

Numéro 87 - 21 décembre 2020

La motion de la Chambre des communes contre la Chine
Le retour de l'hystérie du «péril jaune»

- Pauline Easton -



À titre d'information

- **La motion contre la Chine**

Qui décide ce qui constitue une menace à la sécurité nationale

- **C'est aux Canadiens et non à la police à décider ce qui constitue une menace à la «sécurité nationale»**
- Anna Di Carlo -
- **Des «évaluations des menaces» d'inspiration étrangère contre le Canada**
- Pauline Easton -
- **Des évaluations de menaces fondées sur des intérêts commerciaux**
- Nick Lin -
 - **Les propos alarmistes au sujet de la chaîne d'approvisionnement du Canada**
 - **Grande opération de désinformation de l'Inde**
- **Un deuxième juge bloque la tentative de Trump d'interdire une application chinoise des médias sociaux**

La motion de la Chambre des communes contre la Chine

Le retour de l'hystérie du «péril jaune»

- *Pauline Easton* -

La Chambre des communes examine une motion qui incite à l'hostilité envers la République populaire de Chine. Les partis cartellisés s'engagent sur la voie imprudente de faire la guerre aux prétendues tentatives chinoises de miner les « institutions démocratiques » du Canada. Sous prétexte d'« éliminer l'ingérence étrangère du processus politique du Canada », la résolution criminalise les Canadiens et les résidents permanents d'origine chinoise et, de manière générale, attise un climat hystérique raciste antichinois. C'est une reprise de l'approche raciste et colonialiste qui, au début du XXe siècle, accusait les personnes originaires d'Asie de constituer un « péril jaune ». Une définition du terme « péril jaune » dans le dictionnaire est : « le pouvoir ou le prétendu pouvoir des peuples asiatiques de menacer ou de détruire la suprématie de la civilisation blanche ou occidentale[1] ».

Selon Wikipédia anglais, c'est « une métaphore colorée qui présente les peuples d'Asie orientale comme un danger existentiel pour le monde occidental[2] ».

La motion mérite également l'attention des Canadiens pour son mode opératoire insidieux. Le droit des citoyens et des résidents d'exprimer leurs opinions sur les affaires internationales est en train d'être transformé en une question de personnes « dupées par une puissance étrangère ». La pratique internationale, voire le droit, des pays de promouvoir leurs intérêts économiques, comme le fait le Canada partout dans le monde, est considérée comme acceptable pour le Canada et les États-Unis, mais pas pour la Chine. Au nom de la sécurité nationale, le Canada, les États-Unis et les autres pays de l'alliance des services de renseignement du « Groupe des cinq » peuvent autoriser des entreprises comme Google, Twitter, Facebook et d'autres à surveiller leurs citoyens parce que cela est considéré comme démocratique, mais si la Chine le fait, c'est considéré comme dictatorial. De même, la domination de la gouvernance du Canada par des partis cartellisés, qui servent tous l'oligarchie financière internationale, est considérée comme démocratique, tandis que la domination du Parti communiste de Chine sur la gouvernance en Chine est considérée comme une dictature.

Le pouvoir des intérêts privés domine ce discours qui définit ce qui est dans l'intérêt national du Canada. Ces intérêts privés se sont emparés de l'État des États-Unis, auquel ils ont également subordonné l'État canadien. Ils utilisent leur appareil de désinformation et leurs budgets pour mettre tout le poids de l'État à contribution dans leur effort pour éliminer les concurrents. Les peuples des pays qui composent le système impérialiste d'États sont censés prendre parti.

Selon David Vigneault, directeur du Service canadien du renseignement de sécurité (SCRS), « 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 lucrative. Cette soif de concurrence pousse des acteurs étatiques hostiles à mobiliser tous les éléments du pouvoir de l'État pour faire progresser leurs intérêts nationaux. Cette menace représente le plus grand danger pour la sécurité nationale du Canada et peut avoir de terribles répercussions sur la croissance économique, la capacité d'innover, la souveraineté et les intérêts nationaux du pays. C'est la raison pour laquelle le SCRS échange régulièrement maintenant avec divers intervenants de l'ensemble du gouvernement du Canada, du secteur privé et du secteur de la recherche pour en apprendre davantage et pour les conseiller sur la nature des menaces éventuelles afin qu'ils puissent mieux se préparer et protéger leurs importants travaux[3]. »

Cet aveu que les « intérêts nationaux » du Canada sont servis par les services de sécurité qui défendent les intérêts des oligarques financiers et économiques dans leurs rivalités pour dominer les marchés et les sphères d'influence montre dans quelle mesure ils trouvent eux-mêmes des

justifications pour « mobiliser tous les éléments du pouvoir de l'État » dans le sens de leur propre positionnement dans cette « économie mondiale lucrative », poussés par leur « soif de concurrence ». Cela confirme la grave menace qui pèse sur les peuples. Dans le modus operandi établi, cette rivalité ne peut que conduire à l'agression, à la guerre et à l'ingérence à l'étranger, et à la répression des mouvements des peuples au pays et à l'étranger. Les peuples se battent pour un monde nouveau où les économies sont organisées de manière à répondre aux besoins de la population et où les relations internationales, y compris le commerce, sont fondées sur l'avantage mutuel et où les conflits d'intérêts sont résolus de manière pacifique.

