



Des membres de la compagnie Talon des Forces armées canadiennes effectuent une mission de reconnaissance (Reco) au cours de l'exercice Wolverine Shield/Strike, au Camp Adazi, en Lettonie, le 7 mars 2023.

Technicien en imagerie des Forces armées canadiennes

L'authenticité comme arme : l'avantage des Forces armées canadiennes dans la guerre de l'information à l'ère de l'IA

ALI MANOUCHEHRI ET MAJOR TYLER CURRIE

Ali Manouchehri est actuellement conseiller principal au Centre d'IA du MDN et des FAC. Avant de se joindre au GSN, il occupait le poste de gestionnaire des données et de l'analytique au sein du SMA (Svc Ex) du MDN.

Le major Tyler Currie occupe le poste d'agent d'intégration et d'accélération de l'IA des FAC au Centre d'IA du MDN et des FAC. Tyler a passé 16 ans au sein de la Branche des services du renseignement et a participé à des opérations de déploiement en Afghanistan ainsi qu'à des missions internationales auprès du Commandement allié de forces interarmées de Naples. Il est titulaire d'une maîtrise en études politiques de l'Université Queen's ainsi que d'une maîtrise en gestion—option Intelligence artificielle (MMAI) de la Smith School of Business de l'Université Queen's.

Le ministère de la Défense nationale (MDN) et les Forces armées canadiennes (FAC) évoluent dans un environnement informationnel où, en situation de crise, la certitude est la première victime.

Par exemple, au cours d'un incident aérospatial relevant du Commandement de la défense aérospatiale de l'Amérique du Nord (NORAD), alors que les forces assurent le suivi d'un aéronef non identifié et interviennent, les commandants et les équipes des affaires publiques peuvent devoir composer simultanément avec une autre menace : des fichiers audio, des vidéos et des textes manipulés au moyen de l'IA qui circulent à la vitesse des machines.¹ Ce qui exigeait autrefois des studios, des budgets importants et plusieurs semaines de travail peut maintenant être produit en quelques minutes au moyen de services d'IA et d'applications de montage largement accessibles, puis diffusé rapidement auprès du public.

Cette réalité opérationnelle met en évidence un autre type de défi, lié à la confiance. L'intelligence artificielle générative accélère la production de contenus convaincants, mais mensongers. Une situation qui fausse les perceptions du public dès les premiers instants d'un incident et complique la gestion de crise au moment le plus critique. Lorsque la confiance s'effrite, la transmission et l'exécution des ordres prennent plus de temps, la coordination ralentit et le risque de conséquences graves augmente.

Dans ce contexte, le Canada est confronté aux mêmes pressions dans l'ensemble de ses missions. À l'étranger, nous menons des opérations avec les alliés, où l'étroite coordination des messages et des décisions est essentielle au maintien de l'unité d'action dans les opérations de coalition. Au pays, le MDN et les FAC viennent en aide à la population canadienne lors de situations de crise—feux de forêt, inondations, opérations de recherche et sauvetage—souvent sous l'œil attentif du public, où les communications doivent être rapides, exactes et dignes de confiance.

Dans le Nord, les grandes distances, les conditions météorologiques rigoureuses et les infrastructures limitées influencent la façon dont l'information circule et dont les collectivités perçoivent le danger. Dans chacun de ces contextes, la capacité d'authentifier un message officiel, de rassurer la population avec calme face à des affirmations trompeuses et de garder une longueur d'avance dans la bataille de l'information est essentielle à la réussite de la mission.

Le raisonnement est simple. Le Canada, de concert avec ses alliés, peut rivaliser efficacement avec ses adversaires sur les plans de la sophistication technologique et de la puissance de calcul, et même les dépasser dans certains domaines technologiques émergents grâce à une main-d'œuvre hautement qualifiée et diversifiée sur le plan culturel, ainsi qu'à une approche fondée sur la collaboration avec ses alliés. L'essentiel consiste à démontrer que nos communications proviennent bien de nous, à vérifier les nouvelles informations avant d'agir et à informer rapidement le public lorsque nous sommes confrontés à la mésinformation ou à la désinformation. En faisant de ces pratiques une norme dans les politiques, la formation, l'approvisionnement et le leadership, le MDN et les FAC préservent leur crédibilité et leur rythme opérationnel face aux acteurs étatiques, aux groupes

mandataires et aux individus opportunistes qui cherchent à exploiter le chaos informationnel à des fins stratégiques.

Nous n'avons pas besoin de surpasser nos adversaires en programmation. En revanche, nous devons être capables de démontrer que nos communications proviennent bien de nous, de vérifier les nouvelles informations avant d'agir et d'informer rapidement le public lorsque nous sommes confrontés à la mésinformation ou à la désinformation.

Les nouvelles conditions de la déception

Les systèmes génératifs apprennent à partir de vastes ensembles de textes, d'images et d'enregistrements audio, puis produisent de nouveaux contenus qui reproduisent les caractéristiques observées. Ils ne raisonnent pas comme les êtres humains.² Parce qu'ils sont conçus pour imiter un style plutôt que pour vérifier les faits, ils peuvent produire des contenus fluides qui paraissent exacts et crédibles, même lorsqu'ils sont faux. Lorsque ces contenus reprennent des éléments familiers, comme une voix connue, une formulation officielle ou une image réaliste, le public est naturellement porté à les considérer comme crédibles.

Les organisations de défense canadiennes doivent désormais composer avec des adversaires capables de produire des imitations convaincantes de contenus officiels en quelques minutes plutôt qu'en plusieurs semaines.³ Ce qui exigeait autrefois du temps, des ressources financières et du matériel spécialisé est désormais peu coûteux et largement accessible. Un article fabriqué de toutes pièces, une image falsifiée ou un enregistrement vocal cloné peuvent être créés rapidement puis diffusés sur de multiples plateformes à un coût négligeable.

