



Gouvernement
du Canada

Government
of Canada

[Canada.ca](#) > [Service canadien du renseignement de sécurité](#)

Allocution de M. David Vigneault, directeur du SCRS, au Centre pour l'innovation dans la gouvernance internationale

De : [Service canadien du renseignement de sécurité](#)

Discours

Ottawa – 9 février 2021 – Bonjour à tous et à toutes. C'est avec grand plaisir que je m'adresse à vous aujourd'hui. Je suis conscient des défis que pose l'organisation d'une activité comme celle-ci dans la « nouvelle normalité » et je tiens à remercier sincèrement le Centre pour l'innovation dans la gouvernance internationale pour son travail. L'activité d'aujourd'hui m'apparaît plutôt étrange : vous me voyez, mais je ne vous vois pas. Or, j'ai l'habitude du contraire. Habituellement, c'est moi qui observe.

J'ai souvent souligné la nécessité de tenir un dialogue approfondi, dans une perspective canadienne, sur la sécurité nationale. Ces questions sont beaucoup trop importantes pour que seuls les membres de l'appareil de sécurité s'en occupent. Votre participation est essentielle. Nous devons multiplier les échanges, rompre avec le traditionnel travail en silo et mettre en commun nos réflexions. Je suis heureux de constater que le Centre a récemment lancé un projet de recherche qui donnera un élan aux efforts visant à combler cette lacune.

9/9/24, 1:23 PM

Allocution de M. David Vigneault, directeur du SCRS, au Centre pour l'innovation dans la gouvernance internationale - Canada.ca

Aujourd'hui, il y a beaucoup d'incertitude dans le monde. Beaucoup de choses ont changé rapidement et, de toute évidence, beaucoup de choses changeront encore.

La pandémie de COVID-19 a eu une incidence profonde sur toutes les facettes de nos vies. Malgré ce stress, les employés du Service sont restés vigilants. Ils ont continué de surveiller les menaces qui pèsent sur la sécurité nationale, celles de longue date comme les nouvelles, pour remplir leur mission : protéger les Canadiens et les Canadiennes. Nous nous sommes tous ajustés à notre nouvel environnement. Les personnes à l'origine des menaces aussi. Aussi, le Service n'est pas resté immobile. Il est notamment sorti de l'ombre pour faire la lumière sur les menaces avec une énergie renouvelée.

La COVID-19 est à l'origine d'une certaine instabilité, d'une situation dont les changements rapides et successifs s'avèrent propices aux auteurs de menaces, qui cherchent à causer des préjudices ou à servir leurs intérêts. Alors que de nombreux Canadiens travaillent de leur domicile, des auteurs de menace peuvent tirer profit de nouvelles occasions de mener des activités malveillantes en ligne.

Par exemple, le Service a constaté que, pour justifier et rationaliser le recours à la violence, des extrémistes utilisent continuellement des services en ligne pour recruter et diffuser des messages haineux, des discours d'opposition aux autorités et des théories de conspiration sur la pandémie. Il a aussi observé une augmentation de l'utilisation de cyberoutils pour voler des informations sensibles, lancer des attaques au rançongiciel et causer des pannes. Le Service est aussi au fait des efforts d'États adverses pour diffuser de fausses informations sur la réponse à la pandémie pour discréditer le gouvernement et effriter la confiance envers la vaccination.

Le monde devient plus petit et plus concurrentiel, et les États cherchent naturellement à tirer profit du moindre avantage pour se positionner en chefs de file dans une économie mondiale.

Cette ambition pousse des acteurs étatiques hostiles à mobiliser tous les éléments du pouvoir de l'État pour faire progresser leurs intérêts nationaux. Cette situation n'a rien de nouveau, mais ces activités se sont intensifiées pendant la pandémie et continueront de s'intensifier alors que nous tentons de nous remettre d'une crise qui a porté préjudice à l'économie de différents pays.

Sur le plan de la sécurité nationale, les activités hostiles des acteurs étatiques, peu importe leur forme, font peser une lourde menace sur la prospérité et la souveraineté du Canada.

À titre d'exemple, l'espionnage peut avoir des conséquences profondes sur les travaux de recherche et de développement et, du coup, sur la réussite des entreprises canadiennes. En compromettant notre capacité à innover et à commercialiser le produit de nos recherches, l'espionnage cause la perte d'emplois et freine la croissance économique.

Quant à l'ingérence étrangère, elle consiste à miner nos institutions et notre démocratie. Elle s'attaque aux citoyens. Plus que tout, l'ingérence étrangère sape notre souveraineté et ébranle les normes de notre société.

