



Le 435^e Escadron de transport et de sauvetage procède à l'évacuation de résidents de Norway House, au Manitoba, pendant les feux de forêt, au cours de l'opération LENTUS, dans le nord du Manitoba, le 30 mai 2025.

Aviateur Nicholas Zahari, Service d'imagerie du 17^e Escadron de soutien aux opérations, Winnipeg

Le lien entre le renseignement d'origine électromagnétique et le cyberdomaine au sein des Forces armées canadiennes

LIEUTENANTE-COLONELLE L. J. REDIGER

La lieutenant-colonelle (Lcol) Leslie Rediger a intégré les Forces armées canadiennes en 2001 à titre d'officière du génie électronique et des communications. Elle a obtenu, en 2006, un baccalauréat en génie mécanique du Collège militaire royal du Canada. Au cours des 15 premières années de sa carrière, elle a appuyé les opérations aériennes en qualité d'officière des systèmes de communications et d'information au sein de différentes escadres de l'Aviation royale canadienne et au Quartier général de la 1^{re} Division aérienne du Canada. Elle a été déployée à plusieurs reprises à l'appui des opérations ATHENA et REASSURANCE. En 2016, la Lcol Rediger est passée aux opérations de renseignement d'origine électromagnétique (SIGINT). Elle a alors occupé les fonctions de commandante de l'Escadron de soutien et de commandante adjointe à la Station des Forces canadiennes Leitrim, ainsi que celles de chef d'état-major du SIGINT au Quartier général du Groupe des opérations d'information des Forces canadiennes. Promue à son grade actuel en 2020, elle a commandé la Station des Forces canadiennes Leitrim, de juin 2023 à octobre 2025. À l'heure actuelle, elle est officière de liaison du COMCYBERFAC, au Royaume-Uni. La Lcol Rediger détient une maîtrise ès arts en leadership de l'Université Royal Roads ainsi qu'une maîtrise en études de la défense du Collège des Forces canadiennes.

Protection, Sécurité, Engagement : La politique de défense du Canada, publiée en 2017, présente « l'évolution rapide de la technologie » comme l'un des principaux facteurs de transformation du contexte de sécurité mondial, qui modifie la nature des conflits.¹ Elle souligne également que l'utilisation du cyberspace et des technologies émergentes par les Forces armées canadiennes (FAC) « apporte de nombreux avantages opérationnels, mais engendre aussi des vulnérabilités critiques ».² Ainsi, pour demeurer concurrentielles et défendre les intérêts du Canada, les FAC doivent être en mesure de protéger leurs biens, préserver leur liberté de manœuvre dans le cyberspace et être en mesure de tirer parti de ce contexte opérationnel, tout en étant prêtes à le faire, afin d'exécuter le mandat qui leur est confié.³

Pour « maximiser l'efficacité du Canada dans le cyberspace » dans *Notre Nord, fort et libre : Une vision renouvelée pour la défense du Canada*, le gouvernement du Canada a ordonné aux FAC de créer le Cybercommandement des Forces armées canadiennes (COMCYBERFAC).⁴ Ce nouveau commandement vise à « améliorer la capacité des Forces armées canadiennes à mener des cyberopérations » et « seront ainsi capables de mettre sur pied et d'employer des cyberforces ainsi que d'autres capacités spécialisées sur court préavis, et de contribuer à la promotion des intérêts canadiens ainsi qu'à la protection de l'armée canadienne et des forces alliées et partenaires sur le territoire national et à l'étranger ».⁵

Le COMCYBERFAC a été créé le 26 septembre 2024. Le Groupe des opérations d'information des FAC a alors été élevé du statut de formation de niveau 3 à celui de commandement. Soutenu sur le plan administratif par le Groupe des services numériques, il relève directement du chef d'état-major de la défense.⁶ À titre d'autorité de la défense en matière de cyberopérations, il est chargé de l'emploi, de la mise sur pied, du maintien, de la gestion et du développement des cyberforces qui lui sont attribuées, y compris le renseignement d'origine électromagnétique (SIGINT) et la guerre électronique interarmées.⁷

