Rapport de synthèse

Auteur: Daniel Jean, sous-ministre retraité, ancien conseiller à la sécurité et au renseignement du Premier Ministre et sous-ministre affaires étrangères, intérêt continu pour ces enjeux avec de multiples affiliations dont Professionnel en résidence honoraire à l'ESAPI de l'Université d'Ottawa actif et membre du conseil d'administration de la Conférence des associations de défense.

Thème du panel : L'appareil de la sécurité nationale du Canada

Cerner les enjeux

- Les travaux de la commission ont soulevé jusqu'à ce jour au moins 6 enjeux pertinents à l'appareil de sécurité nationale :
  1) L'absence d'une culture de sécurité nationale qui affecte l'évaluation stratégique et remet en question nos instruments juridiques et approches surtout lors de crises ponctuelles.
  2) Le défi de développer des produits de renseignement de qualité avec une fiabilité clairement énoncée.
  3) La distribution des produits auprès des fonctionnaires clefs et des responsables politiques pertinents guidant les actions, si nécessaires et possibles.
  4) Une approche systémique pour que les produits pertinents soient portés à l'attention de ces mêmes fonctionnaires et responsables politiques clefs avec acquiescement documenté de leur prise de connaissance.
  5) Dans un monde où les joyaux de la couronne sont de plus en plus à l'extérieur du gouvernement, favoriser un changement culturel fondamental pour mieux alerter et soutenir les Canadiens contre l'ingérence étrangère.
  6) Une gouvernance horizontale chez les fonctionnaires et au Cabinet où enjeux et options sont discutés en profondeur pour assurer une meilleure cohérence et coordination.

- Regardons ces 6 enjeux et de possibles améliorations tout en répondant à certaines questions adressées au panel.

1) L'absence d'une culture de sécurité nationale qui affecte l'évaluation stratégique et remet en question nos instruments juridiques et approches surtout lors de crises ponctuelles.

Répond en partie à la question 1

1. ***Les services canadiens de renseignement disposent-ils des pouvoirs juridiques, des capacités techniques et des ressources suffisantes pour détecter, collecter et analyser les informations relatives à l'ingérence étrangère, en particulier dans l'environnement en ligne? Disposent-ils des pouvoirs et des outils nécessaires pour contrer efficacement l'ingérence étrangère? Que peut-on faire de plus pour améliorer la capacité du Canada à détecter et à contrer la menace?***

Historiquement, nos lois ont la plupart du temps été amendées à la suite de crises. Par exemple la loi créant le SCRS en 1984 à la suite à la Commission McDonald[1], les actes terroristes menant à la loi sur la sécurité nationale de 2015[2] et il va sans dire que le présent débat sur l'ingérence étrangère a mené à l'adoption rapide du projet de loi C-70[3].

Les enjeux du jour qui préoccupent les citoyens ont rapidement réaccaparé l'attention minant l'évaluation stratégique et les tentatives de divers gouvernements de créer plus d'espace pour ces discussions stratégiques. La création récente d'un Conseil de la sécurité nationale est une nouvelle tentative mais il est encore tôt pour en juger.

La loi C-70 récemment adoptée corrige plusieurs des lacunes, en particulier celles de la Loi sur le SCRS de 1984 tant au niveau de l'amener dans l'ère numérique que de lui permettre un rôle plus actif d'articuler la menace auprès d'acteurs externes. La mesure visant une mise à jour régulière de la loi est encourageante mais devra être plus qu'un exercice procédural.

2) **Le défi de développer des produits de renseignement de qualité avec une fiabilité clairement énoncée ;**

Les délibérations de cette commission ont mis en lumière le défi de développer des produits de renseignement de qualité et avec des degrés de fiabilité clairement énoncés. Il est frappant de constater comment différents acteurs ont pu interpréter différemment les mêmes documents de renseignement.