Vigneault félicite le gouvernement d'avoir adopté la loi de 2017 sur la sécurité nationale, qui a reçu la sanction royale en juin 2019. Cette loi a été largement contestée par les Canadiens lorsqu'elle a été présentée par le gouvernement Harper, puis adoptée par le gouvernement Trudeau avec des amendements d'apparence pour faire croire que les droits étaient protégés. Selon le directeur du SCRS, les modifications « ont réglé certains problèmes et conféré au SCRS quelques nouveaux pouvoirs, mais il reste encore du travail à faire ». Il appelle plus explicitement à un renforcement des pouvoirs de police quand il écrit qu'« il faudra pousser la réflexion plus loin encore pour faire en sorte que le SCRS dispose des outils dont un service de renseignement moderne a besoin dans le contexte de la menace d'aujourd'hui, et celui de demain ».

Un des exemples de « contexte de la menace d'aujourd'hui » autour duquel la communauté de la sécurité crée l'hystérie actuellement est la prétendue ingérence étrangère dans la distribution des vaccins de la COVID[4].

Il est important de souligner le rôle prépondérant, et occulte par définition, des services de renseignement des « Groupe des cinq » dans le processus décisionnel. Ces services agissent comme ils l'entendent sans que les citoyens ne sachent jamais ce qu'ils font et comment ils le font. Les décideurs au sein du gouvernement agissent également comme ils l'entendent.

En imposant des conceptions de la sécurité, de la paix et de la démocratie tirées de la période de la guerre froide, ils montrent que leurs agissements sont intéressés. Les intérêts que ces conceptions servent et ceux qui les servent ne reconnaissent pas, et représentent encore moins, les membres du corps politique dont les voix ne sont pas entendues, voire dont les voix sont totalement absentes de ce qui passe pour débat.

Tous les partis à la Chambre des communes soutiennent cette motion. Ils se chamaillent sur des détails, comme à savoir si elle doit être adoptée ou non avant d'être examinée par le Comité spécial sur les relations sino-canadiennes, qui est lui-même un instrument de propagande contre la Chine et dont le but est de cacher le désespoir de ceux qui veulent éliminer la Chine comme concurrent[5].

Notes

1. Dictionnaire *Collins*

2. Le terme « péril jaune » a été inventé en Europe après la défaite militaire de la Chine par le Japon en 1895 et a été initialement appliqué au Japon pour créer une peur d'invasion face à la montée en force des puissances d'Asie orientale.

La peur de l'invasion s'est poursuivie au XXe siècle et a été renforcée par diverses représentations racistes d'Orientaux aux allures sinistres dans des livres et des films. Parmi celles-ci, on peut citer la création de l'écrivain anglais Sax Rohmer, le génie insidieux et diabolique du Dr Fu Manchu.

Au début de la Première Guerre mondiale, en l'absence d'invasion réelle le discours sur le péril jaune a commencé à s'estomper, mais la création de la peur au sujet de la Chine et des immigrants d'Asie de l'Est s'est poursuivie avec d'autres expressions dénigrantes, en appui aux politiques racistes d'immigration au pays et à l'agression impérialistes à l'étranger.

3. *Rapport public du SCRS 2019 : Des renseignements et des conseils fiables pour un Canada sûr et prospère*, mai 2020

4. « CSIS warns of threats to vaccine distribution chain », Catharine Tunney, CBC News, 17 décembre 2020

5. Le site web du Comité dit que « le Comité a été nommé par la Chambre pour tenir des audiences servant à examiner tous les aspects des relations sino-canadiennes, y compris ceux qui ont trait aux relations consulaires, économiques et diplomatiques, au droit et à la sécurité. »

Il dit également :

« Les liens entre le Canada et Hong Kong sont anciens et bien connus, notamment en raison de la participation de soldats canadiens, dont nombreux sont morts, à l'effort de guerre pour repousser l'invasion japonaise pendant la Deuxième Guerre mondiale. Aujourd'hui, on estime à 300 000 le nombre de Canadiens vivant à Hong Kong.

« Les libertés et le haut degré d'autonomie de Hong Kong ont été consacrés par la déclaration conjointe sino-britannique de 1984, un traité enregistré auprès des Nations unies. Comme on l'a dit au comité spécial, la communauté internationale a été invitée à soutenir le cadre « un pays, deux systèmes » et à coopérer à la réussite de sa mise en oeuvre. Le Comité spécial note que, bien que le cadre doive durer jusqu'en 2047, de sérieuses questions ont été soulevées par la *Loi de sécurité nationale* promulguée le 30 juin 2020. En outre, le Comité spécial réaffirme que les libertés consacrées par la Déclaration conjointe et la Loi fondamentale de Hong Kong, notamment la liberté d'expression et de réunion, sont garanties par le Pacte international relatif aux droits civils et politiques, qui s'applique à Hong Kong. »

Parmi les personnes et les représentants d'organisme qui ont témoigné devant le Comité cette année il y a :

Réunion 8, le mardi 8 décembre 2020 :

