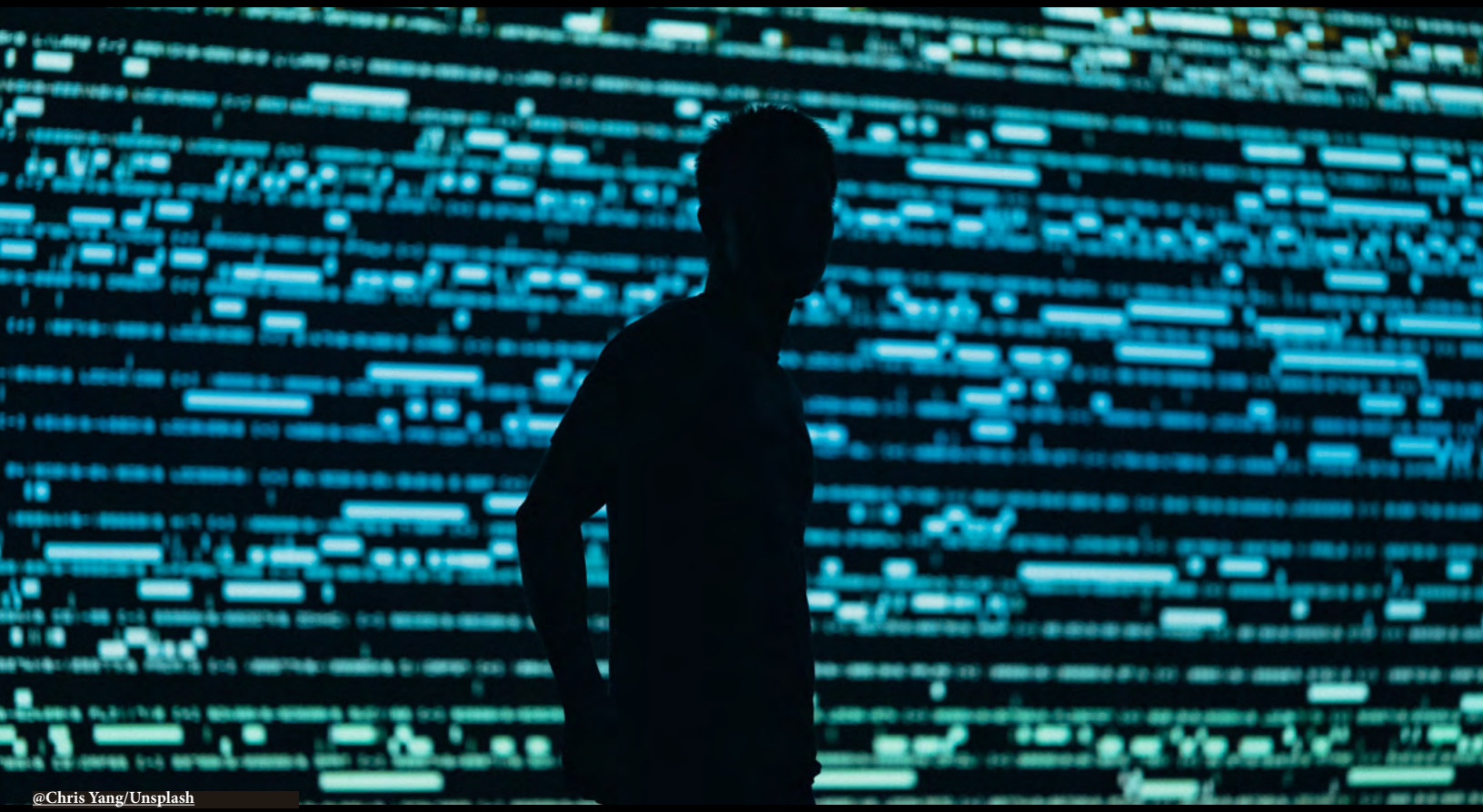
UQÀM | CHAIRE RAOUL-DANDURAND EN ÉTUDES STRATÉGIQUES ET DIPLOMATIQUES

CHRONIQUES DES NOUVELLES CONFLICTUALITÉS



@Chris Yang/Unsplash

Espionnage économique : quand le commerce durcit ses mœurs

Par Alexis Rapin

La récente inculpation d'un espion chinois présumé chez Hydro-Québec met en lumière les imposants efforts déployés par Pékin pour obtenir des secrets technologiques à l'étranger. Majeur, cet enjeu reste cependant souvent mal compris, et surtout inadéquatement traité, au Canada.

À la mi-novembre, un employé d'Hydro-Québec d'origine chinoise, soupçonné d'espionnage industriel au profit de Pékin, a été arrêté dans la région du grand Montréal. Actif dans les équipes de recherche et développement (R&D) de la société d'État, il aurait transmis à la République populaire certains secrets relatifs au développement de batteries pour véhicules électriques. Un marché sur lequel la Chine se montre particulièrement entreprenante depuis quelques années. Selon la Gendarmerie royale du Canada, les actes reprochés à l'espion présumé s'échelonneraient de janvier 2018 à août 2022.