- Pensez en particulier au rapport récent du Comité des parlementaires sur la sécurité nationale et le renseignement (le CPSNR) [4] et ceux qui ont eu accès au matériel classifié et mettez-

[1] https://www.thecanadianencyclopedia.ca/en/article/royal-commission-on-inquiry-into-certain-activities-of-the-royal-canadian-mounted-police
[2] https://www.justice.gc.ca/fra/jp-cj/sn-ns/lat15-ata15.html
[3] https://www.noscommunes.ca/committees/fr/SECU/StudyActivity?studyActivityId=12773790
[4] CPSNR, Rapport spécial sur l'ingérence étrangère dans les processus et les institutions démocratiques du Canada, 3 juin 2024

les en parallèle avec le témoignage récent du SCRS sur les cas les plus flagrants d'ingérence qui apportait des nuances importantes[5].

Dans les premières semaines après les fuites de renseignement, on a assisté à de dangereuses extrapolations traitant le renseignement comme de l'évidence. Le commentaire d'opinion du Dr Carvin dans le Globe and Mail[6] a été très utile pour différencier clairement ces termes.

- S'il arrive parfois qu'un élément de renseignement, par exemple une interception d'une conversation sans équivoque pourrait, s'il est possible de le faire sans mettre en danger les sources, méthodes et enquêtes être utilisé comme évidence---- La plupart du temps le renseignement repose sur de l'information qui représente divers degrés de fiabilité.

La collecte et l'analyse du renseignement doit demeurer indépendante et elle informe de manière neutre le développement des stratégies, politiques publiques et opérations. Toutefois, le renseignement ne peut être développé dans un « vide».

- Des échanges réguliers entre les auditoires visés et les auteurs du renseignement sont primordiaux pour que celui-ci bénéficie de toute la diligence valeur ajoutée désirable.
- Sur la qualité et la fiabilité du renseignement, l'exemple cité des différentes interprétations doit éclairer nos services de renseignement sur la nécessité de se mettre dans l'esprit des auditoires qui ne sont pas des experts en renseignement et s'assurer que le document est clair sur ce qui peut être établi avec certitude versus les hypothèses et les différents degrés de fiabilité sur lesquelles ils reposent.
- Beaucoup de progrès a été fait dans l'habileté de la communauté de la sécurité nationale à travailler horizontalement sur différents enjeux mais le travail au plan renseignement demeure encore trop cloisonné.

3) La distribution des produits auprès des fonctionnaires clefs et des responsables politiques pertinents guidant les actions, si nécessaires et possibles

S'attarde en grande partie aux question 2 et 3

> **Q2** ***Quelles mesures peuvent être prises pour rendre efficaces et efficientes les relations entre les agences de renseignement du Canada et les décideurs du gouvernement ?***

[5] https://www.cbc.ca/news/politics/foreign-interference-csis-1.7336005

[6] Stephanie Carvin, The Globe and Mail, Opinion: What are we talking about, when we talk about intelligence?, 3 mars 2023

Q3 ***Quelles mesures peuvent être prises pour améliorer la communication des renseignements et la compréhension des implications des menaces d'ingérence étrangère avec les parties prenantes externes telles que les partis politiques et les candidats? Les modifications apportées à l'article 19 de la Loi sur le Service canadien du renseignement de sécurité dans le projet de loi C-70 sont-elles susceptibles d'améliorer l'échange d'informations? Qu'est-ce qu'elles aborderont et qu'est-ce qu'elles n'aborderont pas?***

S'il est crucial d'accroître la qualité des produits de renseignement, il l'est tout autant de s'assurer que ceux-ci soient portés à l'attention des auditoires concernés et que les plus importants à l'attention des plus hauts échelons de ces auditoires, soit par la lecture ou le breffage écrit ou oral de leur synthèse.

On parle de différents auditoires concernés au pluriel parce que dans le monde complexe d'aujourd'hui :

- La communauté de la sécurité et du renseignement doit constamment travailler avec les autres ministères et agences, par exemple économiques dans les enjeux de sécurité économique ou avec les ministères/ agences à caractère social sur des enjeux comme la désinformation ou les institutions assurant l'intégrité des élections comme la Commissaire aux élections fédérales.
- Les constatations de cette commission sur l'ingérence renforcent l'importance que les parlementaires mais aussi les partis politiques soient régulièrement informés sur l'évolution des menaces pertinentes. Comme indiqué précédemment, ces informations devraient guider leurs codes de conduite.