Ministère des Affaires étrangères, du Commerce et du Développement

- Shawn Steil, directeur général, Politique et coordination de la Chine élargie

Ambassade du Canada en République populaire de Chine

- Dominic Barton, ambassadeur extraordinaire et plénipotentiaire du Canada en République populaire de Chine

Réunion 8, le mardi 24 novembre 2020 :

À titre personnel

- L'hon. John McCallum, ancien ambassadeur du Canada en République populaire de Chine

- Robert G. Wright, ancien ambassadeur du Canada en République populaire de Chine

Réunion 7, le lundi 23 novembre 2020 :

Ministère des Affaires étrangères, du Commerce et du Développement

- Weldon Epp, directeur général, Direction générale de l'Asie du nord et Océanie

- Marta Morgan, sous-ministre, Affaires étrangères

- L'hon. François-Philippe Champagne, ministre des Affaires étrangères

Réunion 6, le mardi 17 novembre 2020 :

Ministère des Affaires étrangères, du Commerce et du Développement

- Shawn Steil, directeur général, Politique et coordination de la Chine élargie

Réunion 5, le lundi 16 novembre 2020 :

Ministère de la Citoyenneté et de l'Immigration

- Mme Nicole Giles, sous-ministre adjointe associée déléguée, Opérations

- Natasha Kim, sous-ministre adjointe associée, Politiques stratégiques et de programmes

- L'hon. Marco Mendicino, ministre de l'Immigration, des Réfugiés et de la Citoyenneté

Réunion 4, le lundi 9 novembre 2020 :

National Democratic Institute

- Adam Nelson, conseiller principal pour Asie-Pacifique

Vancouver Society in Support of Democratic Movement

- Mabel Tung, présidente

À titre personnel

- Bill Chu, fondateur, Canadians for Reconciliation
- Victor Ho, éditeur en chef à la retraite, Sing Tao Daily, édition Colombie-Britannique
- Steve Tsang, directeur, SOAS China Institute, University of London

Réunion 3, le lundi 2 novembre 2020 :

Consulat général du Canada à Hong Kong et Macao

- Jeff Nankivell, consul général du Canada à Hong Kong et Macao, Affaires mondiales Canada

Réunion 2, le lundi 26 octobre 2020 :

À titre personnel :

- Angela Gui
- Nathan Law, militant de Hong Kong, ancien législateur

À titre d'information

La motion contre la Chine

La motion contre la Chine a été présentée à la Chambre des communes le 17 novembre 2020 par le député conservateur Michael Chong. La motion et le débat montrent le refus de résoudre pacifiquement les problèmes dans les relations internationales et en font une question de lutte entre factions, de promotion d'intérêts commerciaux et de positions anti-chinoises hystériques. Voici le texte de la résolution :

« Que, étant donné (i) que la République populaire de Chine, qui est dirigée par le Parti communiste chinois, menace les intérêts nationaux du Canada et les valeurs de la population canadienne, y compris les Canadiens d'origine chinoise en territoire canadien, (ii) qu'il est essentiel que le Canada se dote d'une politique étrangère rigoureuse et fondée sur des principes appuyée par des actions de concert avec ses alliés, la Chambre demande au gouvernement : a) de prendre une décision au sujet de l'implication de Huawei dans le réseau 5G du Canada dans les 30 jours suivant l'adoption de la présente motion ; b) d'élaborer un plan robuste, comme l'a fait l'Australie, pour lutter contre l'ingérence de plus en plus forte de la Chine au Canada et l'intimidation sans cesse croissante des Canadiens vivant au Canada, et de le présenter dans les 30 jours suivant l'adoption de la présente motion. »

En présentant la résolution, Michael Chong a dit que bien que le gouvernement libéral ait « réalisé certains accomplissements en matière d'affaires étrangères », comme la renégociation de l'accord de libre-échange avec les États-Unis, dans son ensemble, « la politique étrangère globale du gouvernement nous déçoit ». Il a déclaré :

« C'est à propos de la Chine que le gouvernement libéral nous a le plus déçus. La Chine n'assume pas les responsabilités qui sont les siennes dans l'ordre mondial international fondé sur des règles où nous évoluons. Elle fait fi des conditions de son entrée à l'Organisation mondiale du commerce. Elle manipule sa monnaie en utilisant des entreprises d'État pour nuire à l'économie d'autres pays. Elle enfreint le droit international de la propriété et fait subir aux Canadiens Michael Kovrig, Michael Spavor, Gary Schellenberg et Hussein Jalil un traitement qui est également contraire au droit international. Elle ne respecte pas non plus le droit international lorsqu'il s'agit des Hongkongais et des minorités religieuses et ethniques, comme les Tibétains et les Ouïghours. En somme, la Chine menace nos intérêts et nos valeurs.

Dans ce contexte, il est très important que le gouvernement du Canada tienne toujours le même discours clair et cohérent. Ce n'est pas ce qui se passe, malheureusement.

En janvier de l'année dernière, le premier ministre a déclaré qu'il ne s'ingérerait pas dans la procédure judiciaire concernant Meng Wanzhou, à Vancouver. La même semaine, l'ancien ambassadeur du Canada en Chine, John McCallum, déclarait que le gouvernement devrait intervenir et échanger Meng Wanzhou contre les Canadiens Michael Kovrig et Michael Spavor.