Si cette récente affaire a créé l'émoi, elle n'est pas la première du genre au Canada. En décembre 2021, c'est à l'Agence spatiale canadienne que des soupçons d'espionnage au bénéfice de la Chine étaient soulevés, à l'encontre d'un ex-ingénieur. Un peu plus tôt, en juillet 2019, deux scientifiques d'origine chinoise travaillant au Laboratoire national de microbiologie de Winnipeg ont été escortés hors des lieux par la GRC puis congédiés, sans plus d'explications des pouvoirs publics. Bien que certains voient là tous les signes d'une affaire de vol de propriété intellectuelle, le flou (et le silence des autorités) persistent à ce jour sur le dossier.

En parallèle, loin des yeux, mais près du disque dur, un cyberespionnage économique quasi constant venu de la République populaire s'abat sur le Canada et ses entreprises : le répertoire des cyberincidents canadiens tenus par l'Observatoire des conflits multidimensionnels démontre qu'au moins 20 campagnes de piratage chinoises ont visé des entités canadiennes depuis 2010. Alors que l'essor de cet espionnage économique au Canada et ailleurs est désormais flagrant pour le grand public, les raisons profondes derrière celui-ci ne sont pas évidentes pour tout le monde. Comment les James Bond modernes en sont-ils venus à préférer les usines et bureaux de recherche aux bases militaires secrètes et autres palais présidentiels ?

Nouveaux joueurs et changements de règles

Les réponses à cette question sont multiples et variables, mais au moins deux grands faits majeurs font actuellement consensus parmi les spécialistes de l'espionnage.

D'une part, les dix dernières années ont consacré, sur la scène internationale, un net regain d'influence de deux pays, la Chine et la Russie, dans lesquels la séparation entre secteurs public et privé est pour le moins ténue. L'emprise des oligarques et du crime organisé en Russie, et la toute-puissance du Parti communiste en Chine, entérinent deux systèmes dans lesquelles l'appareil d'État est allègrement et agressivement mis au service de la compétitivité des entreprises ou du succès de certains milieux d'affaires. Un phénomène qui a largement pris de court des démocraties libérales jusqu'alors plutôt habituées à laisser le privé s'occuper de lui-même, et qui voient désormais leurs entreprises ciblées par des services de renseignement adverses.

D'autre part, un peu plus récente, mais non moins importante, la résurgence du nationalisme économique a quant à elle réécrit les règles, longtemps sacro-saintes, de la mondialisation et du libre-échange : de nouvelles politiques protectionnistes, le recours de plus en plus fréquent aux sanctions économiques, et le progressif découplage technologique entre la Chine et les États-Unis dessinent désormais un marché global dans lequel tout ne se vend et ne s'échange plus aussi facilement qu'auparavant. Dans cet ordre international économiquement fragmenté, les incitations à espionner, copier puis produire soi-même ce que l'on ne peut plus acheter à autrui sont donc toujours plus fortes.

Cas d'école en la matière, la grande saga Huawei laisse même entrevoir entre la Chine et les États-Unis l'avènement d'un cercle vicieux liant ces deux dynamiques : les craintes d'espionnage économique et autres pratiques déloyales suscitent des rétorsions

et mesures protectionnistes américaines, qui en retour viennent elles-mêmes stimuler d'autres actes d'espionnage chinois, dans le but d'obtenir les technologies ou savoirs dont l'accès vient d'être limité, et ainsi de suite. Entre méfiance mutuelle et velléités de découplage, beaucoup d'observateurs estiment ainsi que nous assistons à la formation et au durcissement progressif de deux « blocs » économiques, appelés à devenir toujours plus hermétiques et à se livrer une concurrence toujours plus féroce.

Au Canada, très tard et trop peu

Coincé entre ces deux géants, comment le Canada se positionne-t-il face à l'enjeu de l'espionnage économique ? En dépit des apparences, l'appareil du renseignement canadien a pris conscience des menaces de l'espionnage industriel chinois depuis près de 15 ans déjà. Cependant, les opportunités et bénéfices découlant de faire affaire avec une nation si florissante ont longtemps poussé secteurs privé et public à rester complaisants sur la question.

Ces atermoiements mettent aujourd'hui le Canada dans une position délicate : son arsenal juridique et ses capacités d'investigation en matière d'espionnage économique sont, comparativement à bon nombre d'autres pays, relativement faibles, à fortiori par rapport aux efforts massifs déployés par Pékin. Preuve de l'insuffisance des moyens canadiens : fin 2021, le procès d'un présumé espion chinois arrêté en 2013 en Ontario a été abandonné, la justice estimant que les autorités fédérales ont échoué à mener leurs poursuites dans un délai raisonnable.

