

Comblent l'écart

Pour la modernisation du NORAD, l'intégration numérique pourrait constituer le défi le plus important et le plus pressant.

Par Grant McDonald et Dan Doran



La mise à jour de la politique de défense en avril 2024 ne faisait aucun doute quant aux achats prioritaires à effectuer au cours des prochaines années : réinvestir dans le matériel pour renforcer les fondations et acquérir de nouvelles capacités en matière de sécurité de l'Arctique, de défense antimissile et de cyber opérations.

Ces priorités ont été appuyées par des programmes précis et des financements planifiés, sur plus de 20 ans, pour des programmes liés aux carrefours de soutien opérationnels nordiques et une station terrienne de satellites dans l'Arctique. Cela s'ajoute aux milliards destinés à la construction d'un nouveau système de satellites mondial et d'un centre de cyberopérations conjoint, et à l'acquisition de missiles de longue portée, de capteurs marins et d'un aéronef de détection aérienne avancée —le tout, en parallèle aux investissements faits pour garder les plateformes existantes opérationnelles d'ici à la mise en service de leurs successeurs de cinquième génération au cours de la prochaine décennie.

Ces engagements reposent sur les 38,6 milliards de dollars déjà attribués à la défense du Nord émanant de la politique de défense *Protection, Sécurité, Engagement* (PSE) visant à permettre au Canada de remplir ses obligations communes dans le cadre du Commandement de la défense aérospatiale de l'Amérique du Nord (NORAD). Même si des critiques ont été formulées par rapport aux dépenses promises ne commençant pas avant 2026, ces engagements importent — surtout à la lumière de l'absence, dans la politique PSE, d'une politique axée sur la numérisation et l'intégration. La mise à jour de la politique de défense contribue grandement à combler l'écart.

Solution centrée sur la position

Face à toutes ces nouvelles vraisemblablement bonnes concernant la modernisation du NORAD et la sécurité du Nord en général, ce qui est moins clair, c'est la façon dont ces nombreuses plateformes d'armes et de capteurs seront synchronisées pour créer un système de structures de prise de décision numérique entièrement intégré, en mesure de gérer efficacement les profils de menace auxquels nous faisons face actuellement ainsi que les menaces de l'avenir activées par IA.

La direction du ministère de la Défense nationale (MDN) ne sera pas étonnée par cette observation, puisqu'elle s'est penchée à parts égales sur les causes de la situation et les moyens d'y remédier dans le Plan de campagne numérique et, plus récemment, dans la Stratégie d'intelligence artificielle des Forces armées canadiennes (FAC).

Par ailleurs, le MDN a déjà déterminé la conclusion souhaitée de son projet visant à procéder à une intégration numérique

complète en vertu de la ligne d'effort 2 du Plan de campagne numérique — surtout pour « concevoir, développer et mettre en service des outils et des concepts de connaissance de la situation tous domaines (CSTD) qui intègrent tous les domaines ». Cela exigera une transformation des concepts opérationnels actuels et une orchestration des activités qui transcendent les domaines, favorisent la réflexion tous domaines et intègrent le chevauchement entre les domaines pour promouvoir l'intégration par la conception — le tout grâce à l'utilisation du Centre Opérations et Renseignement de la Défense nationale (CORDN) comme véhicule d'opérationnalisation, de commande et de contrôle.

Ce sont tous de bons signes. Toutefois, les prochaines étapes du projet d'intégration numérique pourraient être plus complexes — et coûteuses.

Projet loin d'être facile

La réussite de l'intégration numérique nécessitera l'application d'une version légèrement modifiée des cinq lignes d'efforts décrites dans la Stratégie d'intelligence artificielle – le succès de chaque ligne étant étroitement lié à celui des autres lignes :

Mise en service et utilisation de capacités numériquement intégrées

Exécution rigoureuse d'une gestion du changement organisationnel et d'une restructuration des activités

Intégration d'une résilience et d'une fiabilité dans l'ensemble des systèmes

Recrutement des bons talents et efficacité de la formation qui leur sera donnée

Collaboration avec les partenaires ministériels et mobilisation transformationnelle du secteur

Ces principes directeurs n'élimineront pas les risques qui jalonnent le parcours d'intégration numérique, mais ils garderont l'organisation axée sur l'objectif ultime des CSTD. Et même s'ils méritaient chacun leur propre article, nous nous concentrerons sur des questions plus épineuses.

Gestion du changement organisationnel (GCO) et restructuration des activités

Ces deux pratiques distinctes sont étroitement liées au niveau de la planification et de l'exécution. L'intégration numérique devra relever la totalité des défis de GCO décrits dans la Stratégie d'IA ayant trait à l'exécution horizontale, à l'acceptation des perturbations et au besoin de s'adapter. Il faudra adopter ces mentalités pour composer avec les changements de processus qu'entraînera l'intégration numérique des plateformes dont la technologie, datant parfois des années 70 et 80, a été mise à niveau — l'équivalent de passer d'un Commodore 64 à un téléphone intelligent.

Collaboration

L'écart à ce chapitre sera aussi difficile à combler et exigera la création d'une nouvelle relation de confiance entre le MDN, les autres ministères et le secteur. Pour établir des ponts, toutes les parties prenantes devront prendre des risques et alimenter activement les liens professionnels et transformationnels en mesure de susciter la confiance requise pour favoriser l'élaboration de solutions créatives et relever ces défis.

Inconnues connues

Dans son livre intitulé *Hard Things – Entreprendre dans l'incertitude*, Ben Horowitz donne quelques perspectives liées à sa riche expérience d'entrepreneur technologique en série. La première fait directement référence à l'intégration numérique : « La chose difficile à propos des choses difficiles, c'est qu'il n'y a pas de réponse toute faite ou de recette simple. » La deuxième fait référence à la façon d'adresser la première et devrait être un mantra pour les leaders à qui on demande de réaliser une intégration numérique. Ces personnes devraient se poser la question suivante : « Qu'est-ce que je ne fais pas? » Voilà ce que nous encourageons la haute direction des FAC, du gouvernement et du secteur à prendre en considération, ensemble.



Grant McDonald est le leader mondial du groupe sectoriel Aérospatiale et défense de KPMG International. **Dan Doran** est leader du groupe Défense et sécurité nationale chez KPMG au Canada et un vétéran des Forces armées canadiennes. Pour en savoir plus, visitez le www.kpmg.ca. Les opinions exprimées ici sont celles des auteurs et ne reflètent pas nécessairement celles de Canadian Defence Review.

Communiquez avec nous

Grant McDonald

Leader Mondial, Aérospatiale et défense; associé responsable des relations avec les dirigeants, gouvernement du Canada
KPMG au Canada
246-434-3900
grantmcdonald@kpmg.ca

Dan Doran

Directeur, Services-conseils, Solutions pour le secteur public |
Leader, Défense et sécurité nationale
KPMG au Canada
613-845-2064
dandoran@kpmg.ca