L'ingérence et l'espionnage, qui s'ajoutent à bien d'autres menaces, contribuent à créer un environnement complexe.

Je vous propose donc maintenant de faire le point sur les menaces auxquelles le Service fait face.

L'extrémisme violent représente toujours une menace grave pour la sécurité publique. Le Service y consacre une part importante de son attention.

La menace découlant de l'extrémisme violent à caractère religieux, politique ou idéologique continue d'évoluer. Elle se complexifie. Souvent, les extrémistes ne sont plus influencés par un seul système de croyances définissable, mais par des doléances variées et très personnelles.

Aujourd'hui, les auteurs de menace exploitent de nombreux outils et services faciles d'accès qui leur permettent de communiquer entre eux en sécurité. Ils utilisent ces outils pour diffuser et intensifier les messages extrémistes, faire du recrutement ainsi que financer et planifier leurs activités sans quitter le confort de leur salon.

Par exemple, le Service a été témoin de changements chez des Canadiens, qui sont passés rapidement de partisans de DAECH à tenants d'une idéologie misogyne violente.

Le Service a constaté une hausse de l'extrémisme violent à caractère idéologique (EVCII). Aussi, depuis 2014, des Canadiens entièrement ou partiellement motivés par leurs opinions relevant de l'EVCII ont fait 21 morts et 40 blessés au Canada. En 2019, deux groupes d'adhérents à ce type d'idéologies ont été inscrits sur la liste des entités terroristes du Canada et quatre autres groupes y ont été inscrits la semaine dernière.

Cet enjeu est vaste et complexe. Il s'agit d'un problème de société qui nécessitera l'adoption d'une approche holistique. Tous les éléments de la société civile devront être mis à contribution pour le régler. Tout comme c'est le cas pour l'extrémisme violent à caractère religieux, le Service participe activement, aux côtés de ses partenaires de l'appareil du renseignement et des organismes d'exécution de la loi, à l'action concertée du gouvernement.

Même si l'extrémisme violent représente une menace persistante pour notre sécurité, et une importante source de préoccupations pour le Service, la plus lourde menace stratégique pour la sécurité nationale du Canada demeure les

activités hostiles d'États étrangers. Alors que le Service concentre ses ressources sur la protection des citoyens, il est témoin des manœuvres d'États hostiles qui mobilisent tous les éléments des pouvoirs étatiques pour faire progresser leurs intérêts nationaux au détriment du Canada.

Par le passé, les espions tentaient de mettre la main sur les secrets politiques, militaires et diplomatiques du Canada. Même si ces informations sont toujours intéressantes, aujourd'hui, ils concentrent leurs efforts sur les propriétés intellectuelles et les recherches avancées effectuées au moyen de systèmes d'ordinateurs de jeunes entreprises, de laboratoires universitaires et de salles de conférences.

Les cyberacteurs étatiques continueront de prendre pour cible les données sensibles et exclusives qui figurent dans ces réseaux, dont certains demeurent relativement ouverts et accessibles. Ils continueront d'utiliser des techniques très créatives et trompeuses pour accéder aux données revêtant une valeur stratégique et tactique.

Ces acteurs peuvent collecter de grands ensembles de données et tirer profit de systèmes d'analyse fondés sur l'intelligence artificielle. Une fois pleinement intégrés, ces systèmes examinent des ensembles de données communes pour détecter les menaces et les faiblesses. Si les données des citoyens ne sont pas protégées par des mécanismes rigoureux, il est facile d'y avoir accès et de les utiliser pour renforcer les capacités en matière d'intelligence artificielle.

Par exemple, en 2020, des sources de nouvelles mondiales ont révélé que Zhenhua Data Technology, qui fait principalement affaire avec l'armée et les services de renseignement chinois, a recueilli des données sensibles sur 2,4 millions de personnes pendant plusieurs années. Environ 20 % de ces données n'étaient pas du domaine public et ont probablement été obtenues au moyen de cyberespionnage.

Des entreprises ont été prises pour cible dans presque tous les secteurs de l'économie canadienne. Elles ont été compromises par des personnes et des cyberopérations. Certaines ont subi des pertes. Depuis de nombreuses années, le Service observe la tenue incessante d'activités liées à la menace parrainées par des États, activités qui sont aujourd'hui de plus en plus fréquentes et sophistiquées. Le SCRS enquête sur ces activités tous les jours, d'un océan à l'autre et à l'étranger.

Je tiens ici à préciser que certains secteurs sont plus visés que d'autres : la biopharmaceutique, la santé, l'intelligence artificielle, les technologies quantiques, les technologies marines et l'aérospatiale.