Pour les praticiens de la défense, ces changements entraînent trois pressions qui se renforcent mutuellement :

- **La rapidité.** Les adversaires peuvent introduire des contenus manipulés dans l'environnement informationnel alors même que les événements sont encore en cours. Un extrait audio falsifié d'un ordre d'évacuation peut se propager sur les réseaux sociaux avant même que les autorités provinciales aient eu le temps de rédiger le véritable message.⁴ Dans un contexte opérationnel, un fragment d'ordre fabriqué de toutes pièces peut parvenir à une unité avant que le quartier général n'ait confirmé l'ordre réel. La rapidité constitue l'avantage de l'adversaire, puisqu'un simple moment d'hésitation suffit à briser le rythme des opérations et à semer le doute.
- **Le coût.** Les outils génératifs sont largement accessibles, faciles à utiliser et peu coûteux. Ce qui nécessitait auparavant des suites de montage professionnelles et du personnel spécialisé peut aujourd'hui être réalisé à l'aide d'un ordinateur portable et d'un simple abonnement à un logiciel. Ainsi, des États hostiles, des groupes mandataires ou même des acteurs isolés peuvent agir à grande échelle. La défense doit donc faire face non seulement à la

désinformation orchestrée par des États, mais aussi à des tentatives opportunistes d'ingérence menées par des acteurs qui ont peu à perdre.⁵

- **La précision.** Les adversaires peuvent tester et affiner leurs messages en temps quasi réel, en fonction de ce qui trouve un écho auprès de publics précis. Une séquence vidéo manipulée qui ne suscite pas la réaction souhaitée dans une collectivité peut être rapidement reformulée et diffusée de nouveau auprès d'une autre.⁶ Cette précision itérative leur permet d'adapter leurs contenus non seulement selon la langue ou la région, mais aussi en exploitant les récits ou les craintes propres à des groupes ciblés, notamment les familles des militaires, les communautés issues de la diaspora ou les partenaires alliés.

Pour le MDN et les FAC, il en résulte un environnement opérationnel où il est possible de créer l'incertitude plus rapidement, à moindre coût et avec davantage de précision que jamais auparavant. Un ordre retardé, un message discrédité par le doute ou une directive concurrencée par une imitation convaincante contribuent tous à éroder la confiance. Les adversaires n'ont plus besoin de tromper tout le monde. Il leur suffit de semer le doute chez un nombre suffisant de personnes, à des moments clés, pour perturber la coordination.

Pour contrer cette menace, l'authentification doit devenir une pratique courante des communications militaires, renforcée par la formation et le leadership jusqu'à devenir un réflexe. Dans le contexte actuel, l'authentification désigne la vérification de l'origine et de l'intégrité d'un message dans la chaîne de commandement. La perception plus générale de l'authenticité, c'est-à-dire la confiance que le public accorde aux communications officielles, demeure essentielle, mais elle relève d'une notion distincte des mécanismes techniques de protection.

Lorsque l'authentification devient une pratique habituelle, qu'il s'agisse de confirmer les ordres dans la chaîne de commandement, d'intégrer des marqueurs d'authenticité aux communications publiques ou de mettre les procédures de vérification en pratique durant les exercices, le rythme des opérations et la crédibilité demeurent entre les mains de l'institution plutôt que de ceux qui cherchent à les perturber.⁷ Ainsi, l'authentification ne constitue pas seulement une pratique de communication; elle représente une mesure de sécurité opérationnelle. Elle protège le rythme des opérations, préserve l'unité d'action et maintient l'avantage décisionnel.

La vérité mise à l'épreuve dans une démocratie

Les dynamiques qui compliquent la prise de décisions sur le plan opérationnel ne se limitent pas au niveau tactique. Elles s'étendent à l'environnement plus vaste dans lequel le MDN et les FAC doivent expliquer leurs décisions à la population canadienne,

rendre des comptes au Parlement et coordonner leurs activités avec leurs alliés. Lorsque des contenus synthétiques brouillent la distinction entre le vrai et le faux, les conséquences dépassent largement une simple perturbation temporaire sur le terrain. La confiance du public envers les institutions chargées de protéger la population canadienne s'en trouve ébranlée.⁸ La crédibilité des dirigeants s'affaiblit lorsque leurs propos et leurs gestes peuvent être présentés de façon plausible comme des fabrications. Enfin, elle introduit des frictions au sein de la coopération alliée. Une hésitation passagère peut quand même ralentir la coopération entre les alliés ou altérer la perception de la fiabilité du Canada. En ce sens, la manipulation par l'utilisation de contenus synthétiques n'est pas simplement une nuisance sur le champ de bataille, mais une menace stratégique qui vise les fondements mêmes de la confiance dont la défense démocratique a besoin.⁹

Les systèmes génératifs compliquent l'établissement de la confiance, en produisant des imitations convaincantes de contenus officiels. Le problème plus profond réside dans le fait qu'une fois que le public sait que de telles falsifications existent, les documents authentiques peuvent eux aussi être remis en cause. Une vidéo montrant réellement une faute, un document consignait véritablement une infraction ou un extrait audio capturant une remarque malvenue peuvent tous être rejetés comme étant des montages. C'est ce que les chercheurs appellent le « dividende du menteur »—la capacité des acteurs malveillants à échapper à leurs responsabilités en prétendant que des preuves authentiques ont été manipulées.¹⁰

Pour relever ce défi, les vérifications techniques ne suffisent pas. Les institutions doivent renforcer leur résilience grâce à des pratiques de communication cohérentes, à une correction transparente des erreurs et à des activités de sensibilisation, permettant au public de reconnaître les communications authentiques et les voies par lesquelles elles sont diffusées. Lorsque le MDN et les FAC reconnaissent rapidement leurs erreurs, les corrigent ouvertement et expliquent leurs processus, ils démontrent que la crédibilité repose sur la transparence et la responsabilisation, et non sur une image artificielle d'inaffabilité. Lorsqu'ils expliquent à l'avance comment les communications officielles seront authentifiées et diffusées, ils donnent à la population canadienne les moyens de reconnaître les tentatives d'usurpation. Ces pratiques n'éliminent pas complètement le dividende du menteur, mais elles en atténuent les effets, en faisant de l'authenticité une attente constante plutôt qu'une considération secondaire.

L'environnement informationnel propre au Canada

Les défis, posés par les systèmes génératifs, dépassent la seule dimension technique. Ils soulèvent une question de confiance qui influe directement sur les opérations dans des contextes propres au Canada.

Les enjeux auxquels sont confrontés le MDN et les FAC sont influencés par la géographie du Canada et par ses institutions. En raison de sa géographie, le pays doit composer avec de vastes distances, des conditions climatiques rigoureuses et des infrastructures limitées, particulièrement dans le Nord. À ces défis s'ajoutent des réalités institutionnelles propres au Canada : il s'agit d'une fédération où les responsabilités sont partagées entre différents ordres de gouvernement, où les dirigeants autochtones exercent une autorité reconnue et où la défense continentale s'appuie sur des mécanismes binationaux comme le NORAD. Ces caractéristiques influencent la circulation de l'information, déterminent les sources d'autorité perçues comme légitimes et façonnent les conditions dans lesquelles la confiance s'établit.