4) Une approche systémique pour que les produits les plus pertinents en soient portés à l'attention de ces mêmes fonctionnaires et responsables politiques clefs avec acquiescement documenté de leur prise de connaissance

Les délibérations de cette commission ont soulevé que certaines informations clefs n'ont peut-être pas été envoyées ou n'ont pas reçu l'attention nécessaire de ceux qui les ont reçues compte tenu de la multitude d'enjeux au quotidien.

On ne peut pas exiger que les dirigeants du gouvernement à l'interne ou des acteurs clefs externes comme les parlementaires ou les partis politiques s'attardent à lire tous les produits de renseignement.

- Toutefois il est essentiel que les cotes de sécurité soient en place pour les plus importants acteurs et que ceux-ci créent l'espace pour les éléments essentiels du renseignement sur la menace qui exigent leur attention.
- Ces échanges doivent être documentés soigneusement pour promouvoir l'imputabilité du système.

5) **Dans un monde où les joyaux de la couronne sont de plus en plus à l'extérieur du gouvernement, favoriser un changement culturel fondamental pour mieux alerter et soutenir les Canadiens contre l'ingérence étrangère ; et**

Répond particulièrement à la question 6,

Q6 ***Les agences de sécurité nationale du Canada devraient-elles mieux communiquer avec le public sur la menace d'ingérence étrangère et sur les moyens de s'en protéger et, dans l'affirmative, comment ?***

mais également la question 4.

Q4 ***Comment résoudre la tension entre la fourniture d'informations suffisamment précises pour être utiles et la protection des impératifs opérationnels et de sécurité qui exigent de limiter le partage d'informations?***

Dans un environnement où les joyaux de la couronne et les cibles d'ingérence par des pays étrangers ou leurs intermédiaires sont de plus en plus externes au gouvernement[7]—Par exemple :

- Les technologies/recherches sensibles dans le secteur privé et nos universités/instituts.
- La manipulation via une désinformation systémique pouvant miner la confiance dans les institutions démocratiques.
- Le suivi, le harcèlement et l'intimidation des diasporas dans le but de faire taire les critiques.
- Le rôle fondamental des partis politiques dans notre démocratie.
- Le fait que certains de ces joyaux de la couronne et vulnérabilités se retrouvent dans divers paliers de gouvernement (provinces, territoires, municipalités, gouvernances autochtones).

L'évolution de cet environnement signifie que notre appareil de sécurité doit d'avantage connaître et tisser des liens de confiance avec ces différents acteurs. Il doit utiliser à bon escient les autorités existantes et nouvelles (C-70) pour informer d'avantage la menace et ses manifestations tout en protégeant, les sources, méthodes et enquêtes.

Cela exige un changement culturel profond qui requiert d'ajuster les méthodes de recrutement, de formation et de suivi pour favoriser un comportement organisationnel adapté à cette nouvelle réalité.
Quelques commentaires pour certains des acteurs clefs :

[7] https://utorontopress.com/9781487550752/intelligence-cooperation-under-multipolarity/ , conclusion

- Parce que la menace cyber est significative pour notre démocratie, nos infrastructures et secteurs critiques, le CST, jadis une des organisations les plus secrètes, a déjà entamé ce virage mais doit aller plus loin et passer de la sensibilisation de la menace à la résilience.
- Le virage requis est considérable pour le SCRS qui, jusqu'à maintenant était menotté dans son engagement externe par une loi désuète mais dont la culture est profondément enracinée à l'ancien environnement.
- Résoudre le conflit quant à la capacité de la GRC de jouer pleinement son rôle de police fédérale quand tant de son attention et ressources sont monopolisées par la police contractuelle.

Bien que la protection des méthodes, sources et enquêtes peut-être une barrière au partage externe, l'aversion au risque est beaucoup plus grande au Canada qu'ailleurs. On sous-estime aussi ce qui peut être accompli avec des sources ouvertes. Il est impératif de négocier ce virage.

