Souverain sans yeux

Pourquoi un Québec indépendant doit se doter d'un service de renseignement.

La fonction de renseignement est constitutive de la souveraineté d'un État : collecter, analyser et exploiter l'information stratégique avant que les décisions adverses ne s'imposent comme faits accomplis. Le Service Canadien du Renseignement de Sécurité (SCRS) et le Centre de la Sécurité des Télécommunications (CST), relevant exclusivement d'Ottawa, partiraient le jour de l'indépendance avec leurs dossiers, leurs sources et leurs bases de données. Les protocoles de l'alliance Five Eyes, regroupant le Canada, les États-Unis, le Royaume-Uni, l'Australie et la Nouvelle-Zélande, interdisent la transmission de renseignements classifiés à un État non-membre. Un Québec indépendant repartirait sans évaluation de menace sur son territoire, sans connaissance des agents étrangers actifs sur son sol, sans historique des cyberattaques sur ses infrastructures.

Les actifs exposés sont quantifiables. Hydro-Québec gère environ 93 milliards de dollars d'actifs et alimente l'ensemble du réseau électrique québécois. La Voie maritime du Saint-Laurent et les ports québécois traitent entre 143 et 153 millions de tonnes de marchandises par année selon les données de la Chambre de commerce maritime. La filière aérospatiale montréalaise génère environ 17 milliards de dollars de revenus annuels en avionique et systèmes embarqués. Selon le rapport IBM Cost of a Data Breach 2024, le coût moyen d'une violation de données au Canada atteint 6,32 millions de dollars par incident, hors intrusions non détectées, que les spécialistes estiment majoritaires.

Le futur État québécois pourrait mettre en place un Service de Renseignement Économique et Stratégique (SRES), chargé d'anticiper les menaces à la puissance économique et institutionnelle du Québec. Les États perdent leurs secrets non par des opérations d'éclat, mais par le rachat d'un fournisseur de composants militaires, un financement universitaire conditionnel à un transfert de données, ou un logiciel de gestion transmettant des informations vers un serveur étranger. Le SRES ciblerait ces vecteurs en combinant sources humaines (fonctionnaires, diplomates, acteurs économiques), analyse de communications électroniques, et exploitation de sources ouvertes : brevets, appels d'offres, registres d'entreprises, publications académiques. En 2019, Bellingcat a reconstitué l'identité complète d'agents du Renseignement militaire russe (GRU) impliqués dans l'empoisonnement de Sergueï Skripal à partir de données publiques croisées, sans accès à des fichiers classifiés.

Mila, centre de recherche en intelligence artificielle (IA) de Montréal et l'un des cinq pôles académiques en IA les plus cités au monde, illustre la vulnérabilité universitaire. Un gouvernement étranger finançant une chaire ou recrutant un chercheur postdoctoral peut rapatrier des connaissances stratégiques avant leur commercialisation, sans enfreindre aucune loi. Le SRES cartographierait ces flux en croisant financements déclarés des laboratoires, affiliations des chercheurs invités et dépôts de brevets dans des juridictions étrangères. La même logique s'appliquerait aux minéraux critiques : lithium, graphite et nickel québécois, parmi les gisements les plus importants d'Amérique du Nord, font l'objet d'un schéma d'acquisition documenté, soit la prise de participation minoritaire dans une junior minière en difficulté, l'offre de financement conditionnelle à un transfert technologique, ou le rachat d'un équipementier local. Le SRES produirait des fiches de risque transmises au ministère responsable avant la signature des contrats.

Le mandat du SRES dépasserait la seule protection économique. La Commission Hogue, dont le rapport final publié le 28 janvier 2025 a documenté des tentatives d'ingérence étrangère, notamment de la Chine et de l'Inde, ciblant des candidats lors des élections fédérales de 2019 et 2021, illustre une menace que le Québec indépendant devrait assumer seul, sans le Groupe de travail fédéral sur les menaces électorales étrangères. La Commission a conclu que ces opérations n'ont pas modifié les résultats électoraux globaux, mais a documenté des cas où l'ingérence a pu affecter le résultat de courses à l'investiture ou d'élections dans des circonscriptions précises. Le SRES intégrerait une division de sécurité intérieure chargée de surveiller les tentatives de manipulation de l'opinion publique par des acteurs étrangers : financement opaque de groupes de pression, amplification artificielle de narratifs polarisants via des réseaux sociaux, recrutement d'élus ou de membres de cabinets ministériels à des fins de collecte de renseignements. Ces opérations ne visent pas à voler des brevets, elles visent à déstabiliser les institutions et à orienter les décisions politiques depuis l'extérieur. La détection reposerait sur le croisement de données financières, d'analyse de réseaux numériques et de renseignement humain.

Cette division assumerait également la gestion des listes de surveillance terroriste et le suivi des processus de radicalisation violente, données actuellement détenues par le SCRS et la Gendarmerie Royale du Canada (GRC). La rupture avec ces structures fédérales créerait un vide immédiat : aucune liste de personnes sous surveillance, aucun historique des filières de recrutement actives sur le territoire, aucune connaissance des individus radicalisés ayant transité par le Québec. L'Estonie, reconstruisant ses services après 1991, a mis près de dix ans à reconstituer une base de données de sécurité intérieure reconnue par ses partenaires de l'Organisation du Traité de l'Atlantique Nord (OTAN). Le SRES transmettrait ses évaluations de menace à une unité de réponse tactique de la Sûreté du Québec (SQ), éliminant le cloisonnement actuel entre renseignement fédéral et capacité d'intervention provinciale. Ce modèle intégré, où l'analyse stratégique du service civil alimente directement l'unité opérationnelle de la police nationale, est celui qu'appliquent les Pays-Bas entre le Service général de renseignement et de sécurité (AIVD) et la police nationale, ou la France entre la Direction Générale de la Sécurité Intérieure (DGSI) et le Recherche, Assistance, Intervention, Dissuasion (RAID).