Contrairement à celui d'États plus centralisés, le système de gouvernance à plusieurs niveaux du Canada fait en sorte qu'aucune institution ne contrôle à elle seule le discours public en période de crise. Un ordre d'évacuation lié à un feu de forêt peut provenir d'une administration municipale, être relayé par une province et recevoir l'appui des Forces armées canadiennes. Dans un tel contexte, la clarté des communications est essentielle, car des acteurs malveillants peuvent exploiter le moindre décalage entre les administrations ou les autorités compétentes afin de semer le doute.

Les crises nationales montrent comment ces pressions s'intensifient lorsque plusieurs administrations et d'importantes populations sont concernées. Les feux de forêt, les inondations et les urgences de santé publique exigent une intervention coordonnée entre les administrations municipales, provinciales, territoriales et fédérales. Dans ces circonstances, une fausse alerte qui paraît officielle ou un faux avis d'annulation d'un ordre d'évacuation peut se propager rapidement dans les médias sociaux.¹¹ Quelques minutes d'hésitation suffisent à rendre les voies d'évacuation plus dangereuses ou à compliquer la coordination des services d'urgence.

Les crises nationales révèlent également la fragilité des systèmes sur lesquels la population canadienne compte. Les feux de forêt peuvent endommager les tours de télécommunications, les inondations interrompre l'alimentation électrique et les pointes de demande surcharger les réseaux locaux. Pour le MDN et les FAC, l'appui aux autorités civiles suppose de se préparer à la fois aux perturbations physiques et à l'arrivée simultanée de contenus synthétiques trompeurs. Un faux message, concernant la fermeture de routes ou la qualité de l'eau, peut combler le vide pendant que les véritables alertes peinent à atteindre la population.

Dans le Nord canadien, les communications présentent des caractéristiques particulières et les conséquences de la confusion peuvent être immédiates. Les collectivités sont de petite taille, très soudées et souvent éloignées des grands centres. Les infrastructures demeurent limitées et les communications peuvent être perturbées par les conditions météorologiques, la géographie ou une capacité de transmission restreinte.¹²

Dans de nombreuses collectivités, le bouche-à-oreille, la radio locale et les pages Facebook communautaires demeurent les principaux moyens de communication.¹³ Cette proximité constitue une force, mais elle accroît également la vulnérabilité des collectivités nordiques. Les rumeurs circulent rapidement parce que les gens se soucient profondément de leurs voisins et réagissent sans délai lorsqu'ils croient qu'ils sont en danger. Un faux message, annonçant la disparition d'une personne, un déversement de matières dangereuses ou un ordre d'évacuation, peut se propager à la vitesse d'une conversation, bien avant qu'une communication officielle soit vue ou jugée crédible.

Pour le MDN et les FAC, cela signifie que la crédibilité dans le Nord ne peut pas reposer uniquement sur des solutions techniques. Elle dépend de relations humaines établies bien avant qu'une situation d'urgence ne survienne. Dans les faits, les aînés autochtones, les radiodiffuseurs locaux et les dirigeants communautaires exercent souvent une influence plus grande que les représentants des autorités éloignées.¹⁴ Lorsque le MDN et les FAC collaborent avec ces acteurs pour promouvoir des pratiques de communication authentiques et les mettent en application durant les patrouilles de routine, les exercices d'entraînement et les opérations saisonnières, ils renforcent un réseau de confiance propre au contexte canadien. Ces réseaux ne se contentent pas de transmettre l'information; ils l'adaptent aux réalités culturelles et linguistiques de la collectivité afin qu'elle soit à la fois comprise et utile.¹⁵

La force de cette approche ne repose pas uniquement sur des éléments visuels comme les logos ou l'image de marque, qui peuvent être imités, mais surtout sur des personnes reconnues et respectées qui communiquent une information crédible. Il s'agit notamment des détenteurs de savoirs reconnus, qui possèdent souvent une expertise particulière et savent le mieux comment rejoindre le plus grand nombre de personnes au sein de leur collectivité.

Lorsque les résidents savent à quoi ressemble un message officiel et où il sera diffusé, et lorsqu'ils ont pu observer ces procédures mises en pratique dans des circonstances normales, ils sont davantage enclins à écarter les captures d'écran ou les messages transférés. Pour le MDN et les FAC, il ne s'agit pas seulement d'une question de technique de communication, mais aussi de respect envers les collectivités nordiques, de reconnaissance du leadership autochtone et de partenariat avec les organisations locales qui bénéficient d'un niveau de confiance que les autorités fédérales ne peuvent atteindre à elles seules.

Le point de vue nord-américain et allié

Dans le contexte de la défense aérospatiale binationale, la capacité de diffuser des mises à jour crédibles en temps quasi réel est essentielle. Par exemple, lorsqu'un ballon ou un aéronef suscite l'attention du public, la population canadienne et américaine s'attend à recevoir rapidement des renseignements rassurants.

Le NORAD repose sur le principe selon lequel le Canada et les États-Unis réagissent comme une seule entité, et cette unité doit être perceptible tant pour les citoyens que pour les dirigeants politiques et les adversaires. Des communications rapides et crédibles ne constituent donc pas un simple complément à la défense continentale; elles en représentent un élément essentiel.¹⁶ Tout comme les réseaux radar offrent une vision commune de l'espace aérien, des mises à jour cohérentes et faisant autorité permettent d'établir une compréhension commune des événements.

Le même principe s'applique aux alliances auxquelles le Canada participe. Les exercices et les déploiements menés en coalition sont particulièrement vulnérables, puisqu'ils exigent un niveau élevé de confiance et de synchronisation entre des partenaires aux profils variés. Les adversaires le savent.¹⁷ Une seule provocation synthétique, un faux rapport après action faisant état d'une défaillance des capacités, une image falsifiée laissant croire à une inconduite ou un faux message évoquant des dissensions entre commandants, peuvent être diffusés au moment précis où une décision importante doit être prise. Même si la supercherie est démasquée quelques heures plus tard, elle mobilise inutilement des ressources, retarde la coordination et mine la confiance au sein de la coalition.