Quoique ce soit relativement bien connu dans la communauté de la défense que le Centre de la sécurité des télécommunications Canada (CST) est l'organisme du gouvernement du Canada chargé du SIGINT étranger,⁸ on sait moins que les FAC disposent de leur propre unité intégrée de SIGINT. Depuis près de 85 ans, la Station des Forces canadiennes Leitrim mène des opérations de SIGINT pour défendre le Canada.⁹ À première vue, l'intégration de l'organisation de SIGINT des FAC au nouveau commandement des cyberopérations peut sembler inhabituelle, puisqu'il s'agit d'une fonction du renseignement et que les FAC disposaient déjà d'un commandement du renseignement. Toutefois, le SIGINT entretient des liens particulièrement étroits avec les cyberopérations. Ces liens ne cessent de se renforcer et de gagner en importance dans le monde interconnecté et riche en technologies au sein duquel les FAC mènent leurs opérations. Le SIGINT et le cyberdomaine sont les deux faces d'une même médaille : malgré leurs objectifs, leurs pouvoirs et leurs capacités distincts, ils sont indissociables et se

renforcent mutuellement. Le présent article propose une introduction à la relation entre le SIGINT et les cyberopérations dans un contexte militaire. Il vise à illustrer leurs interdépendances et leur caractère complémentaire au sein du nouveau COMCYBERFAC.

Lexique

Pour amorcer cette réflexion, il importe d'abord de définir la terminologie. Les progrès technologiques dans le domaine des renseignements devançant souvent l'évolution de la doctrine. Ainsi, il n'existe aucune définition universellement reconnue de termes comme « cyberspace », « cyberopérations » ou « cyberdomaine ». L'OTAN, les alliés et les partenaires les interprètent de manière quelque peu différente et les emploient souvent de manière interchangeable. Aux fins de la présente discussion, pour garantir la cohérence terminologique, le présent article s'appuie sur la *Banque de la terminologie de la défense* (BTD) du ministère de la Défense nationale.

Le cyberspace et le cyberdomaine

Le terme « cyberspace » désigne l'« environnement physique comprenant toutes les ressources qui traitent, stockent ou communiquent des données numériques ».¹⁰ Contrairement aux autres milieux opérationnels au sein desquels les FAC mènent leurs activités, la terre, la mer, l'air et l'espace, le cyberspace est « omniprésent dans tous les autres environnements ».¹¹ Le cyberdomaine est une notion plus vaste qui intègre non seulement le cyberspace, mais également l'infrastructure qui l'appuie et le rend possible, de même que ses utilisateurs et les activités connexes.¹²

Le cyberspace comprend la couche des cyberpersonnages, qui intègre les profils en ligne et les autres moyens par lesquels les personnes et les objets sont représentés en ligne, tandis que le cyberdomaine s'étend aux humains qui interagissent réellement avec le cyberspace. De même, le cyberspace comprend la couche physique, notamment l'ensemble du matériel informatique, des téléphones, des capteurs et des dispositifs de stockage de données. Le cyberdomaine intègre cette couche ainsi que la couche géographique, qui représente les emplacements physiques où se trouvent les dispositifs du réseau et leur environnement immédiat.¹³

Cyberopérations

Le terme « cyberopération » ou cyberop désigne un vaste éventail d'activités, menées dans le cyberspace afin d'atteindre des objectifs stratégiques et tactiques. Ces activités se divisent en cyberopérations défensives et offensives. Les cyberops défensives visent à préserver et à assurer la liberté d'action dans le cyberspace,¹⁴ notamment en défendant les réseaux et les données contre les adversaires. Les cyberops offensives, en revanche, visent à projeter la puissance dans le cyberspace

afin de produire des effets précis.¹⁵ Elles ont pour objet de perturber, de dégrader ou de détruire la liberté de mouvement de l'adversaire dans le cyberspace, ou encore d'avoir d'autres répercussions, par l'intermédiaire du cyberspace, sur ses activités ou ses capacités.

La dépendance croissante des acteurs étatiques et non étatiques à l'égard du cyberspace, de ses systèmes informatiques intégrés et de ses capteurs a exigé un accroissement proportionnel des capacités en matière de cyberopérations des FAC. Il est essentiel que les FAC puissent défendre leur territoire dans le cyberspace et tirer parti de ce milieu pour atteindre leurs adversaires et agir contre eux. *Protection, Sécurité, Engagement : La politique de défense du Canada* établit comme attente que les cyberforces des FAC soient en mesure « de cibler, d'exploiter, d'influencer et d'attaquer [dans le cyberspace] à l'appui des opérations militaires »,¹⁶ en s'appuyant sur des plateformes émergentes dans les milieux terrestre, maritime, aérien et spatial afin d'intégrer les systèmes de capteurs.¹⁷ La politique de défense souligne également la nécessité d'empêcher l'adversaire d'avoir une incidence sur les capacités C4ISR des FAC (commandement, contrôle, communications, informatique, renseignement, surveillance et reconnaissance), lesquelles sont indispensables à la conduite des opérations des FAC à l'échelle mondiale.¹⁸