6) **Une gouvernance horizontale chez les fonctionnaires et au Cabinet où enjeux et options sont discutés franchement et en profondeur pour assurer une meilleure cohérence et coordination.**

Offre des pistes additionnelles en réponse à la question 1.

Sans être parfaite, la gouvernance horizontale au niveau des fonctionnaires dans le domaine de la sécurité nationale a fait des progrès significatifs depuis la création du poste de CSNR en 2003.

- L'agilité à répondre de manière cohérente et coordonnée aux crises via le Comité DMOC a atteint un niveau de maturité encourageant et la création d'un comité de cabinet (le GRI) a permis l'extension au Cabinet.
- L'aspect de décloisonner le renseignement tout en protégeant son indépendance dont j'ai parlé plus tôt est le prochain pas qu'il faut franchir.
- Au niveau du développement des politiques, il y a des efforts raisonnables visant à promouvoir de saines discussions dans le développement des politiques liées au mandat du gouvernement tout en anticipant les enjeux émergents. On note aussi des progrès importants à intégrer les acteurs externes à l'appareil, par exemple les ministères/agences économiques lorsqu'on parle de sécurité économique (annexe 2).
- L'absence d'appétit et de temps pour des discussions plus stratégiques demeurent un défi. La création du nouveau Conseil sur la sécurité nationale offre une opportunité mais il est trop tôt pour juger.

Le **rôle du CNSR** est clef à cette gouvernance horizontale tant au niveau des fonctionnaires que comme lien essentiel avec le Premier Ministre et le Cabinet. Il

n'y a pas d'obstacles à codifier le rôle du CSNR dans la loi. Toutefois, à moins de remettre en question le modèle de Westminster où les responsabilités demeurent sous les ministres et leurs institutions, cela viendra sans doute articuler le rôle qui est le miroir du Bureau du Conseil Privé (BCP) i.e. :

- Avis indépendant au PM.
- Soutien et avis au Cabinet.
- Rassembler (« convening ») pour promouvoir cohérence et coordination des efforts de politique publique et opérationnels.

On accorde beaucoup d'attention au **rôle** alors que les **attributs** du titulaire sont probablement tout aussi importants. Le CSNR doit être une personne :

- Expérimentée et respectée de ses pairs pour pouvoir favoriser cohérence et coordination et mettre au défi les hypothèses ou propositions.
- Capable d'offrir cette « fearless advice » aux auditoires clefs (PM, Cabinet).
- Qui offre une valeur ajoutée tant à la communauté qu'aux auditoires clefs (PM, Cabinet). Il est le tissue conjonctif mais ne peut-être « l'amplificateur » unidirectionnel de l'un ou l'autre.

Annexe 1 Recommandations

R1- Les instances politiques et l'appareil de sécurité nationale doivent de manière responsable mieux sensibiliser les Canadiens à la menace d'ingérence étrangère et ce qu'elle signifie pour notre prospérité et nos libertés démocratiques et les engager dans les efforts continus de prévention et résilience.

R-2 L'élaboration du renseignement tout en demeurant indépendant et neutre quant au développement des politiques ou des opérations doit se décloisonner et engager les clients pour bénéficier à la fois de la mise au défi et des vérifications des faits et hypothèses mais également de la valeur ajoutée du complément d'information.

R-3 Les interprétations divergentes faites par différents acteurs à la lecture des mêmes éléments de renseignement dans le cadre du récent débat sur l'ingérence étrangère doivent éclairer nos services de renseignement sur la nécessité de se mettre dans l'esprit des auditoires qui ne sont pas des experts en renseignement et s'assurer que le document est clair sur ce qui peut être établi avec certitude versus les hypothèses et les différents degrés de fiabilité sur lesquelles ils reposent et dans un langage adapté à un auditoire externe.