Ces perturbations ne brisent généralement pas les alliances, mais leur effet cumulatif réduit la marge de manœuvre et complique l'action collective. Les différences entre les priorités nationales sont naturelles au sein d'une coalition. Toutefois, les contenus synthétiques malveillants exploitent ces différences, alimentent la méfiance et freinent l'unité d'action.¹⁸

Lorsque le Canada et les États-Unis utilisent des méthodes d'authentification reconnues, comme l'utilisation de repères visuels uniformes dans leurs communications et de signatures cryptographiques intégrées aux images et aux vidéos ainsi que le recours systématique aux canaux officiels, le public apprend à reconnaître les communications authentiques et les journalistes peuvent rendre compte des événements avec davantage d'assurance, même sous pression.¹⁹ Ainsi, l'authentification ne constitue pas seulement une protection contre la confusion; elle devient un atout stratégique qui renforce la crédibilité de la défense continentale.

Pour le Canada, la crédibilité au sein des opérations alliées dépend non seulement du professionnalisme de ses forces, mais aussi de la rapidité et de la clarté avec lesquelles leurs actions sont présentées aux partenaires et au public. Dans cette perspective, l'authentification devient une véritable monnaie opérationnelle : elle permet de maintenir le rythme des opérations, de renforcer la confiance et d'empêcher les adversaires de transformer le doute en retard. Que ce soit dans le contexte de la défense continentale, des collectivités nordiques ou des opérations internationales, les FAC doivent acquérir des habitudes de communication rigoureuses bien avant qu'une crise ne survienne.

Les affaires publiques et la voix crédible du Canada

Les pratiques de vérification qui protègent la chaîne de commandement doivent également s'appliquer à la façon dont le MDN et les FAC communiquent avec le public. La culture d'une organisation se manifeste dans le ton, le moment choisi et la clarté de ses communications. Les affaires publiques commencent donc bien avant une crise. Si le MDN et les FAC expliquent en termes simples que les faux contenus convaincants font désormais partie de l'environnement informationnel, montrent comment reconnaître les communications authentiques et adoptent une communication régulière lorsque les enjeux sont limités, la population saura à quoi s'attendre lorsque les enjeux deviendront importants.²⁰ En situation de crise, la population canadienne réagit mieux lorsque les processus sont expliqués clairement : quelles mesures sont prises pour vérifier l'information, à quel moment la prochaine mise à jour sera diffusée et comment éviter de propager de faux renseignements pendant que les faits sont en cours de vérification.²¹

La voix du Canada doit également représenter son identité. La population canadienne accorde de l'importance à l'équité et à un langage direct. Une courte vidéo diffusée rapidement sur une plateforme officielle par un commandant peut avoir une forte portée morale, puisqu'elle revêt à la fois un caractère personnel et institutionnel. De même, un communiqué indiquant clairement quelles informations seront rendues publiques et selon quel échéancier renforce la crédibilité de l'institution, puisqu'il engage le MDN et les FAC à respecter un calendrier précis et permet au public de savoir à quoi s'attendre. Dans les communications bilingues, le fait de s'exprimer avec la même clarté dans les deux langues officielles témoigne d'un souci d'inclusion et contribue à renforcer la confiance. Lorsque des communautés autochtones sont concernées, un dialogue direct avec leurs dirigeants, mené de manière culturellement adaptée et, au besoin, par l'intermédiaire de personnes de confiance, renforce la légitimité des messages diffusés et favorise l'adoption de réflexes de vérification de l'information.

La vérification dans la chaîne de commandement

Les contenus synthétiques n'ont pas besoin de tromper l'ensemble d'une formation pour produire leurs effets. En situation opérationnelle, même un bref instant de doute peut perturber une action coordonnée. Lorsque de nombreux éléments doivent se déplacer de concert, l'hésitation d'une seule unité peut briser l'élan, accroître les risques et offrir à l'adversaire une marge de manœuvre. Le danger ne réside pas dans une désinformation à grande échelle, mais dans les petites fissures de confiance qui peuvent se propager au sein d'une formation lorsque l'on ne peut pas se fier immédiatement à l'information. Ce risque n'a rien de nouveau.

Les forces armées ont toujours dû s'assurer de l'authenticité des ordres. Par le passé, les unités recouraient à des indicatifs d'appel, à des mots de code ou même à des émissaires pour confirmer les instructions. Pendant la Seconde Guerre mondiale, par exemple, les procédures d'authentification par sommation et réponse constituaient une mesure de sécurité courante. Aujourd'hui encore, les contrôles radio demeurent une discipline de base.²² Le principe est demeuré le même : peu importe l'urgence de la situation, les unités doivent avoir la certitude que les ordres reçus sont authentiques. Les moyens de communication modernes ont accéléré la circulation de l'information, mais ils ont également multiplié les points d'entrée par lesquels un message faux ou qui a été manipulé peut s'introduire dans le système. À l'ère des contenus synthétiques, la différence tient au réalisme des faux ordres et au peu de temps dont disposent les destinataires pour en vérifier l'authenticité.²³

Un ordre inattendu reçu au cours d'une manœuvre illustre bien cette réalité. Le message peut sembler authentique, tant par sa forme que par son contenu. Toutefois, si son moment de diffusion soulève des doutes et qu'aucune procédure de vérification n'a été prévue, la décision la plus prudente consiste souvent à suspendre l'action jusqu'à ce qu'une autorité supérieure confirme l'ordre.²⁴ Si l'ordre s'avère authentique, cette attente aura déjà fait perdre un temps précieux. S'il est faux, l'unité aura évité une erreur, mais au prix d'un ralentissement et d'une perte d'initiative. Dans les deux cas, l'incertitude a un coût. Dans un environnement où le rythme des opérations est soutenu, quelques secondes d'hésitation peuvent modifier l'issue d'un engagement, faire basculer l'initiative ou créer une occasion dont l'adversaire peut tirer parti.

Les pratiques de la défense doivent donc privilégier des méthodes de confirmation simples et rapides. Un signal convenu à l'avance, un bref échange au moyen d'un canal secondaire ou toute autre procédure préétablie peuvent dissiper le doute en quelques secondes. Ces mesures de protection ne sont pas nouvelles. Les contrôles radio, les procédures d'authentification par sommation et réponse ainsi que la confirmation au moyen de canaux secondaires font depuis longtemps partie des pratiques courantes. Ce qui a changé, c'est le contexte opérationnel. L'IA générative soulève de nouveaux défis auxquels les procédures existantes n'ont pas été conçues pour répondre : des enregistrements audio synthétiques reproduisant avec une grande fidélité la voix d'un commandant, des vidéos truquées montrant en apparence la transmission d'ordres ou encore des messages texte qui imitent avec précision le style et la présentation des communications légitimes.

