

# Note stratégique



## La coopération de renseignement dans un monde multipolaire : Perspectives non américaines

Jonathan Mayne et Marco Munier

*Cette note stratégique fait suite à la [conférence](#) organisée par le Réseau d'analyse stratégique intitulée « La coopération de renseignement dans un monde multipolaire : perspectives non américaines » du 6 mai 2021.*

Cette conférence a réuni d'éminents professionnels et universitaires du renseignement et des études stratégiques dont : [Jill Sinclair](#) du ministère de la Défense nationale, [Daniel Jean](#), ancien conseiller en matière de sécurité nationale et de renseignement auprès du premier ministre du Canada, [Artur Wilczynski](#) du Centre de la sécurité des télécommunications, [Heather De Santis](#) de Sécurité publique Canada, [Björn Fägersten](#) de l'Institut suédois des affaires internationales, [Claudia Hillebrand](#) de l'Université Cardiff, [Gustav Gressel](#) du Conseil européen des relations étrangères, [Adriana Seagle](#) de l'Université Bellevue, [Sarah-Myriam Martin-Brûlé](#) de l'Université Bishop's, [Stephanie Carvin](#) de l'Université Carleton, [Thomas Juneau](#) de l'Université d'Ottawa, [Reg Whitaker](#) de l'Université Victoria, [Nancy Teeple](#) du Collège militaire royal du Canada, [Patrick F. Walsh](#) de l'Université Charles Sturt et [Justin Massie](#) de l'Université du Québec à Montréal.

Même si elle est souvent peu traitée, la coopération en matière de renseignement n'est pas un nouveau phénomène. En particulier, depuis l'émergence du terrorisme international, la coopération en matière de renseignement s'est étendue à un niveau mondial. Cette menace continue de poser un défi aux services de renseignement, mais la transition actuelle de la puissance et l'intensification de la concurrence stratégique entre les grandes puissances exigent un changement de la vision de la coopération en matière de renseignement.

Dans ce cadre, la conférence visait à établir une meilleure compréhension de la montée de la concurrence entre les grandes puissances dans un monde numérique. Ce phénomène soulève de nombreux défis dans une société libre et ouverte qui nécessite une coopération en matière de renseignement pour les relever. Quatre grands thèmes ont été abordés lors de cette conférence : les défis de la coopération de renseignement, l'Union européenne (UE) en tant qu'acteur du renseignement, le rôle du concept de Renseignement, Surveillance et Reconnaissance sur la stabilité stratégique et l'avenir du Groupe des cinq (*Five Eyes*), dont le Canada et l'Australie, en matière de coopération de renseignement.

Dès lors, on peut tirer de cette note stratégique le manque de coopération internationale sur des sujets d'intérêt stratégique à l'heure de la compétition entre les grandes puissances comme les nouvelles technologies et les réticences nationales à pleinement partager les renseignements essentiels, sauf en cas de crises. Cette note stratégique met également en lumière le manque d'imputabilité et de surveillance

des activités de partage de renseignements. Toutefois, il n'en demeure pas moins que la coopération continue de s'accroître, et des acteurs comme l'UE vont jouer un rôle de plus en plus important dans le milieu du renseignement et de la coopération transnationale de renseignement. Cela dit, avec la croissance importante des besoins de coopération, de nombreux défis émergent pour des pays comme le Canada, qui dépend des capacités de renseignement d'alliés plus puissants. Dans un tel cas, il faut renforcer la capacité d'identifier nos propres menaces et intérêts nationaux, tout en continuant la coopération avec nos alliés en apportant une expertise particulière.