Les incohérences ont continué cette année. En juillet, le ministre des Affaires étrangères a déclaré à la Chambre qu'il envisageait d'imposer des sanctions aux dirigeants chinois responsables de ce qui se passe à Hong Kong. Le lendemain, le gouvernement a affirmé à Reuters que cette mesure avait été écartée.

En septembre, le ministre des Affaires étrangères déclarait au *Globe and Mail* que les efforts visant un accord de libre-échange avec la Chine étaient abandonnés, alors que le même jour, l'ambassadeur du Canada en Chine affirmait devant un auditoire à Edmonton, dont l'ambassadeur de Chine au Canada faisait partie, que le Canada devrait en faire plus en Chine et accroître ses échanges commerciaux.

Ce n'est qu'un exemple parmi tant d'autres.

Le gouvernement reconnaît implicitement lui-même que sa politique envers la Chine ne marche pas. Il l'a reconnu par le changement de son discours sur la Chine cet automne, et il l'a reconnu en annonçant qu'il envisageait de présenter un nouveau cadre pour la Chine d'ici le 24 décembre. Voilà pourquoi j'ai présenté cette motion aujourd'hui.

Tout nouveau cadre pour la Chine doit inclure deux éléments.

D'abord, il doit inclure une décision sur Huawei. En mai de l'année dernière, le gouvernement a affirmé qu'il prendrait une décision à propos de l'implication de Huawei dans le réseau 5G du Canada avant les élections de 2019. En juillet de la même année, le gouvernement a changé d'idée en disant qu'il prendrait une décision après les élections de 2019.

Les dernières élections remontent maintenant à plus d'un an, et la décision se fait toujours attendre. Le gouvernement réfléchit à cette question depuis des années. Son attentisme et ses tergiversations menacent la sécurité nationale du Canada. À cause des retards du gouvernement dans ce dossier, Telus, une grande entreprise de télécommunications canadienne, a acheté de l'équipement de Huawei pour son réseau. Elle l'a installé dans la région de la capitale nationale, où se trouvent la plupart des bureaux des institutions fédérales du Canada, comme la GRC, le SCRS, le ministère de la Défense nationale et d'autres installations militaires. Pourtant, elle avait conclu une entente avec le gouvernement fédéral, qui excluait l'utilisation d'équipement de Huawei dans la région. On apprend maintenant que le gouvernement fait des pieds et des mains pour que Telus retire son équipement, qui a été installé sur quelque 80 tours et sites dans la région de la capitale nationale. Selon l'article 7 de la loi chinoise sur le renseignement national, Huawei doit offrir son soutien, son aide et sa coopération à la Chine dans ses activités de renseignement.

L'inaction du gouvernement relativement à Huawei révèle autre chose : l'écart abyssal entre ses belles paroles et la réalité. Il dit croire au multilatéralisme, mais il ne saisit pas les occasions qui se présentent. Huawei en est un parfait exemple. Quatre des partenaires en matière de renseignement du Groupe des cinq, l'Australie, la Nouvelle-

Zélande, les États-Unis et le Royaume-Uni, ont exclu Huawei de leur réseau ou ont limité sa participation. Le Canada est le seul à rester les bras croisés.

Il est grand temps que le gouvernement prenne une décision concernant Huawei. Aucun cadre relatif à la Chine ne peut être complet sans une telle décision. Tout nouveau cadre relatif à la Chine doit aussi comprendre un plan rigoureux pour contrer les activités subversives que la Chine mène au Canada. Par l'entremise de ses représentants et des activités qu'elle mène sur notre territoire, la Chine menace les intérêts et les valeurs du Canada. Elle intimide des Canadiens, particulièrement des Canadiens d'origine chinoise. Elle espionne les citoyens et les entreprises du Canada, ainsi que le gouvernement fédéral, et elle lance des cyberattaques contre eux. Elle fait de la désinformation. Elle pratique l'accaparement des ressources par les élites en offrant des avantages financiers et des sinécures à des fonctionnaires et à des politiciens à la retraite. Elle soutient financièrement des instituts de recherche qui appuient les positions de Pékin, comme l'Institut Confucius. Elle s'adjoint des médias et des organismes locaux de langue chinoise sur le terrain pour promouvoir les intérêts de Pékin. Elle surveille et mobilise des étudiants chinois qui fréquentent des universités canadiennes pour étouffer les débats sur les campus et menacer d'autres étudiants, comme elle l'a fait à l'Université de Toronto et à l'Université McMaster. Elle s'ingère dans la communauté chinoise en sollicitant un appui politique contre ceux qui ne soutiennent pas Pékin.

Le Service canadien du renseignement de sécurité, la GRC, Amnistie internationale et le Comité spécial sur les relations sino-canadiennes de la Chambre ont documenté d'innombrables exemples d'activités d'influence menées par la Chine au Canada. Tout nouveau cadre relatif à la Chine doit comprendre un plan qui en fait davantage pour protéger les Canadiens contre les activités d'influence de la Chine au Canada, comme l'ont déjà fait nos alliés, notamment l'Australie.