Les procédures actuelles du MDN et des FAC reposent sur l'hypothèse selon laquelle les communications sont généralement fiables, à moins qu'un motif précis ne justifie le doute. Dans un contexte où des contrefaçons convaincantes peuvent être produites rapidement et à grande échelle, cette hypothèse ne tient plus. Le problème ne réside pas dans l'absence de procédures

de vérification, mais dans le fait qu'elles ne sont pas appliquées de façon systématique lorsque l'information provient de canaux familiers. La formation met souvent l'accent sur la vérification d'ordres manifestement suspects, comme ceux qui arrivent par des moyens inhabituels ou qui contredisent les plans connus, mais elle ne prévoit pas toujours des exercices portant sur des instructions plausibles qui auraient été subtilement manipulées.

De plus, les contraintes opérationnelles peuvent réduire l'efficacité des procédures existantes. Durant des urgences au pays, comme les inondations ou les feux de forêt, les dommages causés aux infrastructures peuvent compromettre les canaux de communication secondaires et rendre plus difficile la confirmation indépendante des ordres. De la même façon, des contenus, manipulés au moyen de l'IA générative, peuvent diffuser de faux renseignements qui nuisent aux opérations des FAC, notamment de fausses alertes concernant une catastrophe, ce qui ralentit les interventions.²⁵ Dans les opérations de coalition, les différences entre les procédures nationales ou les barrières linguistiques peuvent ralentir les vérifications au moment où la rapidité est la plus essentielle. Enfin, dans les opérations de combat menées à un rythme élevé, la pression d'agir rapidement peut l'emporter sur le réflexe de vérifier un ordre, surtout lorsqu'il semble provenir d'une source digne de confiance.

Il ne s'agit donc pas d'inventer de nouvelles procédures, mais d'intégrer systématiquement les procédures existantes aux pratiques courantes, en les adaptant aux menaces que présentent les contenus synthétiques. Cela suppose de mettre en pratique les procédures de vérification non seulement pour les ordres manifestement suspects, mais aussi pour les instructions apparemment ordinaires reçues au cours des exercices. Cela suppose également de vérifier et d'entretenir les canaux de communication secondaires avec la même rigueur que les canaux principaux. Enfin, cela exige de former le personnel à reconnaître que, dans le contexte actuel, la vérification n'est pas un signe d'hésitation, mais de professionnalisme, au même titre que le maniement des armes ou la navigation.

Le leadership joue un rôle déterminant dans cette discipline. Les commandants doivent établir clairement que tout ordre inhabituel doit être vérifié et que la vérification sous pression témoigne non pas d'une faiblesse, mais d'un comportement professionnel.²⁶ Les unités qui répètent ces procédures durant les exercices les appliqueront naturellement en opération. Lorsque les dirigeants appellent constamment que la vérification fait partie des attentes et qu'ils la reconnaissent comme un signe de bon jugement plutôt que d'hésitation, la culture de toute la formation évolue progressivement. Il en résulte non seulement une diminution des erreurs, mais aussi le maintien de la confiance au sein de la chaîne de commandement lorsque des adversaires cherchent à semer la confusion.

L'intégration de la confiance aux politiques, à la formation et au leadership

La crédibilité ne peut pas reposer uniquement sur la technologie. Elle doit être renforcée par l'ensemble des leviers de la défense : les politiques, la formation et les pratiques de leadership. Pour demeurer utiles, les lois et les politiques n'ont pas à suivre chaque évolution technologique. Elles doivent surtout donner des orientations claires et inspirer confiance à ceux qui prennent des décisions et qui communiquent au nom de l'institution. Pour le MDN et les FAC, cela signifie que la doctrine, les directives et les procédures opérationnelles normalisées doivent tenir compte du fait que les contenus synthétiques ne constituent plus une anomalie, mais une caractéristique permanente de l'environnement informationnel. Les politiques qui reposaient autrefois sur l'hypothèse que l'information était digne de confiance jusqu'à preuve du contraire doivent désormais partir du principe qu'elle peut être contestée.

Les politiques, à elles seules, ne suffisent toutefois pas. C'est grâce à la formation que les principes deviennent des réflexes. De la même façon que les militaires apprennent à effectuer des contrôles radio ou à effectuer des exercices de routine, le personnel du MDN et des FAC peut apprendre à réagir sans hésitation devant une information ambiguë. Un officier de quart confronté à une vidéo suspecte devrait immédiatement savoir à qui signaler l'incident et quelles mesures prendre. Un commandant qui reçoit un ordre inhabituel devrait avoir le réflexe d'en confirmer l'authenticité au moyen d'un canal secondaire.

Le problème n'est pas l'absence de ces connaissances, mais plutôt le fait qu'elles ne sont pas mises en pratique de façon régulière dans des conditions réalistes. À l'heure actuelle, la formation traite souvent la vérification de l'information comme une préoccupation secondaire, abordée en salle de classe plutôt qu'intégrée dans les exercices sur le terrain. Le personnel peut savoir, en théorie, à qui s'adresser lorsqu'il est confronté à un contenu suspect, mais sans mise en pratique régulière dans des situations de stress, cette connaissance ne se transforme pas en réflexe. Les comptes rendus après action d'exercices récents ont relevé des cas où des unités ont hésité ou pris des décisions à partir d'informations non vérifiées parce que les procédures de vérification, bien que connues, n'étaient pas suffisamment ancrées dans les habitudes de travail.²⁷

Ces situations ne devraient pas être laissées à l'improvisation sur le terrain. Les procédures de vérification devraient être intégrées à tous les niveaux de formation, depuis l'instruction de base jusqu'aux grands exercices interarmées, afin que les membres des FAC les appliquent aussi spontanément que les manœuvres de combat, la navigation ou les procédures radio.