Nous recommandons enfin pour le Canada une *canadianisation* du renseignement, c'est-à-dire d'orienter la collecte et l'analyse des renseignements étrangers vers une poursuite plus claire et plus ferme des intérêts proprement canadiens, contrairement à la réception de renseignements bruts ou finis qui peuvent ou non refléter les besoins et intérêts canadiens. À cette recommandation s'ajoutent aussi plusieurs initiatives intéressantes, notamment l'engagement plus prononcé et horizontal de la communauté de la sécurité nationale et du renseignement (SNR) envers les entités non traditionnelles qui sont maintenant ciblées par les menaces émergentes. Des acteurs tels que les entreprises innovantes du domaine des technologies de pointe et les centres de recherche et d'excellence technologique ont à disposition des compétences et des connaissances qui pourraient permettre à la communauté de la SNR de mieux répondre aux menaces émergentes qui demandent une plus grande approche multidisciplinaire. Soutenir le développement des connaissances et des stratégies d'atténuation face aux menaces ne ferait que disposer les acteurs externes à vouloir partager davantage avec la communauté de la SNR.

## Les défis de la coopération en renseignement

La coopération de renseignement, aussi connue sous les noms de liaison et de partage de renseignements, est l'une des activités de renseignement la plus secrète et qui comporte de nombreux défis en constante évolution, notamment au sein des démocraties occidentales.

Tout d'abord, il faut comprendre que toute agence de renseignement [opère](#) principalement selon ses propres intérêts et pour soutenir les objectifs de politique étrangère, de sécurité, et de défense de son pays. Dans ce contexte, la coopération s'effectue lorsqu'il y a un avantage évident surpassant les coûts. Cela est notamment le cas pour combler un manque d'informations, aller chercher une expertise différente, réduire les coûts d'une opération, lutter contre une menace commune, ou encore obtenir ou espérer obtenir quelque chose en échange.

Toutefois, il existe de nombreuses contraintes, voire restrictions, à la coopération de renseignement. Plusieurs éléments peuvent limiter l'échange de renseignements : des perceptions différentes des menaces ; des intérêts nationaux différents ; les cadres juridiques nationaux ; les cultures organisationnelles ; les pratiques des agences de renseignement étrangères, notamment au regard des droits humains ; ou encore la peur que l'information échangée soit fuitée ou communiquée à une tierce partie, compromettant non seulement le lien de confiance, mais aussi les méthodes et les sources des agences de renseignement. Cette dernière préoccupation explique en partie pourquoi la coopération de renseignement est l'une des activités les plus secrètes et invisibles des agences de renseignement et l'une des plus difficiles à cartographier et à surveiller.

Cette invisibilisation de la coopération de renseignement va s'accroître à mesure que les besoins de coopération vont augmenter, comme c'est le cas depuis la lutte contre le terrorisme jusqu'à la compétition entre les grandes puissances d'aujourd'hui. Il y a alors un paradoxe qui se forme, entre

l'augmentation de l'invisibilité des activités de renseignement conduite par l'augmentation des besoins de coopération, et le désir et la nécessité de plus en plus importante de rendre les activités de renseignement démocratiquement responsables et imputables.

Or, on se retrouve aujourd'hui avec une augmentation du volume de renseignements échangés, une multiplication des acteurs bénéficiant de la coopération et une flexibilité grandissante sur les arrangements, souvent ad hoc et temporaires, de la coopération. Si l'on ajoute à cela la globalisation de la coopération de renseignement à l'ère de la lutte contre le terrorisme, il devient alors important de trouver des mécanismes d'imputabilité et de surveillance de cette activité de renseignement. Si la coopération de renseignement est, de façon pragmatique, utile et nécessaire, l'histoire nous enseigne que de nombreuses erreurs, dommageables pour le citoyen, ont été commises par les activités d'échanges de renseignements.

Toutefois, les mécanismes actuels d'imputabilité et de surveillance sont limités par les frontières et les lois nationales, rendant complexe le suivi des échanges de renseignements. Il faut alors renforcer ces mécanismes, ou créer des mécanismes d'imputabilité et de surveillance supranationaux, permettant de rendre plus transparents les échanges de renseignements. Un modèle intermédiaire, non supranational, mais institutionnalisé et transnational, est le Conseil de surveillance et de révision du renseignement du Groupe des cinq ([FIORC](#)), composé des principaux organes de surveillance nationaux des cinq pays membres, et s'occupant entre autres d'améliorer la transparence des activités de renseignement.

