Conflits géoéconomiques : les secteurs stratégiques canadiens sous le tir croisé des services d'espionnage étrangers

Simon Piché-Jacques (UQÀM)
Mai 2021

SOMMAIRE EXÉCUTIF

Ces dernières années, plusieurs secteurs stratégiques du Canada comme l'aérospatial, les télécommunications et l'industrie pharmaceutique ont été la cible d'opérations clandestines parrainées par des gouvernements étrangers. Leurs services de renseignements utilisent d'importants moyens cybernétiques, humains et financiers pour recueillir de l'information privilégiée, et sont devenus particulièrement proactifs dans l'arène corporative. Cette réalité soulève plusieurs questionnements sur l'évolution du rôle des services de renseignements canadiens à l'égard de la multiplication d'opérations d'espionnage. À ce titre, David Vigneault, directeur du Service canadien du renseignement de sécurité (SCRS), soulignait récemment que l'espionnage économique constitue désormais la menace principale pour l'économie et l'intérêt national. Pour circonscrire ce problème, les services de renseignements canadiens doivent traiter l'espionnage économique de façon proactive, sans toutefois contrevenir à son modèle socioéconomique. En somme, il s'agit de mieux coordonner, conseiller et appuyer les secteurs stratégiques canadiens à risque, autant dans la sphère publique que privée.

INTRODUCTION

Les États investissent aujourd'hui massivement dans les processus de recherche et développement (R&D) des secteurs stratégiques, mettent en œuvre des stratégies de découplage soutenues par des politiques protectionnistes et multiplient l'obtention de brevets. En coulisses, la conquête agressive des marchés extérieurs s'effectue par divers moyens clandestins comme la création de sociétés-écrans, les partenariats de recherche, les faux appels d'offres, les cyberintrusions dans les chaînes d'approvisionnement et la dissimulation de projets militaires derrière des volets civils. Les semi-conducteurs, les systèmes d'armement, les brevets pharmaceutiques, les banques de données médicales, les structures organisationnelles et les logiciels deviennent des cibles, puisqu'ils procurent un avantage stratégique potentiel sur les rivaux. Comme le souligne le Rapport annuel 2020 du Comité des parlementaires sur la sécurité nationale et le renseignement, certains États misent de manière récurrente sur des opérations d'espionnage, tant pour court-circuiter les processus coûteux de R&D que pour affaiblir leurs plus proches concurrents. Or, le Canada représente une cible de choix. Les attaques contre Nortel (2004-2009), le ministère des Finances (2011), le Conseil du Trésor (2011) et le Conseil national de recherche du Canada (2014) en témoignent.

DÉVELOPPEMENT

D'un intérêt sectoriel diffus à un enjeu d'intérêt national

La mondialisation, la connectivité grandissante entre les nations et l'avènement des technologies numériques ont accéléré la vitesse de production, ont réduit la marge d'incertitude et ont mis en évidence l'importance de la communication en temps réel. Ces développements amorcent un changement de paradigme : la géoéconomie est devenue la pierre angulaire des relations internationales. En l'absence d'une menace monolithique d'ordre politique et militaire, les États manifestent un appétit grandissant pour le développement national sur les plans technique et scientifique, ainsi que pour la prise de contrôle de marchés extérieurs. Pour être en mesure de suivre la cadence, tous les coups sont permis. Or, le mode opératoire de l'espionnage économique reste sensiblement le même, comme les demandes d'informations, l'exploitation de sources ouvertes (*open source*), les demandes d'achat et le partage de technologies. Toutefois, il s'est accru et complexifié, notamment avec l'utilisation de moyens cybernétiques et l'appui remarqué des services de renseignements.

Autocratie et démocratie : entre proactivité et réactivité

Les autocraties ont-elles un avantage sur les démocraties en matière d'acquisition d'information stratégique ? Il s'avère *a priori* moins contraignant du point de vue socioéconomique et institutionnel pour les régimes autoritaires d'utiliser leur appareil de renseignement pour soutenir des politiques mercantilistes. L'appareil de sécurité dans ces régimes adopte habituellement une vision proactive et offensive du renseignement économique (ex : Chine, Russie, Iran et Corée du Nord). Dans cette perspective, l'appareil de sécurité mise davantage sur l'identification et la poursuite d'objectifs qui ont un intérêt stratégique pour l'État, contrairement au Canada, dont la posture des services de renseignements est réactive et le rôle se résume à alerter les autorités responsables, ainsi qu'à gérer des menaces intérieures.

Loin de concevoir le libre marché comme un lieu sanctuarisé, les États qui optent pour une posture proactive de leurs services de renseignements dans la sphère commerciale ont tendance à concevoir l'interaction public-privé de manière avantageuse, et iront jusqu'à instrumentaliser leurs fleurons nationaux comme une extension de l'appareil de sécurité nationale. En Chine, par exemple, l'enchevêtrement des sphères publique et privée est une caractéristique des plans stratégiques nationaux comme le PRC Medium and Long-Term S&T Plan (2006) et Made in China 2025 (2015). Le ministère de la Sécurité de l'État (MSE) et l'Armée populaire de Chine (APL) sont d'ailleurs directement impliqués dans le développement de sociétés d'État chinoises. Les craintes des autorités canadiennes face à ces sociétés (comme Huawei et AVIC) sont largement liées à cette synergie entre les entreprises et l'appareil d'État chinois.