Les officiers des affaires publiques devraient également disposer, à l'avance, de messages préapprouvés, leur permettant d'intervenir rapidement lorsque des contenus faux ou trompeurs circulent. Ainsi, ils n'auraient pas à attendre des autorisations

juridiques ou stratégiques en pleine crise, mais pourraient immédiatement signaler l'existence de contenus contestés, avertir le public que leur authenticité ou leur exactitude n'a pas encore été établie et l'orienter vers des sources officielles fiables où seront publiées les mises à jour. La préparation préalable de ces messages évite que le silence soit interprété comme une confirmation et permet au MDN et aux FAC d'intervenir d'emblée avec clarté et assurance. Pris isolément, ces gestes peuvent sembler modestes. Ensemble, ils créent un état de disponibilité opérationnelle qui permet aux opérations et aux communications de se poursuivre avec constance, même lorsque des adversaires cherchent à semer la confusion. Des exercices reproduisant des communications falsifiées et des contenus synthétiques permettraient aux équipes des affaires publiques d'intégrer les procédures de vérification avec autant d'aisance que les fantasmes maîtrisent le maniement des armes.

Le leadership constitue le lien qui transforme les principes en habitudes. Lorsque les officiers supérieurs et les dirigeants démontrent, par leur exemple, une vérification rigoureuse sous pression, leurs subordonnés y voient un comportement professionnel plutôt qu'un signe d'hésitation. Un commandant qui exige une confirmation rapide avant d'exécuter un ordre inhabituel établit une norme qui se diffuse dans toute la formation. Un responsable des affaires publiques qui corrige une déclaration avec la même rapidité et la même visibilité que lors de sa diffusion initiale montre que la crédibilité repose sur la franchise. Dans une culture militaire, où le ton et le rythme donnés par les dirigeants influencent l'ensemble de la chaîne hiérarchique, ces exemples se propagent rapidement.

En définitive, la confiance doit être intégrée à tous les échelons de la défense : inscrite dans la doctrine, renforcée par une formation régulière et incarnée par les dirigeants, tant en période normale qu'en situation de crise. Ensemble, ces trois piliers, soit les politiques, la formation et le leadership, permettent aux FAC d'aborder les interférences fondées sur des contenus synthétiques non pas comme une menace improvisée, mais comme une réalité opérationnelle à laquelle elles sont pleinement préparées.

La mesure d'une norme canadienne de réussite

Le MDN et les FAC possèdent une longue expérience de l'évaluation de la disponibilité opérationnelle, et cette même rigueur doit s'appliquer à l'environnement informationnel.²⁸ Le premier indicateur est le temps. L'institution doit mesurer le délai nécessaire pour classer un contenu suspect, fournir une évaluation interne du degré de confiance qu'il inspire et diffuser une mise à jour publique crédible. Elle doit également mesurer le temps requis pour confirmer ou écarter des ordres inhabituels au moyen des procédures établies, ainsi que la fréquence à laquelle ces procédures sont mises en pratique durant les exercices. De la même façon que les rapports sur la disponibilité opérationnelle



Un observateur-contrôleur-entraîneur (OCE) responsable de l'évaluation de l'ex GLOBAL RESOLVE, suit et met à jour les mouvements des troupes dans le secteur d'entraînement au moyen d'une tablette de la trousse d'assaut tactique (TAK), ce qui permet la communication en temps réel entre différents éléments d'OCE sur le terrain. Image prise dans la zone d'entraînement du Yukon près de Fairbanks, en Alaska, le 17 février 2026.

Cpl Dustin LeVasseur Pearce

mesurent les réserves de munitions, l'état de service des équipements ou les effectifs disponibles, le MDN et les FAC peuvent évaluer leur préparation informationnelle en fonction de la rapidité et de la fiabilité avec lesquelles ils valident ou rejettent des contenus contestés.²⁹

Le rendement doit s'améliorer de façon constante, comme dans les autres domaines de la disponibilité opérationnelle. Par exemple, si une formation met actuellement vingt minutes à transmettre un ordre suspect au niveau supérieur et à le confirmer, les exercices devraient viser à réduire ce délai à dix minutes, puis à cinq, sans compromettre l'exactitude ni la sécurité. Si les équipes des affaires publiques ont besoin d'une heure pour coordonner une première déclaration lors d'une urgence au pays, l'objectif devrait être de ramener ce délai à quelques minutes grâce à des messages préapprouvés, à une délégation claire des pouvoirs et à des mécanismes d'escalade bien établis. Chaque exercice devient ainsi une occasion de raccourcir les délais tout en renforçant la confiance.

Des sondages et des mécanismes de rétroaction peuvent également enrichir cette évaluation. Il conviendrait notamment de demander à la population canadienne si elle sait où trouver les communications réelles du MDN et des FAC et si elle est en mesure de les reconnaître. Les journalistes et les partenaires de la société civile pourraient également être consultés afin de déterminer si les outils de vérification sont accessibles et fiables. Les alliés pourraient, quant à eux, indiquer si les méthodes canadiennes sontinteropérables avec les leurs et s'ils accordent immédiatement leur confiance aux communications canadiennes dans un contexte multinational. Bien que qualitatives, ces formes d'évaluation sont aussi essentielles à la résilience que les indicateurs quantitatifs. Les travaux des chercheurs qui étudient

la confiance envers les institutions et leur crédibilité offrent d'ailleurs des cadres utiles pour mesurer ces dimensions.³⁰

Le succès ne se traduira pas par la disparition des faux contenus. Ils continueront d'apparaître, et les adversaires continueront d'innover. Le succès se mesurera plutôt à la capacité du Canada de réagir avec calme, de communiquer rapidement et de préserver la confiance lorsque des messages falsifiés apparaissent. Concrètement, cela signifie moins d'interruptions opérationnelles causées par des ordres non authentifiés, moins de situations où de fausses alertes circulent plus vite que les communications officielles lors d'urgences au pays et moins d'occasions où des récits fabriqués détournent l'attention des objectifs d'un exercice ou d'un déploiement allié. Lorsqu'ils sont suivis de façon constante, ces indicateurs permettent à la défense de déterminer non seulement si elle est prête, mais aussi si la population canadienne et les alliés ont confiance dans cet état de préparation.