Les nouvelles technologies de ces secteurs d'activité font partie des plus vulnérables à l'espionnage étatique, parce qu'elles sont en grande partie créées dans les universités et de petites entreprises. Ces dernières représentent des cibles d'autant plus attirantes que leur effectif est parfois peu informé des risques pour la sécurité et que leurs installations sont souvent moins bien protégées que celles des grands organismes. En outre, elles sont plus susceptibles de chercher à conclure des partenariats et des marchés financiers dont, malheureusement, des pays étrangers abuseront.

Malheureusement, les enquêtes du Service montrent que cette menace a causé un préjudice important aux entreprises canadiennes. Sur le plan collectif, cela met en danger l'économie du savoir du Canada. Quand le Canada perd ses technologies et savoir-faire les plus innovants à cause de l'espionnage, c'est son avenir qui lui est volé.

Nos adversaires ne jouent pas selon les règles généralement convenues dans le monde.

Contrairement au Canada, certains pays ne font pas preuve de l'ouverture et de l'appui nécessaires à l'établissement de relations équitables. D'autres servent ardemment les intérêts de leurs secteurs économiques, militaires et du renseignement au détriment du Canada. Il n'est plus ici question d'échanges commerciaux entre entreprises privées.

Il s'agit plutôt de capitalisme d'État, une situation qui désavantage toujours le secteur privé du Canada.

Les employés et ex-employés, les étudiants, les professeurs, les entrepreneurs, les partenaires commerciaux et toutes autres personnes qui disposent de connaissances ou d'un accès aux systèmes d'un organisme peuvent être visés par un service de renseignement hostile et lui fournir des informations sensibles, à leur insu ou non.

Une personne bien placée qui agit pour le compte d'un auteur de menace peut compromettre un système et causer des dommages ou encore ouvrir une porte dérobée lui ouvrant accès aux données, qu'il se trouve de l'autre côté de la rue ou de l'autre côté de l'océan. Elle peut voler l'information sans détour et la faire sortir sur une clé USB.

Ce n'est pas un secret, le Service s'intéresse surtout aux activités des gouvernements de pays comme la Russie et la Chine. Cependant, il n'ignore pas l'évolution des activités liées à la menace et sait qu'elles peuvent être menées de partout dans le monde.

La Chine est un acteur important sur la scène internationale et un partenaire important du Canada à certains égards. Depuis des décennies, le Canada et les Canadiens entretiennent des relations avec des chercheurs, des universitaires, des artistes, des gens d'affaires chinois, entre autres. La mosaïque culturelle

de notre pays est d'autant plus riche en raison de la présence de Canadiens d'origine chinoise aux quatre coins du Canada, des grandes villes aux petits villages.

Je tiens à préciser ici que la menace n'émane pas de la population chinoise, mais du gouvernement de la Chine qui exécute une stratégie visant à faire des gains géopolitiques sur tous les fronts (économie, technologie, politique et armée). Ainsi, il exploite tous les éléments de pouvoir étatique dont il dispose pour mener des activités qui menacent directement notre souveraineté et notre sécurité nationale. Nous devons tous renforcer nos défenses.

Passons maintenant à la menace que constitue l'ingérence étrangère.

Il y a toujours eu de l'ingérence étrangère au Canada, mais l'importance, la rapidité, la portée et le retentissement de cette influence se sont accrus en raison de la mondialisation et des technologies. Le Service a constaté que les médias sociaux sont de plus en plus utilisés pour diffuser de fausses informations ou lancer des campagnes destinées à semer la confusion, à diviser la population, à interférer dans les bons débats publics et les discours politiques pour, finalement, engendrer des tensions sociales.

Ainsi, des États étrangers déploient des efforts contre les politiciens, les partis politiques et les processus électoraux pour influencer les décisions prises au Canada, l'opinion publique et, finalement, compromettre ses processus démocratiques. C'est une menace parmi les plus graves. Notre système électoral s'est avéré résilient, mais il faut travailler dur pour qu'il le reste. La vigilance est la meilleure défense qui soit.

Des États mènent régulièrement des activités hostiles. Ils menacent ou intimident des personnes au Canada pour susciter la peur, faire taire les dissidents et exercer une pression sur leurs opposants politiques. L'opération mondiale secrète du gouvernement de la Chine en est un bon exemple.

Connue sous le nom de Fox Hunt, cette opération s'attaque à la corruption. Mais elle servirait aussi à trouver et à faire taire les personnes qui s'opposent au régime.