## L'Union européenne : le renseignement comme vecteur d'autonomie stratégique

Depuis de nombreuses années, l'UE, poussée notamment par la France et l'Allemagne, tente d'acquérir une certaine [autonomie stratégique](#), c'est-à-dire renforcer son indépendance, ses capacités et sa résilience sur un certain nombre de domaines comme la sécurité et la défense, ou encore la politique étrangère de façon générale. Dans un monde multipolaire, caractérisé par la réapparition de la compétition entre les grandes puissances, certains acteurs au sein de l'UE et certains États membres sont de plus en plus motivés à atteindre une autonomie stratégique, pour d'une part sortir l'UE de sa dépendance vis-à-vis des États-Unis en matière de sécurité et de défense et d'autre part pour confronter les ambitions russes et chinoises en Europe.

Il semble que pour atteindre cet objectif, un des vecteurs soit la création d'une véritable capacité de renseignement au niveau de l'UE. En effet, l'atteinte d'une autonomie stratégique, c'est-à-dire avoir la capacité d'agir selon ses intérêts, passe par la compréhension de l'environnement stratégique. Pour l'UE, le défi est de définir ses propres menaces, sans dépendre de la perception des menaces américaine.

Or, les capacités de renseignement de l'UE, tout comme la coopération de renseignement en son sein, sont loin d'être suffisantes à l'heure actuelle. Outre le besoin de renforcer les capacités nationales de renseignement de certains pays, la structure même de l'UE est un défi pour les services de renseignement. Basée sur un espace de libre circulation et de libre-échange, elle est souvent exploitée pour la commission de crimes ou d'actes d'espionnage, et rend le travail des agences nationales de renseignement particulièrement difficile. Le besoin de coopération devient donc indispensable. Pourtant, l'échange de renseignements reste encore limité, sauf lorsqu'un évènement majeur survient.

Au niveau européen, il n'existe pas d'organe supranational responsable du renseignement. Il existe toutefois des organes facilitant la coopération au niveau européen, sans mandat de collecte de renseignements, mais recevant les renseignements des agences de renseignement des membres de l'UE

comme le Centre d'analyse du renseignement, la Direction du renseignement de l'État-Major de l'UE ou encore Europol. Si en matière de criminalité et de terrorisme, la coopération de renseignement a été satisfaisante, il n'en est pas de même pour les quatre secteurs indispensables pour une autonomie stratégique que sont l'autonomie décisionnelle, opérationnelle, commerciale et technologique. À ces niveaux, la coopération de renseignement au sein de l'UE est assez rudimentaire, compte tenu des divergences d'intérêts nationaux, de volonté politique et de perception des menaces.

Comme il n'est pas possible de créer une agence supranationale européenne de renseignement sans changer de traité, l'UE doit mettre l'accent sur le renforcement de la coopération de renseignement entre les pays membres à travers des entraînements conjoints, des opérations conjointes ou encore des formations conjointes pour renforcer la confiance mutuelle. Un des exemples est le [projet](#) de la Coopération structurée permanente (PESCO) de créer un centre de coordination sur la surveillance des domaines du cyberspace et de l'information. Ultiment, créer une réelle capacité de renseignement européenne nécessitera une certaine perte d'autonomie nationale et de souveraineté nationale.

## Le concept de Renseignement, Surveillance et Reconnaissance : opportunité stratégique ou vecteur d'instabilités ?

Le [Renseignement, surveillance et reconnaissance](#) (RSR) est un concept stratégique qui permet aux décideurs d'anticiper les changements, d'atténuer les risques et d'orienter les résultats. C'est une activité à la fois de renseignement et d'opérations qui synchronise et intègre la planification et l'exploitation de capteurs, de ressources et des systèmes de traitement pour appuyer en direct les opérations actuelles et futures. En d'autres termes, le RSR est une capacité avancée de renseignement permettant d'avoir l'avantage décisionnel.