Conclusion

L'intelligence artificielle générative a transformé les conditions dans lesquelles la vérité doit se frayer un chemin pour capter l'attention. Elle a rendu les faussetés peu coûteuses, rapides à produire et convaincantes. Cette réalité touche au cœur même de l'efficacité militaire.³¹ Lorsqu'un message falsifié peut ralentir une prise de décision, lorsqu'une vidéo fabriquée de toutes pièces peut fragiliser l'unité des alliés ou lorsqu'une fausse alerte peut exposer des Canadiens à un danger, les adversaires ont atteint leur objectif sans avoir à tirer un seul coup de feu. C'est dans cet environnement concurrentiel que les FAC évoluent désormais. Le Canada n'est pas démuni dans cette lutte. La défense n'a pas à éliminer chaque faux contenu; elle doit démontrer l'authenticité de l'information avant que les faussetés ne se propagent. Cela exige des commandants qui s'attendent à ce que l'information soit vérifiée avant toute manœuvre, des équipes des affaires publiques qui communiquent rapidement et avec franchise, ainsi que des politiques et des outils qui font de l'authentification une pratique courante. Cela exige également des dirigeants qui appliquent la même rigueur à leurs communications qu'à la conduite des opérations. Enfin, cela signifie de faire en sorte que la voix du MDN et des FAC soit immédiatement reconnaissable dans tous les contextes, que ce soit dans les postes de commandement du NORAD, dans les collectivités nordiques, lors de crises au pays ou au cours d'opérations menées en coalition à l'étranger.

Le MDN et les FAC ont toujours fondé leur identité sur le professionnalisme, l'intégrité et la capacité d'agir sous pression.³² Dans les luttes informationnelles qui se déroulent aujourd'hui, ces mêmes qualités constituent le fondement de leur avantage. En démontrant l'authenticité de leurs communications, en préservant le rythme des opérations et en s'exprimant d'une voix qui représente les valeurs canadiennes d'honnêteté et de respect, le MDN et les FAC doivent se protéger contre la tromperie et défendre la démocratie qu'ils servent.