Renseignement d'origine électromagnétique

Le terme « renseignement d'origine électromagnétique » intègre tant la discipline du renseignement elle-même que les activités de collecte de renseignements menées dans le cyberspace et dans d'autres parties du spectre électromagnétique, ainsi que les produits qui alimentent le système de renseignement dans son ensemble.¹⁹ Essentiellement, le SIGINT consiste à intercepter, recueillir, décrypter, traduire et analyser des signaux de communication ou des signaux autres que des signaux de communication, puis à produire des rapports qui contribuent au processus général de collecte du renseignement.²⁰ Compte tenu du caractère délicat de ces activités, les processus, les capacités et les produits exigent des mesures particulières de protection et de traitement; ainsi, ils ne peuvent faire l'objet de discussions publiques.²¹

Le SIGINT se divise en trois sous-catégories : le renseignement sur les communications (COMINT), le renseignement électronique (ELINT) et le renseignement tiré de signaux d'instrumentation étrangers (FISINT). Le COMINT est constitué de renseignements recueillis par l'interception de communications électromagnétiques, vocales ou textuelles par exemple, autrement que par leur destinataire prévu.²² L'ELINT est axé sur les émissions électromagnétiques autres que les communications, notamment celles des systèmes radars.²³ Ces émissions peuvent révéler des renseignements sur leur source, notamment la fréquence utilisée, la fréquence de répétition et la direction d'arrivée, entre autres caractéristiques.²⁴ Enfin, le FISINT, domaine plus spécialisé, désigne le « renseignement technique tiré de

l'interception d'émissions électromagnétiques d'origine étrangère associées à l'essai et à l'utilisation de systèmes aérospatiaux, de surface et sous-marins ». ²⁵ Il sert notamment à recueillir des renseignements sur les émissions et les données provenant de systèmes de missiles et de systèmes de contrôle.²⁶ Ensemble, ces trois sous-catégories fournissent les renseignements essentiels à l'atteinte des objectifs de défense nationale et continentale ainsi qu'à l'orientation des opérations de sécurité nationale, de la politique étrangère et de la cybersécurité.²⁷

Le SIGINT a un long historique de clandestinité. Étroitement protégé par les personnes chargées de l'exécuter, il appuie dans l'ombre les opérations des FAC depuis la Seconde Guerre mondiale.²⁸ Pierre angulaire des opérations militaires, le SIGINT permet de mieux comprendre les intentions, les capacités et les activités de l'adversaire. Il appuie ainsi la prise de décisions stratégiques, la défense du continent et la connaissance de la situation des forces déployées à l'échelle mondiale.²⁹

À l'instar des cyberopérations, le SIGINT a pris une importance accrue au sein des opérations des FAC dans le contexte de la guerre moderne, où les progrès technologiques ont transformé le champ de bataille, la stratégie militaire et les activités de collecte du renseignement. L'environnement d'information, de plus en plus interconnecté, crée des vulnérabilités. Il permet à l'entreprise de SIGINT d'accéder aux communications, aux capteurs et aux systèmes d'armes de l'adversaire afin de produire des renseignements essentiels sur ses capacités et ses intentions. L'utilisation considérablement accrue des systèmes des technologies de l'information, des capteurs intégrés et des systèmes de commandement et contrôle a renforcé l'importance du SIGINT pour la défense des biens des FAC et l'exploitation des vulnérabilités de l'adversaire. Elle ouvre ainsi la voie à des cyberactivités défensives et offensives actives qui exploitent ces mêmes vulnérabilités.