Toutefois, la supériorité des États-Unis dans ce domaine crée une asymétrie qui pourrait remettre en question la stabilité stratégique. Traditionnellement, la stabilité stratégique est maintenue par la dissuasion nucléaire. Aujourd'hui, dans les doctrines stratégiques des grandes puissances, le nucléaire est incorporé avec d'autres capacités plus traditionnelles. La multiplication des domaines de confrontation, notamment l'espace et le cyberspace, demande une dissuasion multidomaines, notamment lorsque des adversaires comme la Russie et la Chine utilisent des tactiques hybrides ou de zone grise, le cyberspace ou encore les nouvelles technologies pour déstabiliser les démocraties occidentales.

**La supériorité des capacités technologiques à des fins de renseignement des États-Unis entraîne le recours croissant des adversaires aux techniques et opérations asymétriques**

L'avantage du RSR dans cette complexification des modes de confrontation est d'anticiper les capacités, les intentions et les actions des adversaires. Cependant, cet avantage stratégique comporte certains risques d'entraîner au mieux de la manipulation et de la désinformation de la part d'adversaires inférieurs, et au pire des comportements agressifs préemptifs. Tout d'abord, les adversaires des États-Unis commencent à exploiter les vulnérabilités des systèmes américains via des méthodes asymétriques dans l'espace, le cyberspace et l'information. Ensuite, cela encourage certains pays comme la Chine et la Russie à déployer des capacités pour interdire l'accès à certaines zones. Enfin, la supériorité technologique américaine amène la Russie et la Chine à multiplier les opérations de renseignement humain sur le territoire américain et dans les pays alliés, notamment en matière d'espionnage.

La supériorité des capacités technologiques à des fins de renseignement des États-Unis, si elle offre des avantages certains en matière d'anticipation, de détection et de ciblage, entraîne également le recours croissant des adversaires aux techniques et opérations asymétriques. Il revient maintenant aux États-Unis de coopérer davantage avec les alliés pour atténuer les vulnérabilités exploitées par ses adversaires.

## Quel avenir pour le Groupe des cinq ?

Le partenariat du Groupe des cinq, l'institutionnalisation la plus avancée de partage de renseignements entre les États-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande, comporte son lot d'avantages et d'inconvénients pour les partenaires les moins puissants comme le Canada ou l'Australie et se retrouve face à de nombreux défis à l'ère de la multipolarité.

Un des défis les plus importants à l'ère de la compétition entre les grandes puissances est la compréhension des nouvelles technologies et la prise en compte des nouveaux domaines de confrontation comme le cyberspace. Le Groupe des cinq et les pays membres au niveau national ont un rôle à jouer pour s'assurer de l'efficacité du renseignement à l'environnement actuel. Par exemple, l'Australie a instauré un Conseil national consultatif et scientifique du renseignement, chargé de proposer une approche plus stratégique et structurelle de l'évolution technologique et de son impact sur la communauté du renseignement australien. Ce type d'initiatives pourrait se développer au sein du Groupe des cinq pour permettre de nouvelles opportunités de coopération dans les domaines des technologies et des sciences. Une approche intégrée permettrait aux pays membres du Groupe des cinq de profiter des efforts de chacun. Pour aller encore plus loin, chaque pays pourrait se concentrer sur un ou des domaines dans lesquels il peut apporter une plus grande expertise et la mettre à disposition de ses partenaires. Ce type de coopération permettrait une économie de ressources tout en comblant les lacunes des appareils nationaux de renseignement par l'expertise que les autres ont à offrir.

La régionalisation des menaces, notamment en Asie du Sud-Est, pose également la question de la coopération entre le Groupe des cinq et les autres pays, comme le [Japon](#). Sans forcément aller jusqu'à l'idée d'une intégration complète et institutionnelle d'autres pays au sein du Groupe des cinq, il serait toutefois opportun de penser à une forme d'expansion du Groupe des cinq, selon des critères géographiques ou de types ou de nature des menaces, et d'introduire, sans forcément intégrer, d'autres pays pour une coopération plus profonde et durable sur un sujet particulier. Le Japon pourrait par exemple être introduit au sein du Groupe des cinq pour une [coopération approfondie](#) par rapport à la menace chinoise en Asie du Sud-Est.

