias, agences publiques.		
Exiger que les déploiements d'IA et de services numériques à incidence élevée évaluent les effets sur le jugement humain, l'explication, l'appel et la confiance.	ISDE, Conseil du Trésor, autorités d'approvisionnement, régulateurs.	Moyen terme	Élevée
Soutenir les intermédiaires communautaires de confiance, surtout pour les diasporas et les groupes visés par l'intimidation ou la manipulation.	Gouvernements fédéral/provinciaux, municipalités, organismes communautaires.	Moyen terme	Moyenne
Créer un réseau canadien de recherche en sécurité cognitive reliant le droit, la psychologie, l'administration publique, la cybersécurité, l'IA, les communications et l'éducation civique.	Universités, groupes de réflexion, société civile, organismes de recherche d'intérêt public.	Moyen terme	Moyenne

Ces recommandations sont conçues pour être progressives. Le Canada n'a pas besoin de créer une super-agence unique de sécurité cognitive. Il a besoin d'un vocabulaire commun, de pratiques d'évaluation partagées et d'une meilleure coordination entre les institutions existantes. La première étape la plus importante est la discipline définitionnelle : la sécurité cognitive devrait être présentée comme intégrité décisionnelle et conscience situationnelle, et non comme contrôle des croyances.

Les communications publiques devraient être traitées comme une infrastructure essentielle pendant les crises. Cela signifie préparer avant les incidents des explications en langage clair, des énoncés d'incertitude, des mécanismes de correction, des communications adaptées aux communautés et une capacité de réponse rapide aux mythes. Une défaillance de communication peut intensifier un incident technique en créant peur, spéculation et méfiance.

L'approvisionnement constitue un autre levier pratique. Les gouvernements qui achètent des outils d'IA, des services de veille des médias sociaux, des systèmes d'identité numérique, des technologies éducatives ou des plateformes de communication publique peuvent exiger des critères de sécurité cognitive : explicabilité, journaux d'audit, contrôle par l'utilisateur, accessibilité, examen des biais, protection de la vie privée, garde-fous contre la manipulation et évaluation indépendante.

Calendrier de mise en œuvre

Phase	Période	Actions prioritaires	Résultat attendu
Phase 1 : vocabulaire et sensibilisation	2026	Publier des documents d'introduction publics; réunir les parties prenantes; définir la sécurité cognitive en termes civiques canadiens.	Langage commun et cadrage public non partisan.

Phase 2 : outils de systèmes humains	2026-2027	Élaborer des listes de vérification pour les communications, l'IA, les incidents cybernétiques et les risques de plateforme.	Outils pratiques pour les institutions et les chercheurs.
Phase 3 : preuve et formation	2027	Créer des protocoles de documentation; former les communicateurs publics, enquêteurs, éducateurs et analystes.	Preuves répétables et qualité de réponse améliorée.
Phase 4 : approvisionnement et normes	2027-2028	Ajouter des critères de sécurité cognitive à l'approvisionnement numérique et à l'examen de l'IA à incidence élevée.	Responsabilité systémique avant le déploiement.
Phase 5 : institutionnalisation	2028 et après	Établir des partenariats de recherche durables et des mécanismes de rapports publics.	Capacité nationale soutenue et résilience civique.

Le calendrier est progressif parce que la sécurité cognitive dépend de la confiance. Aller trop rapidement vers l'application sans définitions communes pourrait créer confusion ou inquiétude. Aller trop lentement laisse le Canada exposé à la conception manipulatrice, aux médias synthétiques, à l'ingérence étrangère, à l'intimidation cyberactivée et aux défaillances de confiance institutionnelle. La meilleure voie est un développement discipliné, transparent et fondé sur des preuves.

Lacunes de recherche et prochaines étapes

Plusieurs lacunes de recherche exigent une attention particulière. Premièrement, le Canada a besoin de meilleures données probantes sur la manière dont différentes communautés vivent la manipulation informationnelle, la confiance institutionnelle et la vulnérabilité numérique. Les moyennes nationales peuvent masquer les réalités locales. Deuxièmement, le Canada doit renforcer les méthodes de mesure des effets cognitifs des incidents cybernétiques et des défaillances de communication publique. Troisièmement, davantage de travaux sont nécessaires sur la persuasion médiée par l'IA, surtout lorsque des systèmes automatisés génèrent des explications personnalisées ou des appels émotionnels. Quatrièmement, il faut des outils d'évaluation pratiques que les organisations non spécialisées peuvent utiliser sans adopter un langage trop technique.

Un programme canadien de recherche devrait inclure des études de cas d'intérêt public, une éducation publique bilingue et multilingue, des consultations communautaires, des recherches sur la transparence des plateformes, une analyse de l'approvisionnement et une révision éthique pour la recherche avec des êtres humains. Le domaine doit demeurer prudent dans ses affirmations sur les états mentaux. La sécurité cognitive devrait étudier des mécanismes observables et des effets documentés plutôt que des affirmations spéculatives.