Le gouvernement est arrivé au pouvoir en parlant de conviction responsable. Ce principe a été abandonné pour celui voulant que le Canada soit un pays essentiel. Nous parlons maintenant d'un nouveau cadre pour la Chine. Tout nouveau cadre doit comprendre une décision au sujet de Huawei ainsi qu'un plan robuste pour protéger les citoyens et les intérêts canadiens des activités d'ingérence subversives de la Chine en sol canadien.

Mon dernier point porte sur le délai prévu dans la motion. Cette dernière demande au gouvernement de prendre ces deux décisions dans les 30 jours. Le gouvernement dit depuis des mois qu'il va présenter un nouveau cadre relativement à la Chine d'ici la fin de l'automne, donc d'ici le 21 décembre. Par conséquent, le délai prévu dans cette motion est très raisonnable. C'est pourquoi j'ai présenté cette motion. J'espère que les députés vont l'appuyer. »

Au nom du Bloc Québécois, Luc Desilets (Rivière-des-Mille-Îles, BQ) a déclaré que son parti était d'accord et qu'il n'avait que quelques inquiétudes quant au délai. Il a déclaré :

« Pourquoi n'attendrait-on pas les conclusions du Comité spécial sur les relations sino-canadiennes, que les conservateurs eux-mêmes ont demandé ? »

Au nom du NPD, Gord Hohn (Courtenay-Alberni, NPD) a remercié Michael Chong pour la motion et a posé une question :

« J'aimerais savoir si, à son avis, le Canada devrait adopter une mesure législative visant à combattre l'ingérence de la Chine et d'autres États au Canada. »

Michael Chong a dit :

« Oui, nous sommes d'avis que le Canada a besoin d'un nouveau cadre législatif pour traiter différents enjeux. À titre d'exemple, selon nous, les anciens politiciens et anciens fonctionnaires de haut niveau devraient inscrire leurs contrats dans un registre lorsqu'ils travaillent pour un État étranger ou une entité contrôlée par un État étranger. Par ailleurs, nous sommes d'avis que les forces de l'ordre devraient être mieux outillées pour contrer les activités subversives par lesquelles la Chine cherche à exercer son influence en sol canadien. Ce ne sont là que deux des changements qui nécessiteraient un nouveau cadre législatif et qui nous permettraient d'être mieux outillés pour contrer ces activités. »

Au nom du gouvernement libéral, le ministre des Affaires étrangères, François-Philippe Champagne, a déclaré :

« Monsieur le Président, j'ai été heureux d'assister au discours du député ce matin. Il a oublié de mentionner une chose, et c'est là-dessus que porte ma question : le leadership du Canada quand il s'agit de passer à l'action.

Pourquoi le député omet-il de dire aux Canadiens qui suivent le débat que le Canada a été le premier pays à suspendre le traité d'extradition entre le Canada et Hong Kong ? Pourquoi ne dit-il pas aux Canadiens que le Canada a suspendu l'exportation d'équipement sensible ? Pourquoi le député ne mentionne-t-il pas que nous avons pris des mesures en matière d'immigration ?

J'ai présidé la réunion du Groupe des cinq et j'ai consulté nos homologues britanniques tout au long du processus. Pourquoi le député omet-il de dire que nous continuons à collaborer avec nos partenaires de partout dans le monde pour exercer notre leadership, passer à l'action et défendre les valeurs et les intérêts canadiens ? »

Qui décide ce qui constitue une menace à la sécurité nationale

C'est aux Canadiens et non à la police à décider ce qui constitue une menace à la «sécurité nationale»

- Anna Di Carlo -

Les évaluations des menaces émises par les services de renseignement canadiens sont remplies de messages qui ciblent la parole et les associations jugées menaçantes pour la sécurité nationale. Le Parti marxiste-léniniste du Canada a déclaré qu'il s'oppose au recours à la menace d'une ingérence étrangère dans les élections et/ou de « nos institutions démocratiques » et/ou de notre « mode de vie », pour justifier la violation des droits de parole et d'association des Canadiens. Selon toute définition moderne qui mérite d'être qualifiée de démocratique, le peuple a le droit de s'opposer à l'ingérence de l'État lorsqu'il est question de son droit de pouvoir s'exprimer et s'associer librement.

Une motion contre la Chine est actuellement devant la Chambre des communes et les « évaluations » actuelles par les agences de renseignement des « menaces à la sécurité nationale » montrent que l'approche du gouvernement libéral et du Parti conservateur, qui se considère comme le gouvernement en attente, est d'autoriser les pouvoirs de police à surveiller de près les discours et les activités politiques pour y rechercher une « ingérence étrangère ». Nous sommes censés croire que l'opposition à « l'ingérence étrangère » résoudra la rivalité interimpérialiste féroce pour les marchés, les sources de matières premières et de main-d'œuvre bon marché et les zones

d'exportation de capitaux et d'influence en faveur du Canada. Donner à la machine de guerre des impérialistes américains et à leur alliance militaire agressive de l'OTAN un contrôle absolu sur les technologies 5G et 6G résoudra-t-il les problèmes auxquels l'humanité est confrontée ou, d'autant, les problèmes fondamentaux qui affectent notre système électoral totalement non représentatif ? La réponse est non !