## La « Canadianisation » du renseignement

Si la multipolarité et la compétition entre les grandes puissances apportent de nombreuses opportunités pour le Groupe des cinq, il subsiste toutefois quelques défis quant à la coopération en matière de renseignement pour des pays comme le Canada. En effet, bien que cela apporte de nombreux avantages au Canada – comme une énorme source de renseignements étrangers bruts et finis, le Canada [dépend](#) des renseignements partagés par ses alliés puisqu'il est dépourvu d'un service de renseignement étranger qui collecte, centralise et coordonne clandestinement des renseignements humains étrangers en dehors de ses frontières. Ce « biais du producteur » vient donc refléter les intérêts et les priorités du pays destinataire et entraîne le risque considérable de se faire manipuler ou encore de servir des intérêts étrangers à défaut de ceux des Canadiens.

Dans le monde du partage de renseignements, la capacité d'acquérir des renseignements représente une forme de pouvoir où l'information est une monnaie d'échange. Ces échanges mutuels peuvent donc être utilisés comme moyen de persuader des partenaires à se conformer à un nexus étranger. Cela est particulièrement vrai pour le Canada sachant qu'il est bien plus souvent consommateur qu'auteur de produits de renseignement étranger. Ce manque de contribution lui a d'ailleurs valu la réputation, auprès de certains de ses partenaires, d'être perçu comme un « profiteur » au détriment d'un contributeur plus actif au partage de renseignements. Ce sentiment est alimenté par deux réalités distinctes. D'emblée, sa position privilégiée au sein du Groupe des cinq, mais aussi, les circonstances géographiques de son territoire qui le positionne directement dans le périmètre de défense et de sécurité des États-Unis.

**En fournissant une contribution canadienne plus importante, le Canada se positionnerait de manière à être pris plus au sérieux et à démontrer que la qualité vaut parfois mieux que la quantité.**

Il est donc dans l'intérêt du Canada de développer ses capacités en la matière, soit par le biais d'un service de renseignement étranger – qui semble toutefois peu probable en ce moment pour [diverses raisons](#) – soit par une « [canadianisation](#) » de la collecte et de l'analyse du renseignement étranger. En fournissant une contribution canadienne plus importante, le Canada se positionnerait de manière à être pris plus au sérieux et à démontrer que la qualité vaut parfois mieux que la quantité.

Recommandé par [Stephanie Carvin](#) et [Thomas Juneau](#), cette « canadianisation » se définit comme une « constellation d'initiatives visant à orienter la collecte et l'analyse de renseignements étrangers vers une poursuite plus claire et plus forte des intérêts proprement canadiens, par opposition à la réception de renseignements bruts et finis qui peuvent ou non refléter un lien avec le Canada. » Quoique naissant et éparpillé, ce phénomène est vraisemblablement en pleine évolution au sein de la communauté de la sécurité nationale et du renseignement. Pour le moment, ce phénomène ne résulte que d'une série de petites initiatives et non d'une stratégie cohérente et élaborée, mais il constitue néanmoins une alternative intéressante, faisable et réaliste. De plus, renforcer les bénéfices de cette dernière permettrait de produire des évaluations indépendantes et plus adaptées aux besoins canadiens qui, en retour, devraient mieux supporter les prises de décisions et ainsi conduire à une élaboration des politiques plus efficace et plus cohérente.

La « canadianisation » du renseignement étranger n'est pas une approche qui est mutuellement exclusive aux autres alternatives, elle s'inscrit en parallèle dans le but commun de permettre au Canada de mieux répondre à ses intérêts et priorités. D'une manière similaire, elle ne doit pas être vue comme une alternative qui vise à miner la démarche du renforcement de la coopération du renseignement, mais bien à positionner le Canada comme un meilleur collaborateur en contribuant davantage, de manière positive et active, à ses partenariats en matière de renseignement. Cette nouvelle posture offrirait la possibilité au Canada de façonner le narratif des enjeux transnationaux en offrant une perspective distincte et propre aux valeurs et priorités canadiennes.