Souvent, les personnes menacées n'ont pas les moyens de se défendre ou ignorent qu'elles peuvent dénoncer ces activités aux autorités canadiennes, y compris au Service. Qui plus est, ces activités ne suivent pas les règles de la diplomatie; elles visent à compromettre les processus démocratiques et à menacer des Canadiens de façon secrète et clandestine.

Aujourd'hui, je trouvais important de faire le point sur le contexte de la menace avec vous, compte tenu de l'importance des changements. Le monde a considérablement changé, tout comme les menaces, et ce, en très peu de temps. Une chose n'a pas changé et ne doit pas changer : c'est le sens de l'innovation et le dévouement des employés du SCRS. La grande qualité des enquêtes du Service, de ses analyses, des conseils qu'il prodigue et son côté décisif quand vient le temps de prendre des mesures pour contrer les menaces n'ont pas changé.

Toutefois, il est important de s'assurer que les pouvoirs du SCRS continuent d'évoluer, de sorte que le Service soit en mesure de relever les défis qui découlent du contexte beaucoup plus complexe dans lequel il évolue. Aujourd'hui, les menaces ont bien changé depuis l'adoption de la *Loi sur le SCRS* en 1984.

Cette *Loi*, qui s'appliquait bien aux menaces à l'ère de la Guerre froide, nuit grandement à la capacité du Service d'utiliser des outils modernes et d'évaluer les données et les informations. Le Service a besoin de lois qui lui permettront de mener des enquêtes axées sur ce genre de données, qui tiennent compte des valeurs véhiculées dans notre démocratie et qui offriront des mesures de protection de la vie privée rigoureuses.

La *Loi* permet au Service de prodiguer des conseils au gouvernement, mais limite sa capacité de fournir des conseils utiles à des partenaires clés, dont bon nombre d'entre vous sont à l'écoute en ce moment. En 1984, le législateur n'avait pas envisagé que, bien des années plus tard, la *Loi sur le SCRS* dresserait indûment des obstacles de nature technique à la collecte de renseignements et, par conséquent, limiterait les enquêtes.

Il s'agit là de quelques exemples des défis qui accompagnent les pouvoirs du Service. Au SCRS, nous prenons notre contrat social envers les Canadiens très au sérieux.

Contrairement à bon nombre de ses adversaires, le SCRS mène ses opérations dans une démocratie dans laquelle tous, même le gouvernement, sont soumis à la loi. Nous nous efforçons de rendre les meilleurs comptes qui soient. Une bonne façon d'y parvenir consisterait à tenir une discussion saine sur les attentes des Canadiens à l'égard des organismes de sécurité nationale et à déterminer si les lois ont évolué au même rythme.

J'aimerais profiter de l'occasion pour donner plus de détails sur la nécessité d'établir de solides partenariats.

Qu'il s'agisse d'extrémisme violent, d'espionnage ou d'ingérence étrangère, aucun organisme gouvernemental ne peut, à lui seul, neutraliser ces menaces. Pour y arriver, il faut établir des partenariats stratégiques entre organismes gouvernementaux, privés ou autres. Les partenariats facilitent la communication des informations, la consultation, la mise en commun des ressources et de l'expertise et la prise de mesures conjointes.

Avec la pandémie, j'observe ce phénomène en temps réel. En partageant sa connaissance de différents dossiers, le Service intensifie sa collaboration avec certains de ses partenaires, comme l'Agence de la santé publique du Canada. Il travaille aussi en étroite collaboration avec Innovation, Sciences et

9/9/24, 1:23 PM

Allocution de M. David Vigneault, directeur du SCRS, au Centre pour l'innovation dans la gouvernance internationale - Canada.ca

Développement économique Canada, entre autres, pour faire connaître la façon dont les investissements étrangers pourraient compromettre la sécurité nationale. Le Service fait tout ce qui est en son pouvoir pour éviter que le Canada prête le flanc aux attaques.

J'ai parlé de la façon dont le Service est sorti de l'ombre pendant la pandémie. Il a immédiatement remarqué que les universités canadiennes, les instituts de recherche médicale, les pharmaceutiques et autres appelés à participer à la lutte nationale contre la pandémie couraient un risque accru de cybersécurité. Le Service a travaillé en étroite collaboration avec ses partenaires dans les universités ainsi que le Centre canadien sur la cybersécurité, pour intervenir comme il se devait.

Il est également nécessaire d'établir des partenariats au-delà de nos frontières, surtout entre les membres du Groupe des cinq et du G-7, entre autres pays démocratiques d'idéologie libérale semblable. Ce n'est qu'en mobilisant des partenaires d'optique commune qu'il est possible de repousser les États hostiles.