Selon le gouvernement libéral et les partis cartellisés à la Chambre des communes, le seul problème auquel sont confrontés notre système électoral et nos institutions démocratiques est l'ingérence d'États étrangers hostiles et d'acteurs non étatiques hostiles. Cela est considéré comme une question de sécurité nationale et, vraisemblablement, d'unité nationale également. Le problème, identifié à maintes reprises par les Canadiens, selon lequel notre système électoral – appelé démocratie représentative – et nos « institutions démocratiques » ne représentent pas les opinions de la majorité de la population, n'est pas abordé. Il n'en reste pas moins que ce système électoral est conçu pour priver le peuple du pouvoir et pour perpétuer une caste dirigeante qui paie les riches.



Les préoccupations des agences de renseignement et des forces de sécurité dominent le discours pour masquer le fait que l'État a été mis au service de la rivalité impérialiste américaine avec la Chine et que l'économie de guerre américaine convoite les grands progrès que la Chine a réalisés dans la mise en oeuvre de l'intelligence artificielle (IA) à des fins pratiques. Cela aggrave la crise dans laquelle les processus électoraux et politiques s'enlisent et ne fait rien pour créer la confiance qu'ils peuvent réaliser un mandat qui est le résultat de la participation politique des Canadiens.

La surveillance policière du discours politique à la recherche d'acteurs étrangers malveillants ne résoudra pas le problème des « fausses nouvelles » que ces acteurs étrangers sont censés générer. Impliquer la population civile et les partis politiques à collaborer à leurs activités d'espionnage ne mettra pas fin au discours et à la désinformation qui se font massivement par le biais des réseaux de communication qui se sont déjà constitués et ceux qui se mettent en place aujourd'hui.

Loin de là, pour faire croire que les « États étrangers hostiles » et les acteurs non étatiques sont le problème, les agences de renseignement elles-mêmes diffusent de « fausses nouvelles » et mènent un grand nombre d'activités perturbatrices par le biais de leurs réseaux de communication. L'exemple récent de ce que l'Inde a fait à l'échelle mondiale, y compris au Canada, en est un bon exemple. Les activités déjà révélées et celles non encore dévoilées des services de renseignement auxquelles le Canada a été intégré, qui font exactement les mêmes choses, en est un autre.

L'affirmation des agences de sécurité selon laquelle leur surveillance du discours politique ne vise pas « la défense d'une cause et la manifestation d'un désaccord légitimes » est ridicule.

On nous dit que « la défense d'une cause et la manifestation d'un désaccord légitimes font partie intégrante de la démocratie », par opposition à « l'ingérence étrangère clandestine ou trompeuse ». Mais les critères pour décider qui et quoi peut faire l'objet d'une enquête et être ciblé par les opérations de surveillance et ce qui sera considéré comme « légitime » sont tous gardés cachés au nom de la sécurité nationale ! Les enquêtes et la surveillance visent à découvrir « des menaces qui peuvent, pour des motifs raisonnables, être soupçonnées de constituer une menace pour la sécurité du Canada », nous dit-on.

En d'autres termes, les opinions et le discours politiques seront ciblés dans les opérations de surveillance pour sauvegarder la sécurité nationale. La prétention est que ce n'est pas en faisant respecter les droits que nous défendons la sécurité nationale, mais en les violant.

L'une des menaces à la sécurité nationale que les agences de renseignement ont citée dans le passé est de « discréditer les institutions libérales-démocratiques afin de faire progresser des modèles de gouvernance alternatifs ». Qu'y a-t-il de mal à faire progresser des modèles de gouvernance alternatifs ? Selon quelle définition peut-on dire que « faire progresser des modèles de gouvernance alternatifs » est une menace pour la sécurité du Canada ? Qui détermine la définition ? Par quel processus ?



Certes, la définition même de la démocratie donne au peuple le droit de décider quels modèles de gouvernance répondent à ses besoins. Comment ce droit peut-il être enlevé au peuple au nom de la sécurité nationale, en prétextant que c'est la police, et non le peuple, qui est responsable de la préservation des institutions démocratiques ? Si les agences de sécurité s'inquiètent de savoir qui constitue une menace pour nos institutions démocratiques, nous leur suggérons de tourner les yeux vers le gouvernement du parti au pouvoir et les partis cartellisés dont les actions quotidiennes

changent de facto le modèle de gouvernance démocratique issu de la rébellion contre le gouvernement par décret. Ce sont leurs manigances intéressées qui ont jeté le discrédit sur les institutions démocratiques, les partis cartellisés, le gouvernement et la Chambre des communes.

Il est inacceptable, par quelque définition ou norme que ce soit à l'exception de celles d'un État policier, que, sur la base de rapports de renseignement et de discussions avec des « représentants élus », le SCRS puisse être autorisé à prendre des « mesures raisonnables et proportionnées » pour porter atteinte au droit de s'exprimer et de s'associer. Une telle activité policière est indéfendable dans un pays qui se dit démocratique et qui prétend que c'est le peuple, et non les agences policières de l'État, qui détermine quelles opinions sont dans l'intérêt du progrès et de l'avancement du Canada, et lesquelles ne le sont pas. Accuser d'autres pays de tyrannie et de régime dictatorial, alors que ces termes ne sont pas définis d'une manière qui signifie quelque chose de rationnel dans les conditions actuelles, ne peut cacher le fait qu'on blâme les autres de ses propres fautes.