Le service s'organiserait autour du cycle du renseignement, processus en quatre étapes se refermant en boucle continue. L'orientation définit les priorités annuelles via un comité interministériel : secteurs économiques exposés, acteurs à risque documenté, processus électoraux en période de vulnérabilité. La collecte mobilise les sources humaines, électroniques et ouvertes. Le traitement croise et valide : une source non corroborée ne constitue jamais un renseignement exploitable. La diffusion transmet l'analyse au décideur compétent et génère de nouvelles questions reconfigurant les priorités de la prochaine orientation, bouclant le cycle. Le format pourrait adopter le modèle des *President's Daily Brief américains*, des synthèses d'une à deux pages orientées vers une décision précise.

Le volet cyber dépasserait la défense périmétrique. L'attribution d'une cyberattaque, soit l'identification de son auteur avec un niveau de preuve suffisant pour justifier une réponse diplomatique ou juridique, constitue une capacité distincte. En 2018, les Pays-Bas ont expulsé quatre officiers de la Direction principale du renseignement russe (GRU) après que le Service de renseignement militaire néerlandais (MIVD) eut documenté, preuves techniques à l'appui, une tentative d'infiltration du réseau de l'Organisation pour l'Interdiction des Armes Chimiques (OIAC) à La Haye, opération rendue possible par une infiltration préalable du groupe plusieurs mois avant l'incident. Le SRES maintiendrait une base de données de Tactiques, Techniques et Procédures (TTPs) propres aux groupes d'attaquants connus. Les TTPs fonctionnent comme une empreinte digitale comportementale : outils, points d'entrée et méthodes d'exfiltration caractéristiques d'un groupe permettent de relier un incident à un acteur connu et de produire une attribution exploitable diplomatiquement. Cette mémoire technique est ce que la transition fédérale ne fournirait pas.

La Slovaquie, après la dissolution de la Tchécoslovaquie en 1993, a négocié dès les premiers mois un protocole de transfert partiel des dossiers territoriaux avec Prague. Le Québec devrait inscrire une exigence identique dans les négociations d'indépendance : évaluations de menace, dossiers sur les réseaux d'influence étrangers, listes de surveillance et données sur les incidents cyber passés. Ce qui ne serait pas transféré serait reconstruit en priorisant les secteurs les plus exposés.

Une loi fondatrice définirait le mandat et les limites du SRES, établissant une distinction juridiquement contraignante entre protéger l'État québécois, soit ses institutions, ses infrastructures et sa capacité de fonctionner, et protéger le gouvernement en place. Le programme COINTELPRO du Bureau Fédéral d'Investigation (FBI), actif entre 1956 et 1971, a ciblé militants civils, syndicalistes et élus sous couvert de sécurité nationale avec l'autorisation du directeur J. Edgar Hoover, illustrant concrètement l'absence d'un tel cadre. « *Le secret est nécessaire à l'efficacité du renseignement, mais la démocratie exige que ce secret soit lui-même gouverné par des règles que les citoyens ont approuvées* » -- Sir David Omand, Securing the State, Hurst & Company (2010). La loi créerait un comité parlementaire de surveillance doté d'un accès réel aux opérations et d'un pouvoir d'enquête indépendant.

Le coût est estimable par comparaison. Le budget du SCRS pour 2024-2025 a atteint 764 millions de dollars canadiens après budgets supplémentaires, en hausse de 7,5 % par rapport aux crédits initiaux, pour couvrir l'ensemble du territoire canadien. Pour un Québec indépendant de 8,9 millions d'habitants assumant des missions équivalentes, économiques, cyber et sécurité intérieure, un service dimensionné à sa population se situerait entre 400 et 600 millions de dollars par année, soit moins de 0,5 % du budget consolidé actuel. Le Center for Strategic and International Studies estime que les cyberattaques contre des infrastructures critiques engendrent entre 500 millions et plusieurs milliards de dollars de dommages par incident. Le service coûterait moins qu'une seule des crises qu'il serait chargé de prévenir.

Former un analyste opérationnel prend entre sept et dix ans : développer des sources, reconnaître les schémas de désinformation et évaluer la fiabilité d'une information dans un contexte précis s'apprennent sur le terrain. Des fonctionnaires québécois travaillant au SCRS et au CST constitueraient le noyau fondateur. Une école nationale du renseignement, adossée à l'Université de Montréal ou à l'UQAM, disposant de départements en sécurité internationale et en cybersécurité, formerait la relève sur un programme combinant théorie analytique, langues étrangères et stages opérationnels.

Sans appareil de renseignement souverain, un Québec indépendant serait gouvernable par d'autres sans le savoir : ressources minières acquises avant que ses ministres ne comprennent ce qui se passe, universités finançant la recherche militaire d'États étrangers, institutions parlementaires infiltrées par des réseaux d'influence étrangers, infrastructures cartographiées et pré-positionnées pour une attaque sans qu'aucune alarme ne sonne. Le SRES serait la réponse à cette vulnérabilité, construit méthodiquement, encadré législativement, financé à la hauteur de ce qu'il protège.

Louis-Martin Carrière