Pour garder le Canada en sécurité, il faut avoir une population bien informée des questions de sécurité nationale. Par là, je veux dire que les citoyens doivent comprendre les dilemmes importants auxquels le Canada est confronté et être conscients qu'il faut s'adapter et répondre de façon réfléchie, significative et opportune.

Je vous invite à considérer le Service comme un partenaire et à communiquer avec lui pour obtenir des informations, des conseils et du soutien lorsque votre entreprise, votre université ou votre organisme sera appelé à naviguer les eaux de plus en plus houleuses de la géopolitique.

Peut-être vous direz-vous qu'en tant qu'universitaires, scientifiques ou entrepreneurs, la sécurité nationale ne vous concerne pas.

Eh bien, je vous assure que la géopolitique s'intéresse à vous.

Il est important que vous compreniez les risques auxquels vous faites face et la façon dont vous pouvez protéger vos intérêts.

Lorsque vous communiquerez avec le Service, vous constaterez l'expertise et le dévouement de ses employés. À titre de directeur, je tire ma plus grande fierté de la qualité de son effectif. Ces personnes sont incontestablement la ressource la plus précieuse de l'organisme.

Le SCRS, en tant que service national de renseignement et de sécurité, doit refléter la société qu'il protège. Notre effectif est divers et inclusif comme la population canadienne elle-même. Grâce à notre diversité, nous sommes mieux à même de comprendre les communautés du Canada et d'assurer le lien de confiance nécessaire entre la société civile et les agences de renseignement. En retour de la confiance des Canadiens, nous nous engageons à répondre à de hautes normes de redevabilité.

Aujourd'hui, j'ai dressé un portrait des principales menaces que nous devons tous connaître et nous efforcer de contrer.

Je peux vous assurer que le SCRS, en collaboration avec le gouvernement du Canada et ses partenaires internationaux, enquête sur les auteurs de menace préjudiciables, les surveille et contrecarre leurs activités dans les limites de son mandat.

Ces efforts s'inscrivent dans ceux que déploie le gouvernement du Canada pour protéger les Canadiens et leurs intérêts. Par exemple, le Service surveille de plus près tous les investissements directs étrangers en vertu des dispositions de la Loi sur Investissement Canada en matière de sécurité nationale et le Groupe de travail sur les menaces en matière de sécurité et de renseignement visant les élections travaille à contrer l'ingérence étrangère dans les élections. Qui plus est, le Service s'est efforcé de cerner les nouveaux

9/9/24, 1:23 PM

Allocution de M. David Vigneault, directeur du SCRS, au Centre pour l'innovation dans la gouvernance internationale - Canada.ca

secteurs à sensibiliser afin d'aider les entreprises privées, les associations et les universitaires à comprendre comment protéger leurs propriétés intellectuelles.

J'aimerais conclure aujourd'hui en vous posant des questions auxquelles je vous demande de réfléchir.

Par exemple, après la pandémie, quelles seront les répercussions de la reprise économique du Canada sur la sécurité nationale?

Quelles sont les attentes des Canadiens quant à l'usage, par les autorités canadiennes, de puissantes technologies d'analyse de données pour le bien commun?

Comment peut-on éviter que nos données et nos travaux de recherche servent, à notre insu, les intérêts liés au commerce, à l'armée et au renseignement d'États hostiles?

Ce ne sont là que quelques questions qui s'imposent lentement au Service et à l'ensemble des Canadiens?

Il n'y a pas de plus grande responsabilité pour un gouvernement que de protéger ses citoyens. Dans le contexte de la menace dynamique d'aujourd'hui, il est important que le gouvernement, la société civile et le secteur privé travaillent de concert pour renforcer nos défenses et pour protéger nos intérêts nationaux. Je vous demande à tous de travailler avec le SCRS pour faire progresser cet appel à l'action afin d'assurer la sécurité des Canadiens et protéger notre économie, pour notre avenir et celui de nos enfants. Je suis optimiste. Je suis convaincu que nous pouvons y arriver. Nous devons y arriver!

Merci Aaron et merci à tous ceux et celles qui m'ont écouté en ligne. Je m'arrête ici, et je répondrai avec plaisir à vos questions.

9/9/24, 1:23 PM

Allocution de M. David Vigneault, directeur du SCRS, au Centre pour l'innovation dans la gouvernance internationale - Canada.ca

Personnes-ressources

Renseignements

Relations avec les médias

(613) 231-0100

media-medias@smtp.gc.ca

Recherche d'information connexe par mot-clés: [Renseignement de sécurité](#)
| [Service canadien du renseignement de sécurité](#) | [Canada](#) | [Sécurité nationale](#) | [grand public](#) | [discours](#)

Date de modification :

2021-02-09