Le lien entre le SIGINT et le cyberdomaine

Les opérations de SIGINT tirent parti du cyberspace et des technologies qui y sont intégrées pour exploiter la dépendance de l'adversaire à l'égard des communications numériques, des appareils interconnectés et de l'emploi généralisé de capteurs. Elles permettent ainsi de produire du renseignement dans tous les milieux opérationnels, y compris le cyberspace. Le renseignement issu de ces processus appuie les opérations des FAC à tous les égards, tant sur le plan tactique que sur le plan stratégique. L'interception des communications et des données provenant des capteurs de l'adversaire fournit, en temps réel, du renseignement sur ses positions et ses mouvements dans tous les milieux (aérien, terrestre, maritime, spatial et cyberspatial), ce qui éclaire les évaluations de la menace et les cycles de ciblage des décideurs. Sur le plan stratégique, elle façonne la connaissance de la situation en révélant les intentions, les capacités et les menaces émergentes de l'adversaire.³⁰

Quoique le SIGINT et les cyberopérations reposent tous deux sur des technologies numériques et s'exercent dans le cyberdomaine, leur portée, leurs méthodes et leurs objectifs diffèrent. Le SIGINT est principalement axé sur la collecte passive de renseignements et l'analyse de transmissions, tandis que les cyberopérations peuvent être passives ou actives. Les cyberopérations défensives visent à protéger les systèmes informatiques et les systèmes de communication contre les intrusions, à garantir leur protection proactive et à intervenir en cas d'attaque. Les cyberopérations offensives, quant à elles, cherchent à pénétrer, à manipuler et à exploiter les systèmes de l'adversaire. La conduite de cyberopérations exige toutefois une compréhension approfondie des auteurs de la menace, de l'infrastructure numérique et de ses vulnérabilités éventuelles. Le SIGINT peut appuyer ces activités en fournissant le renseignement requis pour identifier les cibles et évaluer les menaces.

Cyberopérations appuyées par le SIGINT

Qu'elles soient défensives ou offensives, les cyberopérations reposent largement sur un renseignement exact et obtenu en temps opportun. Le SIGINT constitue un élément fondamental de l'appui aux cyberopérations : l'interception et l'analyse de signaux de communication et d'autres transmissions permettent de cerner les vulnérabilités des systèmes, de détecter des tendances dans les cyberactivités et de mieux comprendre les auteurs de la menace. Les cyberopérateurs des FAC doivent être en mesure de comprendre la topologie des réseaux ciblés, notamment l'interconnexion des systèmes, les protocoles employés ainsi que l'emplacement et la nature des vulnérabilités au sein de ces réseaux.³¹

Dans le cadre des cyberopérations défensives, le SIGINT peut révéler la structure et le comportement de l'environnement numérique, de même que les intentions et les capacités des adversaires et d'autres auteurs de la cybermenace. Par ailleurs, il peut contribuer au renseignement sur les menaces, en repérant des indicateurs de compromission, ce qui permet aux FAC de renforcer la sécurité des systèmes, de déployer des contre-mesures et d'intervenir en cas d'intrusion. Dans le cadre des cyberopérations offensives, le SIGINT peut éclairer le choix des cibles, le moment d'intervention et les tactiques à employer afin que les cyberactions soient précises et efficaces.

Le SIGINT peut également faciliter l'attribution, c'est-à-dire le processus qui consiste à déterminer l'auteur d'une cyberattaque. L'attribution repose sur la corrélation entre les communications interceptées et les comportements connus des auteurs de la menace. Cette fonction revêt une importance particulière dans le contexte actuel des menaces, où les acteurs étatiques et non étatiques utilisent des méthodes perfectionnées pour dissimuler leur identité.

Le SIGINT est essentiel à la cartographie de la topologie des réseaux et à la compréhension des cybermenaces. Son rôle dans le cadre des cyberopérations va au-delà de l'interception,

car il permet une analyse approfondie qui éclaire la planification stratégique et renforce la connaissance de la situation des décideurs. Pour les FAC, ce lien est mis en évidence par le regroupement des unités de SIGINT et des cyberunités au sein d'un même commandement. La création du COMCYBERFAC favorise une meilleure communication et une coopération accrue entre ces capacités essentielles sur le plan stratégique.