R-4 Compte tenu que les délibérations de cette commission ont soulevé que certaines informations clefs n'ont peut-être pas été envoyées ou n'ont pas reçu l'attention nécessaire de ceux qui les ont reçues en raison de la multitude d'enjeux au quotidien, il est essentiel que les cotes de sécurité soient en place pour les plus importants acteurs (officiels, ministres, parlementaires et partis politiques) et que ceux-ci créent l'espace pour que les éléments essentiels du renseignement sur la menace, qui exigent leur attention, leur soit communiqués. Ces échanges doivent être documentés soigneusement pour promouvoir l'imputabilité du système dans son ensemble.

R-5 Dans un environnement où les joyaux de la couronne et les cibles d'ingérence par des pays étrangers ou leurs intermédiaires sont de plus en plus externes au gouvernement, notre appareil sécurité doit d'avantage connaître et tisser des liens de confiance avec ces différents acteurs externes. Il doit effectuer un important virage culturel et utiliser à bon escient les autorités existantes et nouvelles (C-70) pour informer d'avantage la menace et ses manifestations tout en protégeant, les sources, méthodes et enquêtes.

Annexe 2
Courtes études de cas illustrant de bonnes réponses à la menace d'ingérence étrangère

Australie

En Australie en 2017, quand le Premier Ministre Turnbull a réalisé à quel point la Chine avait pénétré divers aspects de la société australienne (financement électoral, influence des parlementaires, anciens politiciens et officiels seniors agissant comme agents sans transparence, des universités sous pression de la Chine en raison de dons et contributions, l'acquisition de technologies sensibles à la fois dans le secteur privé et les universités), il a recruté John Garnaut, un avocat de formation devenu journaliste spécialisé sur la Chine pour travailler avec ASIO (l'équivalent de SCRS) afin d'évaluer discrètement la situation et développer un ensemble de mesures qui sont subséquemment devenues publiques (réforme du financement électoral, création d'un registre des agents étrangers, un affûtage des mesures et pénalités pour contrer l'IE et une attention particulière aux investissements étrangers)[8]. Certaines de ces mesures ont fini par susciter des représailles de la part de la Chine. Au cours des dernières années, le Gouvernement a continué d'affûter ses instruments et efforts de dissuasion. Des condamnations récentes[9] en matière d'ingérence viennent appuyer ces démarches.

Canada Sécurité économique. Sur le plan de la sécurité économique, la réponse du Canada à partir de 2015 aux préoccupations avec l'acquisition de technologies sensibles ou de ressources stratégiques par la Chine illustre qu'une approche pangouvernementale concertée avec des mesures ciblées peut porter fruits. Il faut se rappeler que la lettre de mandat de 2015[10] du Ministre de l'ISDE l'invitait à promouvoir les investissements dans les secteurs prometteurs mais à une époque où un pourcentage croissant de l'investissement étranger direct dans le monde provenait de Chine. Les fonctionnaires de l'appareil de sécurité nationale et leurs collègues pertinents des ministère économiques ont travaillé étroitement à sensibiliser leurs ministres et le Cabinet sur les risques de certains investissements. Le gouvernement a répondu avec une succession de mesures

[8] John Garnaut, How China Interferes in Australia And How Democracies Can Push Back, Foreign Affairs, 9 mars 2018

[9] https://www.afp.gov.au/news-centre/media-release/first-sentence-foreign-interference-handed-down

[10] https://www.pm.gc.ca/fr/lettres-de-mandat/2015/11/12/archivee-lettre-de-mandat-du-ministre-de-linnovation-des-sciences-et

administratives, réglementaires et législatives. Un regard sur les statistiques de la Loi sur l'investissement au Canada au cours des sept dernières années démontre une croissance des rejets et abandons d'investissement étrangers dans des secteurs sensibles. Les différentes mesures envoient un message que le Canada n'est pas ouvert à des investissements étrangers qui pourraient être injurieux à la sécurité nationale et le projet de loi C-34, qui a reçu la sanction royale le 22 mars 2024, va aiguiser plusieurs de ces outils.[11]

[11] ISDE, Document d'information mis à jour : Loi modifiant la Loi sur Investissement Canada, 27 mars 2024