Pour Sécurité Cognitive Canada, la prochaine étape consiste à convertir ce document d'orientation en trois produits complémentaires : un bref document de sensibilisation public de deux pages, une liste de vérification d'évaluation des systèmes humains et une feuille de route de développement de la recherche pour les partenariats avec des organisations universitaires, civiques, publiques et communautaires. Ces produits devraient préserver le même cadrage calme : percevoir, analyser, intégrer.

Étapes prioritaires :
• Créer un glossaire canadien de la sécurité cognitive à l'usage du public et des institutions.
• Rédiger une liste de vérification des systèmes humains pour l'influence numérique et les communications

publiques.
• Élaborer un bref document bilingue de sensibilisation sur la sécurité cognitive et la résilience civique.
• Cartographier les responsabilités canadiennes de gouvernance en matière de cybersécurité, d'IA, de vie privée, de protection des consommateurs, d'élections et de sécurité publique.
• Identifier des partenaires de recherche pour l'étude éthique et non partisane des environnements informationnels numériques et de la confiance publique.

Conclusion

La sécurité cognitive offre au Canada une manière pratique de comprendre la couche humaine de l'environnement informationnel numérique. Elle ne remplace pas la cybersécurité, la protection de la vie privée, la littératie médiatique, la sécurité publique ou les droits démocratiques. Elle les relie par la réalité vécue de l'interprétation : ce que les personnes voient, ce qu'elles jugent crédible, la manière dont elles prennent des décisions et la capacité des institutions à préserver les conditions du jugement indépendant.

Le défi du Canada n'est pas seulement le contenu hostile. Il réside dans l'interaction entre plateformes, systèmes d'IA, cyberopérations, escroqueries, communication institutionnelle, confiance sociale et vulnérabilité humaine. Un Canada résilient a besoin de personnes capables d'évaluer l'incertitude, d'institutions qui communiquent honnêtement, de systèmes numériques responsables et de communautés soutenues plutôt que blâmées.

Un cadre national de sécurité cognitive devrait donc être civique, transparent, respectueux des droits et fondé sur des preuves. Son but est de promouvoir la conscience situationnelle, et non de contrôler les croyances. Son indicateur de succès n'est pas l'accord uniforme, mais une capacité publique renforcée à percevoir, analyser et intégrer l'information sous pression.

Références

[1] Centre canadien pour la cybersécurité. Évaluation des cybermenaces nationales 2025-2026. Gouvernement du Canada, 2024. https://www.cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2025-2026

[2] Commission sur l'ingérence étrangère dans les processus électoraux et les institutions démocratiques fédérales. Rapport final. Gouvernement du Canada, 2025. Voir aussi la couverture de l'Associated Press sur le rapport final, 28 janvier 2025.

[3] Innovation, Sciences et Développement économique Canada. Loi sur l'intelligence artificielle et les données - document d'accompagnement. Gouvernement du Canada. https://ised-isde.canada.ca/site/innover-meilleur-canada/fr/loi-lintelligence-artificielle-donnees-liad-document-daccompagnement

[4] Gouvernement du Canada, Bureau de la consommation. Interfaces truquées. Innovation, Sciences et Développement économique Canada. https://ised-isde.canada.ca/site/bureau-consommation/fr/interfaces-truquees

[5] Parlement du Canada. Projet de loi C-70, Loi sur la lutte contre l'ingérence étrangère, L.C. 2024, ch. 16. Sanction royale, 20 juin 2024.

[6] Commissariat à la protection de la vie privée du Canada. Documents d'orientation, de recherche et de politique sur les renseignements personnels, l'influence en ligne et la confiance numérique. https://www.priv.gc.ca/

[7] Centre de la sécurité des télécommunications Canada. Cybermenaces contre le processus démocratique du Canada : mise à jour de 2023. Gouvernement du Canada.

[8] Bureau de la concurrence Canada. Pratiques commerciales trompeuses et orientations d'application de la Loi sur la concurrence. Gouvernement du Canada.

[9] Secrétariat du Conseil du Trésor du Canada. Directive sur la prise de décisions automatisée et documents relatifs à l’évaluation de l’incidence algorithmique. Gouvernement du Canada.

[10] Conseil de la radiodiffusion et des télécommunications canadiennes et documents de politique numérique du gouvernement du Canada relatifs aux plateformes en ligne, aux communications et à la réglementation d’intérêt public.

Citation suggérée

Sécurité Cognitive Canada. (2026). La sécurité cognitive au Canada : analyse des systèmes humains, résilience civique, confiance publique et environnement informationnel numérique. Rapport de recherche COGSECCAN RR-002-FR.

Avis de non-responsabilité

Ce rapport est destiné à la recherche d’intérêt public et à des fins éducatives. Il ne constitue pas un avis juridique, médical, psychologique, de cybersécurité, d’approvisionnement, financier ou professionnel. Les constats sont fondés sur des sources publiques citées et sur une synthèse analytique au moment de la publication.

Contact : info@cogsec.ca