Soutien des cyberopérations au SIGINT

L'évolution initiale du SIGINT au Canada reposait sur deux objectifs principaux : tirer parti de sa situation géographique particulière pour assurer la défense souveraine du pays, et utiliser cette même situation géographique, de concert avec des initiatives nationales de collecte, afin de participer au partenariat de renseignement du Groupe des cinq avec les États-Unis, le Royaume-Uni, l'Australie et la Nouvelle-Zélande, tout en tirant parti de ce partenariat.³² Ces impératifs existent encore à l'heure actuelle. Le SIGINT est une activité fondamentalement collective, car l'omniprésence des systèmes d'information, des capteurs et des émetteurs rend presque impossible le traitement du déluge de données numériques provenant de toutes ces sources. Repérer, décrypter, analyser et communiquer les renseignements pertinents afin de répondre aux besoins en renseignement et d'appuyer les opérations des FAC représente un défi considérable. La mise en commun de ce fardeau avec des pays partenaires qui partagent les mêmes intérêts accroît le volume de données pouvant être traitées et exploitées. Sans la collaboration des alliés du Canada, ce défi serait vraisemblablement insurmontable, particulièrement lorsque les opérations se déroulent dans le cyberspace. La superficie du Canada et sa proximité avec des pays adverses lui procurent un avantage géographique. Le pays peut ainsi offrir des apports particuliers, accroître sa pertinence dans ce domaine, faciliter l'accès au renseignement de ses partenaires et tirer pleinement parti des capacités du Groupe des cinq afin d'appuyer les opérations des FAC à l'échelle mondiale.³³ Dans un environnement numérique en constante évolution, ce partenariat est plus que jamais essentiel. En investissant à la fois dans des infrastructures souveraines de SIGINT et dans des infrastructures intégrées, le Canada veille à ce que ses apports ne soient pas seulement complémentaires, mais qu'ils fournissent également des renseignements distincts et utiles aux opérations des FAC et du Groupe des cinq. Ces capacités souveraines permettent au Canada d'aligner ses opérations sur les priorités en matière de sécurité nationale, ce qui renforce la pertinence et l'incidence de son renseignement. Leur caractère intégré permet également au Canada de renforcer la défense collective et la mise en commun de renseignements au sein de l'alliance.

Les opérations de SIGINT dépendent fortement d'infrastructures de réseau sécurisées, des télécommunications et des communications radioélectriques, des flux de données provenant de capteurs, de fonctions informatiques complexes, de

l'automatisation, de l'analyse de données et, surtout, de l'intégration et de la communication avec les partenaires et les alliés. Comme cette infrastructure est répartie à l'échelle du pays et du monde, cela pose un défi technique et de sécurité considérable et durable. Toutes ces activités tirent parti du cyberspace et aucune ne serait possible sans l'appui des cyberopérations. Les cyberopérations de l'adversaire constituent une menace importante pour les opérations des FAC, y compris le SIGINT, notamment en refusant ou en manipulant l'information, en menant une collecte rapide ou soutenue, ou en exécutant des activités de tromperie.³⁴

Ce sont les cyberopérations défensives qui garantissent aux opérations de SIGINT la liberté de manœuvre dans le cyberspace, tout en protégeant les biens, les systèmes et les installations essentiels à la recherche, à la détection, à l'analyse et à la diffusion du SIGINT. Par ailleurs, le SIGINT et les cyberopérations offensives concourent à repérer les points d'accès et à comprendre le terrain dans le cyberspace, ce qui permet de recueillir du renseignement et de produire des effets. Ce lien essentiel entre les cyberopérations et le SIGINT garantit l'efficacité et la pérennité de ces deux capacités.

Conclusion

La création du COMCYBERFAC témoigne de la reconnaissance délibérée, par le gouvernement du Canada et les FAC, que le

cyberspace est un milieu opérationnel contesté au sein duquel les FAC doivent pouvoir manœuvrer, défendre leurs positions et produire des effets. Dans ce contexte, l'intégration des capacités de SIGINT et des cybercapacités au sein d'un même commandement constitue une réponse logique aux réalités des conflits modernes. Comme le démontre le présent article, le SIGINT et les cyberopérations sont étroitement interdépendants. Le SIGINT fournit le fondement de renseignement nécessaire à la conduite efficace des cyberopérations défensives et offensives, tandis que les cybercapacités protègent, facilitent et amplifient la collecte et l'analyse du SIGINT. Ensemble, ces deux éléments forment un cycle de renforcement mutuel qui améliore la connaissance de la situation, appuie la prise de décisions, préserve la liberté d'action des FAC dans tous les milieux et facilite la projection de la puissance militaire au moyen du cyberspace.

À mesure que les menaces gagnent en ampleur, en perfectionnement et en rapidité, l'importance de cette relation entre le SIGINT et les cyberopérations ne peut que croître. Le regroupement, au sein du COMCYBERFAC, de l'expertise, des pouvoirs et des capacités permet aux FAC de mieux intégrer le renseignement d'origine électromagnétique et les cyberopérations, de renforcer leurs partenariats avec les alliés et d'intervenir avec détermination dans le cyberdomaine omniprésent. En fin de compte, l'efficacité des cyberforces des FAC ne reposera pas sur la puissance de capacités isolées, mais sur la puissance de la collaboration, de l'intégration et de l'innovation.