Notes

- 1 Joseph Vossler, Gerald Mazur, Andre Slonopas, Danyl Miller, Edward Olbrych, Aaron Sweeney, et Jacob Strahan, « Artificial Intelligence as a Force Multiplier in U.S. Military Information Campaigns », *Cybersecurity and Information Systems Information Analysis Center (CSIAIC)*, 28 octobre 2024, à l'adresse : <https://csiac.dtic.mil/articles/artificial-intelligence-as-a-force-multiplier-in-u-s-military-information-campaigns/>.
- 2 Cole Stryker et Mark Scapicchio, « What Is Generative AI? », *IBM Think*, 22 mars 2024, à l'adresse : <https://www.ibm.com/think/topics/generative-ai>.
- 3 Service canadien du renseignement de sécurité, « Répercussions des hypertrucages sur la sécurité nationale », gouvernement du Canada, 14 juillet 2025, à l'adresse : <https://www.canada.ca/fr/service-renseignement-securite/organisation/publications/evolution-de-la-desinformation-un-avenir-hypertrucue-repercussions-des-hypertrucages-sur-la-securite-nationale.html>.
- 4 Akshay Kulkarni, « BC Wildfire Service Faces Challenges from AI-Generated Misinformation », *CBC News*, 6 août 2025, à l'adresse : <https://www.cbc.ca/news/canada/british-columbia/bc-wildfire-service-ai-misinformation-1.7602041>.
- 5 Centre canadien pour la cybersécurité, « Évaluation des cybermenaces nationales 2025-2026 », gouvernement du Canada, 30 octobre 2024, à l'adresse : <https://www.cyber.gc.ca/sites/default/files/evaluation-cybermenaces-nationales-2025-2026-f.pdf>.
- 6 « An existential threat: Disinformation 'single biggest risk' to Canadian Democracy », *Digital Forensic Research Lab (DFRLab)*, 19 mars 2024, à l'adresse : <https://dfrlab.org/2025/03/19/canada-disinfo-existential-threat/>.
- 7 National Security Agency, Federal Bureau of Investigation, et Cybersecurity and Infrastructure Security Agency, *Contextualizing Deepfake Threats to Organizations*, 12 septembre 2023, à l'adresse : <https://media.defense.gov/2023/Sep/12/2003298925-1-1/O/CSI-DEEPPAKE-THREATS.PDF>.
- 8 *Increasing Threats of Deepfake Identities*, Department of Homeland Security, consulté le 29 septembre 2025, à l'adresse : https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf.
- 9 Di Cooke, Abigail Edwards, Alexis Day, Devi Nair, Sophia Barkoff, et Katie Kelly, *Crossing the Deepfake Rubicon: The Maturing Synthetic Media Threat Landscape*, Center for Strategic and International Studies, 1^{er} novembre 2024, à l'adresse : <https://www.csis.org/analysis/crossing-deepfake-rubicon>.
- 10 Bobby Chesney et Danielle Citron, « Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security », *California Law Review* 107, n° 6, décembre 2019, à l'adresse : <https://www.californialawreview.org/print/deep-fakes-a-looming-challenge-for-privacy-democracy-and-national-security>. Voir également Vaccari, Cristian et Andrew Chadwick, « Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News », *Social Media + Society*, 6(1), 2020.
- 11 Akshay Kulkarni, « AI-Generated Media and Misinformation of N.W.T. Wildfires Circulating, Fire Officials Warn », *CBC News*, 6 août 2025, à l'adresse : <https://www.cbc.ca/news/canada/north/ai-generated-media-and-misinformation-of-n-w-t-wildfires-circulating-fire-officials-warn-1.7623579>.
- 12 Alexander Dalziel et Daniel Nikoula, *Polarized: Climate Change, Geopolitics and Disinformation in the Arctic*, Laboratoire sur l'intégrité de l'information de l'Université d'Ottawa, juillet 2025, à l'adresse : <https://infolab.uottawa.ca/common/Uploaded%20files/PDI%20files/Polarized-EN-FINAL.pdf>.
- 13 Rob McMahon, Michael B. McNally, Eric Nitschke, Kyle Napier, María Alvarez Malvido, et Murat Akçayir, « Codesigning Community Networking Literacies with Rural/Remote Northern Indigenous Communities in Northwest Territories, Canada », *Journal of Computer-Mediated Communication* 29, n° 1, janvier 2024, à l'adresse : <https://doi.org/10.1093/jcmc/zmad042>.
- 14 Ministère de la Défense nationale, « Programme de réconciliation avec les peuples autochtones du ministère de la Défense nationale – Subventions et contributions », Gouvernement du Canada, 27 mars 2025, à l'adresse : <https://www.canada.ca/fr/ministere-defense-nationale/programmes/financement-reconciliation-autochtones.html>.
- 15 Jayde Lavoie, Jill Barclay, et Wilfrid Greaves, *Improving the Canadian Armed Forces' Recruitment and Retention of Indigenous People: Best Practices from the New Zealand Defence Force*, North American and Arctic Defence and Security Network, Queen's University, 8 septembre 2020, à l'adresse : https://www.naadsn.ca/wp-content/uploads/2020/09/20-September_Policy-Brief-CAF-1.pdf.
- 16 Ministère de la Défense nationale, « Déclaration conjointe sur la modernisation du NORAD », Gouvernement du Canada, 14 août 2021, à l'adresse : <https://www.canada.ca/fr/ministere-defense-nationale/houvelles/2021/08/declaration-conjointe-sur-la-modernisation-du-norad.html>.
- 17 Jill Goldenziel et Daniel Grant, « Information Resilience: Countering Disinformation and Its Threat to the U.S. Alliance System », *War on the Rocks*, 15 novembre 2023, à l'adresse : <https://warontherocks.com/2023/11/information-resilience-countering-disinformation-and-its-threat-to-the-u-s-alliance-system/>.
- 18 Patrick Samaha, « Weaponized AI, The New Frontline in Global Disinformation Warfare », *NATO Association of Canada*, 24 juin 2025, à l'adresse : <https://natoassociation.ca/weaponized-ai-the-new-frontline-in-global-disinformation-warfare/>.
- 19 Pour connaître les normes actuelles et les initiatives en cours, voir *Content Authenticity Initiative* (CAI), qui élabore des normes techniques relatives à la provenance des contenus (contentauthenticity.org), ainsi que Coalition for Content Provenance and Authenticity (C2PA), qui fournit des spécifications pour l'intégration de métadonnées cryptographiques aux médias numériques (c2pa.org). Le Centre d'excellence OTAN pour la communication stratégique a également publié des orientations sur la lutte contre la désinformation dans les contextes militaires (stratcomcoe.org).
- 20 Ministère de la Défense nationale, *Stratégie de communication de l'Armée canadienne 2024-2026*, gouvernement du Canada, 15 juillet 2025, à l'adresse : <https://www.canada.ca/fr/armee/services/pour-le-soldat/strategie-de-communication-de-l-armee-canadienne-2024-2026.html>.
- 21 Eric J.G. Storm, *Needing Unified Direction: Developing Capabilities for Operations in the Information Environment*, Collège des Forces canadiennes, 2025, à l'adresse : <https://www.cfc.forces.gc.ca/259/290/950/305/StormSF50DL.pdf>.
- 22 George I. Back et George Raynor Thompson, « Military Communication », *Encyclopaedia Britannica*, consulté le 29 septembre 2025, à l'adresse : <https://www.britannica.com/technology/military-communication>.
- 23 Di Cooke, Abigail Edwards, Alexis Day, Devi Nair, Sophia Barkoff, et Katie Kelly, *Crossing the Deepfake Rubicon: The Maturing Synthetic Media Threat Landscape*, Center for Strategic and International Studies, 1^{er} novembre 2024, à l'adresse : <https://www.csis.org/analysis/crossing-deepfake-rubicon>.
- 24 Daniel L. Byman, Chongyang Gao, Chris Meserole, et V. S. Subrahmanian, *Deepfakes and International Conflict*, Brookings Institution, janvier 2023, à l'adresse : https://www.brookings.edu/wp-content/uploads/2023/01/FP_20230105_deepfakes_international_conflict.pdf.
- 25 Des incidents récents montrent comment l'intelligence artificielle générative amplifie les risques de mésinformation : durant les feux de forêt de 2025 dans les Territoires du Nord-Ouest et en Colombie-Britannique, des images générées par l'IA ont exagéré l'ampleur des dégâts et ont largement circulé dans les médias sociaux. Voir : *N.W.T. fire officials warn of AI-generated images, misinformation circulating online* | CBC News; *AI-generated wildfire images spreading misinformation in B.C., fire officials warn* | CBC News. En 2022, une vidéo hypertrucquée, montrant le président Zelenskyy, exhortant les troupes ukrainiennes à se rendre, a circulé en ligne dans le but de miner le moral pendant les combats. Voir : *Une vidéo hypertrucquée montrant la capitulation de Volodymyr Zelenskyy inquiète les experts* : NPR.
- 26 Gen. Gary Brito, « Professionalism Is the Foundation of the Army and We Will Strengthen It », *War on the Rocks*, 18 mars 2024, à l'adresse : <https://warontherocks.com/2024/03/professionalism-is-the-foundation-of-the-army-and-we-will-strengthen-it/>.
- 27 Bien que les comptes rendus précis après action demeurent classifiés, cette observation concorde avec les conclusions d'exercices de l'OTAN, portant sur la lutte contre les menaces hybrides, selon lesquelles la vérification de l'information est un aspect auquel la formation devrait accorder une plus grande attention. Voir Centre d'excellence OTAN pour les communications stratégiques, *Hybrid Threats: A Strategic Communications Perspective*, 2019.
- 28 *Léthos des Forces armées canadiennes : Digne de servir*, ministère de la Défense nationale, 19 juillet 2023, à l'adresse : https://www.canada.ca/content/dam/dnd-mdn/documents/reports/Lethos_des_Forces_armees_canadiennes_-_digne_de_servir_FINAL.pdf.
- 29 Ministère de la Défense nationale, « Directive du CEMD/SM sur la posture de la force et la disponibilité opérationnelle (PF&DO) des FAC pour 2024-2025 », Gouvernement du Canada, 12 mars 2025. Protocole de transfert hypertexte sécurisé : <https://www.canada.ca/fr/ministere-defense-nationale/organisation/politiques-normes-directives-sm-cemd/directive-cemd-sm-posture-force-disponibilite-operationnelle-fac.html>.
- 30 Mayer, R. C., Davis, J. H., et Schoorman, F. D. An integrative model of organizational trust. *Academy of Management Review*, 20(3), 1995, 709-734; et Grimmelikhuijsen, S., et Knies, E. Validating a scale for citizen trust in government organizations. *International Review of Administrative Sciences*, 83(3), 2017, 583-601.
- 31 Austin Coombs, « Persuade, Change, and Influence with AI: Leveraging Artificial Intelligence in the Information Environment », *Modern War Institute*, 25 octobre 2024, à l'adresse : <https://mwi.westpoint.edu/persuade-change-and-influence-with-ai-leveraging-artificial-intelligence-in-the-information-environment/>.
- 32 *Léthos des Forces armées canadiennes : Digne de servir*, ministère de la Défense nationale, 19 juillet 2023, à l'adresse : https://www.canada.ca/content/dam/dnd-mdn/documents/reports/Lethos_des_Forces_armees_canadiennes_-_digne_de_servir_FINAL.pdf.