Plus inquiétant encore, l'appareil du renseignement canadien ne semble pas seulement peiner à tenir les espions de la République populaire à distance des centres de recherche, mais aussi de ses propres rangs : en 2019, Cameron Jay Ortis, alors directeur du Centre national de coordination du renseignement de la GRC, a été arrêté pour avoir transmis des secrets à une puissance étrangère, très vraisemblablement la Chine.

Protéger ses ambitions

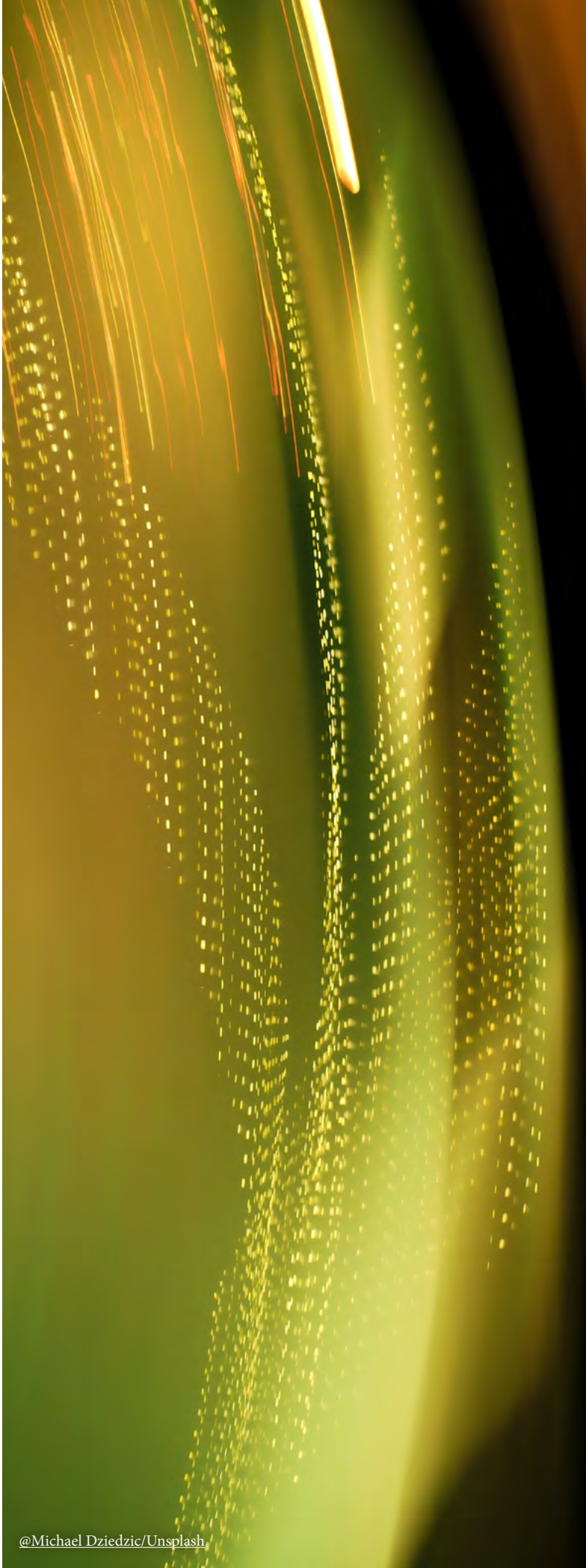
La récente inculpation du chercheur d'Hydro-Québec Yuesheng Wang consacre la toute première application de la loi canadienne portant sur le vol de propriété intellectuelle par des puissances étrangères, et, en ce sens, constitue un progrès. Pour autant, beaucoup reste à faire pour tenter de faire reculer les auteurs d'actes d'espionnage économique, particulièrement sur le plan cyber : la politique d'attribution[1] de cyberattaques étatiques du Canada par exemple demeure timide, Ottawa se refusant généralement à désigner des coupables si aucun pays allié ne se joint publiquement à ses conclusions.

Sur le plan judiciaire également, nombre de ressources font encore défaut pour adéquatement traduire en justice les espions présumés. À ce jour, aucun procureur fédéral n'a par exemple le mandat spécifique de poursuivre de tels actes. Alors que le Canada nourrit de grandes ambitions de recherche et développement dans des domaines de pointe, tels que l'intelligence artificielle ou les technologies quantiques, celui-ci doit rapidement se doter des moyens de protéger ses bonnes idées s'il entend les voir à l'avenir récompensées.

Alexis Rapin est chercheur à l'Observatoire des conflits multidimensionnels de la Chaire Raoul-Dandurand.

Pour en savoir plus sur la Chaire Raoul-Dandurand et ses travaux : https://dandurand.uqam.ca/

1 Dans le vocable de la cybersécurité, le terme d'attribution désigne le fait d'imputer officiellement une cyberattaque à un acteur spécifique. Sur la scène internationale, il s'agit le plus souvent d'un gouvernement désignant publiquement un autre État comme responsable.



@Michael Dziedzic/Unsplash