Notes

- Gouvernement du Canada, *Protection, Sécurité, Engagement : La politique de défense du Canada* (Ottawa : ministère de la Défense nationale, 2017), 14.
- Ibid.*, 72.
- Gouvernement du Canada, Joint Doctrinal Note (JDN): Cyber Operations 2017-02 2-0, Ottawa : ministère de la Défense nationale, 2017, 1-1.
- Gouvernement du Canada, *Notre Nord, fort et libre : Une vision renouvelée pour la défense du Canada*, Ottawa : ministère de la Défense nationale, 2024, 26.
- Ibid.*, 26.
- Forces armées canadiennes, Military Organization Order 2025001-2025006, 14 juillet 2025.
- Ministère de la Défense nationale, « Message de la SM et de la CEMD : Une nouvelle ère pour le domaine cybernétique : Lancement du Commandement Cyber des Forces armées canadiennes », La Feuille d'érable, 26 septembre 2024. Tiré de <https://www.canada.ca/fr/ministere-defense-nationale/feuille-derable/defense/2024/09/nouvelle-ere-domaine-cybernetique-lancement-commandement-cyber-forces-armees-canadiennes.html>.
- Centre de la sécurité des télécommunications, « Mandat », Gouvernement du Canada, dernière modification le 7 avril 2021. Tiré de <https://www.cse-cst.gc.ca/fr/renseignements-organisationnels/mandat>.
- George T. Fraser et Robert Lynn Wortmann, *History of Canadian Signals Intelligence & Direction Finding*, publié à compte d'auteur, 2005.
- « Cyberspace », Banque de la terminologie de la défense, fiche 694338, consulté le 6 février 2026.
- Canada, JDN: Cyber Operations, 2-1.
- « Cyber Domain », Banque de terminologie de la défense, fiche 694360, consulté le 6 février 2026.
- Canada, JDN: Cyber Operations, 2-3-2.4.
- « DCO », Banque de terminologie de la défense, fiche 693742, consulté le 18 septembre 2025.
- « OCO », Banque de terminologie de la défense, fiche 693752, consulté le 18 septembre 2025.
- Canada, *Protection, Sécurité, Engagement*, 65.
- Ibid.*, 39, 109.
- Ibid.*, 56.
- Gouvernement du Canada, CAF SIGINT Primer, ministère de la Défense nationale, avril 2021, 1.
- Gouvernement du Canada, B-GJ-005-200/FP-001, PIFC 2-0, Le renseignement, Ottawa : ministère de la Défense nationale, 2011, 1-16.
- Gouvernement du Canada, CAF SIGINT Primer, 1.
- Gouvernement du Canada, « COMINT », Banque de la terminologie de la défense, fiche 3843, consulté le 18 septembre 2025.
- « ELINT », Banque de la terminologie de la défense, fiche 507, consulté le 18 septembre 2025.
- Canada, CAF SIGINT Primer, 21.
- « FISINT », Banque de terminologie de la défense, fiche 695891, consulté le 18 septembre 2025.
- Gouvernement du Canada, CAF SIGINT Primer, 21.
- Gouvernement du Canada, B-GJ-005-200/FP-001, PIFC 2-0, Le renseignement, 1-4.
- George T. Fraser et Robert Lynn Wortmann, op.cit.
- Gouvernement du Canada, Centre de la sécurité des télécommunications, « Renseignement étranger », dernière modification le 6 avril 2023. Tiré de <https://www.cse-cst.gc.ca/fr/mission/renseignement-etrange>.
- Centre de la sécurité des télécommunications, « Renseignement étranger ».
- Gouvernement du Canada, JDN: Cyber Operations, 5-14.
- Wesley Wark, « Favourable Geography: Canada's Arctic Signals Intelligence Mission », *Intelligence and National Security* 35, no 3 (2020) : 319-330, DOI : 10.1080/02684527.2020.1724629.
- Maria A. Robson, « The Third Eye: Canada's Development of Autonomous Signals Intelligence to Contribute to Five Eyes Intelligence Sharing », *Intelligence and National Security* 35, no 7 (2020) : 954-969, DOI : 10.1080/02684527.2020.1768477.
- Gouvernement du Canada, JDN: Cyber Operations, 1-1.