Cependant, en se fondant sur ce constat, il faudrait d'abord que ces valeurs, priorités et besoins canadiens soient mieux définis pour que de tels produits puissent voir le jour et ce n'est malheureusement pas quelque chose que nos décideurs politiques semblent présentement intéressés à régler. Certes, les capacités canadiennes en matière de renseignement étranger font défaut à plusieurs niveaux. Cependant, une définition plus claire des priorités de la politique étrangère du Canada servirait de support à une « canadianisation ».

La prochaine étape serait de réfléchir à ce qui pourrait être fait pour encourager la poursuite de cette tendance au Canada. Il va de soi qu'une meilleure intégration des efforts de la communauté canadienne de la sécurité nationale et du renseignement (SNR) est requise afin de mieux faire face aux menaces émergentes, car l'évolution de l'environnement de ces dernières ne permet plus la négligence et les erreurs au niveau de l'anticipation des menaces sans qu'elles n'aient de conséquences considérables sur la sécurité et la prospérité du Canada.

## Considérations pour le Canada au niveau de la coopération

C'est dans cette optique d'encourager la poursuite d'une « canadianisation » qu'il est fortement recommandé que la communauté de la SNR continue ses [efforts](#) de collaboration auprès des ministères et organismes de la fonction publique qui ne sont pas traditionnellement rattachés aux enjeux liés à la sécurité nationale et au renseignement. Il en va de même pour les nouvelles cibles non gouvernementales, qu'il s'agisse d'universités, de centres d'excellence, de groupes de réflexion, d'entreprises privées ou des médias. En effet, la réalité est que les services de renseignement n'ont plus le monopole de l'information et que l'expertise et les connaissances requises pour faire face aux menaces demandent une plus grande multidisciplinarité. Ces ressources et compétences peuvent être mises à disposition par les différents acteurs non gouvernementaux grâce à une collaboration plus étroite.

Dès lors, afin de mieux comprendre ces nouvelles menaces et les mesures d'atténuation possibles, il serait opportun que la communauté de la SNR s'investisse plus sérieusement dans un engagement continu et horizontal avec ces nouvelles cibles non gouvernementales pour lesquelles bâtir et maintenir une confiance mutuelle reste à consolider. Une collaboration entière pourrait faire en sorte que la société civile et le secteur privé canadien soient plus conscients des menaces émergentes. De plus, bien qu'elle se soit développée au cours des dernières années, cela contribuerait à renforcer la littératie du renseignement à travers tous les secteurs affectés, puisque la communauté de la SNR reste encore nébuleuse pour plusieurs secteurs et hauts fonctionnaires. Dès lors, par des actions de sensibilisation et de transparence, elle devrait être mieux apte à véhiculer au sein des acteurs externes son rôle, ses priorités, ses limites, ce dont elle a besoin pour être efficace et comment elle peut être utilisée de manière réaliste. La clarification de ses besoins et de ses capacités réelles reste à être mieux définie et pourrait possiblement répondre à la mentalité de cloisonnement entre la population canadienne et la communauté de la SNR.

Une piste de réflexion intéressante pour parvenir à ce dénouement passe par le biais d'une initiative similaire au projet de recherche collaboratif [Public Intelligence](#) ou à [l'Open Source Enterprise](#) établi par le Directeur du renseignement national américain. Sous la responsabilité du Conseiller à la sécurité nationale et au renseignement au sein du Bureau du Conseil privé, cette ressource agirait à titre de base de données centrales de l'exploitation des sources ouvertes de tous les médias — presse écrite, audiovisuelle et en ligne. Elle viserait également à regrouper les contributions collectives de chercheurs indépendants, d'universités, de centres d'excellence, de groupes de réflexion, d'entreprises privées et des médias. Elle inclurait aussi les rapports et les publications provenant des divers ministères et organismes de la fonction publique tels que les différents plans stratégiques, les rapports annuels d'examen et de surveillance des activités ainsi que les évaluations de menaces courantes qui affectent les différents secteurs canadiens. Ce cadre serait possible d'accès pour tous les citoyens canadiens de manière publique et transparente.