Des «évaluations des menaces» d'inspiration étrangère contre le Canada

- Pauline Easton -

Le 16 novembre, le Centre canadien pour la cybersécurité du Centre de la sécurité des télécommunications (CST) a publié une « Évaluation des cybermenaces nationales 2020 ». Pour juger de cette évaluation, il est important de connaître les critères utilisés. Or, ces critères ne sont pas expliqués ouvertement et ne sont pas soumis à la discussion. Au contraire, on doit discerner les critères soi-même et réfléchir sérieusement à quels critères serviraient les peuples lorsqu'il s'agit de discuter de la sécurité nationale. Sans fixer les points de référence qui servent les peuples et la société, les « faits saillants » du Centre pour la cybersécurité ne sont pas remis en question. En plus, ces critères sont utilisés par le gouvernement, par les partis cartellisés ayant des sièges à la Chambre des communes et les agences de l'État à tous les niveaux pour adopter des lois, criminaliser les

individus et les collectifs, et financer la production de guerre.

Le « résumé » du rapport du Centre pour la cybersécurité du CST énumère ce qu'il appelle sept « faits saillants ». On y affirme, entre autres, que des « auteurs malveillants continueront à tenter de voler la propriété intellectuelle portant sur la lutte contre la COVID-19 pour appuyer leurs programmes de santé publique nationaux ou tirer profit de la reproduction illégale de cette propriété par leurs propres sociétés ».

Comprendre pourquoi la Chine, la Russie et l'Iran auraient besoin de « voler la propriété intellectuelle portant sur la lutte contre la COVID-19 » alors qu'ils ont leurs propres intellectuels qui sont parmi les meilleurs au monde demande beaucoup d'imagination. Cela illustre le haut niveau de paranoïa que les agences de renseignement essaient de répandre. La création d'hystérie contre des pays ciblés est la même méthode qui a été utilisée dans la période récente lorsque l'hystérie contre les musulmans et l'islamophobie ont été promues et poussées au paroxysme pendant que d'autres étaient accusés de xénophobie. Tous les musulmans étaient considérés comme des terroristes ou des terroristes potentiels et des pays entiers ont été envahis et bombardés, ont été la cible d'assassinats, de torture, de la guerre des drones et de tous les crimes imaginables contre des êtres humains. On peut apprécier comment les cercles dirigeants créent de l'hystérie pour attaquer la Chine et organiser l'infiltration de groupes terroristes à la justification qu'ils donnent que ces actions défendent les Ouïghours qui sont des musulmans, en butte à l'hostilité présumée du gouvernement chinois. Pendant ce temps, les pogroms organisés par le gouvernement au pouvoir en Inde contre la population musulmane sont passés sous silence. Des arguments similaires sont utilisés pour justifier l'infiltration du Tibet et l'organisation de l'instabilité contre la Chine dans la région.



Tout cela n'est qu'une reprise de la désinformation organisée par l'État pour maintenir le corps politique dérouté, divisé et submergé afin qu'il n'établisse pas un ordre du jour qui sert ses intérêts et ceux de l'humanité. Ces évaluations hystériques de la menace semblent être conçues pour empêcher le peuple de s'attaquer à ce que les dirigeants eux-mêmes préparent. Cela comprend notamment de décider ce qui constitue une menace cybernétique, un crime et une guerre cybernétique, lesquels justifient une agression. Ces évaluations reposent sur une conception qui vise à diviser les Canadiens selon qu'ils soutiennent ou s'opposent à tout ce que les agences de sécurité disent être un danger pour la société.

Le modus operandi est bien connu. Ce climat d'hystérie est méprisable en raison de ses conséquences antisociales néfastes dues au stress, à l'anxiété et à la criminalisation accrue des gens qui sont ainsi déshumanisés et catégorisés en tant que « criminels », ou « traîtres », ou « espions », tous des termes qui laissent entendre que ces personnes méritent tout ce qui leur arrive.

En outre, plusieurs de ces cercles ont bien saisi que les rapports qui brandissent le spectre des menaces et des dangers posés par les acteurs étrangers servent à faire pression pour obtenir un financement accru des services de sécurité et de leur arsenal d'outils et de gadgets. Des dépenses massives sont consacrées à la cybersécurité qui est liée à l'industrie de la défense et de la production de guerre.

Une des méthodes utilisées, qui est moins bien comprise, est comment les services de sécurité

essaient d'engager le peuple dans des diversions. Une méthode est la demande que les entreprises de médias sociaux ne participent pas à l'espionnage cybernétique, ce qui est une demande juste. Cependant, les agences de sécurité manipulent le mouvement antiguerre pour qu'il mène des campagnes qui sont alors utilisées pour masquer le fait que les grandes sociétés de médias sociaux sont financées par le département de la guerre des États-Unis dès le moment où elles apparaissent.