Les technologies à double usage : le fer de lance d'États révisionnistes ?

L'intérêt mondial pour les technologies à double usage s'accroît, qu'il s'agisse du nucléaire, des systèmes de propulsion, de l'électronique ou des capteurs au laser. Au Canada, l'affaire entourant l'exportation clandestine de semi-conducteurs vers la Chine par un professeur de l'Université McGill est l'un des meilleurs exemples illustrant la convoitise d'États étrangers pour les technologies à double usage. Si les semi-conducteurs sont des composants essentiels aux technologies émergentes (5G, intelligence

artificielle et satellites quantiques), ils sont également indispensables pour la fabrication de missiles balistiques et de systèmes militaires de pointe. Alors que le marché mondial de l'industrie des semi-conducteurs est dominé par les États-Unis, la Corée du Sud et Taiwan, la Chine, qui consomme près de 60 % de cette production mondiale, tend à utiliser l'espionnage pour acquérir un avantage sur ce marché.

Les technologies à double usage trouvent également une utilité dans le domaine aérospatial. Les récents satellites lancés en orbite peuvent de plus en plus accomplir des tâches allant au-delà de la reconnaissance, la navigation, la météorologie et la communication. Plusieurs de ces satellites sont maintenant en mesure de collecter des informations sur des infrastructures civiles et militaires, de cartographier des territoires, de repérer des mouvements de troupes au sol et d'espionner d'autres satellites, comme ce fut le cas lorsque deux satellites « inspecteurs » russes se sont placés dans l'orbite d'un satellite de reconnaissance américain du programme *Keyhole* en février 2020.

CONCLUSION

Le Canada doit être conscient qu'il est reconnu mondialement pour son savoir-faire et ses investissements massifs en R&D dans certains secteurs de pointe. Pour protéger ce patrimoine immatériel, il s'avère important que le paradigme qui guide les services canadiens puisse continuer d'offrir un soutien stratégique aux décideurs, de s'arrimer au contexte international en perpétuelle évolution et de s'adapter à la mutation du secteur de la défense. Cela dit, il faut toutefois éviter d'interpréter les enjeux économiques internationaux de manière mercantiliste ou d'alimenter un climat de conflit permanent comme le font certains États.

IMPLICATIONS/RECOMMANDATIONS

- Le Canada devrait consolider le rôle du contre-espionnage (SCRS et Centre de la sécurité des télécommunications [CST]). Celui-ci a évolué ces dernières années face à l'émergence de menaces « stratégiques ». Néanmoins, le Canada doit faire du renseignement une condition *sine qua non* pour la concurrence internationale et la sécurité économique, notamment en ce qui a trait à la surveillance des activités clandestines sur le territoire, à sa capacité de collecte, à ses analyses à valeur ajoutée, ainsi qu'à son rôle-conseil à l'égard du secteur privé.

- Les services de renseignements devraient poursuivre leurs campagnes de sensibilisation auprès des entreprises des secteurs stratégiques, des organismes gouvernementaux et des universités. Il est impératif d'implanter une véritable culture de sécurité au sein d'entités qui possèdent des actifs de propriété intellectuelle. Au-delà de l'installation de dispositifs de sécurité physique, le Canada doit presser ces entités d'effectuer périodiquement des évaluations des menaces et des risques (EMR) de leur environnement stratégique. Les services de renseignements canadiens devraient également continuer d'encourager les entreprises à dénoncer les incidents d'espionnage économique, même si cela peut affecter la confiance des actionnaires.

- Dans le même ordre d'idées, le contre-espionnage canadien doit s'assurer que les mesures de sécurité mises en place par les entreprises stratégiques des cinq « Supergrappes » soient en phase avec les nouveaux types de menaces. Réunissant notamment des PMEs, des chercheurs universitaires et des organismes à but non lucratif, une Supergrappe est un programme de financement visant à encourager les industries les plus prometteuses du Canada. Le contre-

espionnage canadien devrait veiller à ce que l'écosystème de ces industries stratégiques en pleine expansion (comme les technologies numériques, les protéines végétales, la fabrication de pointe, l'intelligence artificielle et les technologies maritimes) soit protégé des risques d'espionnage en collaborant étroitement avec Innovation, Sciences et Développement économique Canada (ISDE).

- Le gouvernement canadien devrait centraliser l'appareil de sécurité nationale et établir un organe central, à l'instar de ses partenaires des Five Eyes (à l'exception de la Nouvelle-Zélande). Comme le propose Wesley Wark, par souci de cohésion, de coordination et de gouvernance, le Canada devrait repenser la structure de l'appareil de sécurité nationale en créant un pôle d'autorité capable d'unir les intérêts et les perspectives concurrentes de la Sécurité publique et du ministère de la Défense. Le Canada a besoin de cette autorité pouvant générer une réponse rapide et exercer un leadership en matière de sécurité économique et de cyberdéfense.