Les bienfaits d'un tel projet semblent pertinents et méritent une considération particulière puisqu'il permettrait de tirer parti de l'expertise des acteurs du secteur public et privé afin de rendre le Canada et

les citoyens canadiens plus résilients face aux menaces. En effet, d'une manière, elle permettrait à la communauté de la SNR d'améliorer ses méthodes et ses mesures d'atténuation potentielles et d'un autre côté elle pourrait favoriser un électorat qui soutient davantage son important travail. Les entreprises privées quant à elle obtiendraient un support à l'égard de l'atteinte de leurs buts et objectifs d'innovation et de prospérité. De son côté, la société civile bénéficierait d'une plateforme qui les outillerait à mieux revendiquer et protéger la sécurité, les droits et les libertés des Canadiens. En somme, dans une perspective de bénéfice mutuel et d'action concertée, soutenir le développement des connaissances face aux menaces émergentes et en constante évolution ne ferait que disposer les acteurs externes à vouloir plus partager avec les intervenants de la communauté de la SNR.

D'autre part, au sein de la communauté de la SNR elle-même, une meilleure coopération inter-agence et un processus d'échange d'information demandent à être accentués. Les priorités, moyens et activités divergentes des différents intervenants engendrent des problèmes de communication et de malentendus qui nuisent à une réponse optimale des demandes en renseignement, mais aussi aux décisions prises par le gouvernement. Si elle semble s'être considérablement améliorée, une coordination encore plus importante est nécessaire au sein de la communauté pour pallier les problèmes qui nuisent à la coopération inter-agence. En effet, la compétition bureaucratique, un vocabulaire interne distinct, des procédures opérationnelles normalisées, des interprétations opposées et des habilitations de sécurité différentes ne contribuent pas à fournir une réponse optimale aux menaces qui pèsent sur le Canada.

Dès lors, une approche similaire au cadre de travail intitulé Une vision (*One Vision*) qui vise à améliorer la coopération et à simplifier le processus d'échange d'information entre le SCRS et la GRC, devrait être mise à l'échelle de la communauté de la SNR. Certes, cela nécessiterait un niveau sans précédent de coordination des politiques nationales et internationales de la SNR canadienne, mais elle permettrait de favoriser une cohésion inter-agence multidimensionnelle. Ainsi donc, elle demanderait l'intégration complète des efforts de différents départements et ministères afin de remédier aux défis des différentes cultures et procédures organisationnelles pour offrir une meilleure réponse face aux menaces qui pèsent sur la société canadienne.

## Conclusion

Tout compte fait, si le désir est réellement de mieux pallier les problèmes liés à l'émergence de nouvelles menaces et de relever les nombreux défis provenant de la transition actuelle du pouvoir et l'intensification de la concurrence stratégique entre les grandes puissances, il faut faire appel à l'innovation, ainsi qu'à une fusion sans précédent des connaissances, des pratiques, de la planification et des cultures de tous les secteurs affectés. Par ailleurs, les alliés et les États partageant des priorités et des valeurs démocratiques similaires doivent comprendre que leurs intérêts nationaux sont mieux servis par le biais d'une coopération en matière de renseignements et d'actions alignées.

De plus, si le Canada souhaite pleinement bénéficier d'une coopération multilatérale en matière de renseignement, il doit être capable d'en faire plus pour lui-même et par lui-même. Plus il sera apte à contribuer de manière active, plus il obtiendra en retour. Cette « canadianisation » du renseignement attribuerait une valeur ajoutée au Canada comme partenaire et lui permettrait de servir des intérêts qui reflètent ses priorités et ses valeurs.

Pour conclure, dans le but de rendre les entreprises et les citoyens canadiens plus résilients face aux menaces, il est recommandé que la communauté canadienne de la SNR établisse un cadre multilatéral de coopération et d'assistance mutuelle avec les différents acteurs externes. Par le biais d'engagements



itératifs et systémiques, les intervenants de la communauté doivent établir des liens avec les autres secteurs de la société canadienne et tirer parti de l'ensemble de leurs connaissances et compétences spécialisées pour faire face à la complexification des menaces en constante évolution.