Les efforts déployés par l'industrie de guerre pour contrôler l'intelligence artificielle mettent dans un état de frénésie les intérêts privés étroits mobilisés et, par conséquent, des sociétés entières, qui sont sujettes à leurs évaluations des menaces, sont-elles aussi déstabilisées. Des sommes faramineuses sont versées à l'industrie de guerre alors que les membres du corps politique sont criminalisés et que l'anxiété engendrée par des menaces potentielles devient un cri de ralliement pour l'unité nationale.

Les découvertes scientifiques appartiennent à l'humanité. Les nouveaux développements des réseaux 5G et les avancées scientifiques des scientifiques chinois en matière de cryptage quantique sont de nouvelles formes de communication de masse créées par les forces de production sociales. Ces développements ne sont la propriété de personne. C'est la plus grande signification de ces nouveaux développements dans les expériences de communications ultra-sécurisées qui sont si importantes pour le fonctionnement de tout réseau à grande vitesse. Aucune entité, qu'il s'agisse d'une nation ou d'une société, ne peut la contrôler ou la monopoliser car elle est basée sur la loi de la physique qui peut être appliquée universellement. Cela comprend les fruits de l'intelligence artificielle qui s'aventure là où la science n'a jamais même mis les pieds. La science et les découvertes scientifiques appartiennent à l'humanité. La revendication des peuples du monde est d'utiliser les produits de la révolution scientifique et technique pour le progrès de l'espèce humaine.

La jeune génération est née avec cette technologie et dans un monde où les découvertes scientifiques révolutionnent toute la compréhension de l'univers jusqu'à présent. Cette génération comprend également la majorité de ceux que l'on appelle les cyberacteurs et les cybercriminels. Ce genre de discours alarmiste ne peut justifier les dépenses consacrées à l'industrie de la guerre et à sa capacité de destruction. Les jeunes générations développeront les capacités nécessaires pour instaurer un monde de paix, de justice et de démocratie, comme elles le font déjà à bien des égards.



La nouvelle génération appartient à cette technologie et à un monde dans lequel les découvertes scientifiques sont en train de révolutionner toute la compréhension de l'univers jusqu'à maintenant. Cette génération comprend la majorité de ceux qu'on appelle les acteurs et les criminels cybernétiques. Ce genre de campagne de peur va atteindre sa limite en ce qui concerne la justification des dépenses pour l'industrie de guerre et sa capacité de destruction. Les nouvelles générations vont développer les capacités qui sont requises pour créer un monde de paix, de justice et de démocratie, comme ils le font déjà de tant de manières.

À l'encontre de tout cela, la perspective unilatérale et intéressée des dirigeants de ce que révèle

l'ensemble des relations sociales est évidente dans chacun des « faits saillants » du Centre canadien de la cybersécurité. À aucun moment les auteurs n'envisagent que la suppression du système antidémocratique de pouvoir actuel contribuera à résoudre les problèmes auxquels la société fait face. La seule préoccupation de ceux qui ont usurpé le pouvoir par la force est d'imprégner le monde entier de leur recherche insatiable de profit, croyant à tort que cela amènera les peuples à leur céder leurs richesses sans mot dire.

Tandis que les dirigeants rêvent en couleur, les peuples du monde continuent de réclamer à la société ce qui leur revient de droit du fait qu'ils sont des êtres humains. Ils continuent de lutter pour une société qui définira les droits sur cette base.

(Photos : VOR, LML)

Des évaluations de menaces fondées sur des intérêts commerciaux

- Nick Lin -

Les services secrets de l'État liés à la machine de guerre impérialiste américaine, qui font partie du réseau d'espionnage mondial appelé Groupe des cinq (Five Eyes), ont récemment publié leurs rapports annuels et « évaluations de menaces ». Les pays qui font partie du Groupe des cinq sont les États-Unis, le Canada, le Royaume-Uni, l'Australie et la Nouvelle-Zélande. L'agence privée de sécurité cybernétique, le Kaspersky Lab, qu'on dit « basée en Russie », a aussi récemment publié une évaluation.

Les pays que les impérialistes américains et leurs alliés appellent « une menace » sont en réalité des pays contre lesquels ils commettent l'ingérence et l'agression, y compris par la guerre cybernétique. Ces calculs sont d'intérêt pour le mouvement antiguerre et le mouvement pour défendre les droits de tous, puisqu'ils peuvent en tirer les conclusions qui s'imposent et trouver comment s'orienter. Il est donc important de ne pas se laisser prendre par les scénarios concoctés par les agences de renseignement pour justifier leurs plus récentes fabulations de ce qui constitue une menace étrangère ou domestique.

Ce qui est totalement absent de toutes ces évaluations de menaces par les agences officielles des États-Unis et des pays du Groupe des cinq, y compris par les intérêts privés tels que le Kaspersky Lab, ce sont les atteintes aux droits privés et politiques des citoyens de ces pays par leur propre gouvernement. Depuis la divulgation de la surveillance illégale massive des citoyens américains par l'Agence de sécurité nationale faite par le lanceur d'alerte Edward Snowden en 2013, les attaques contre les droits privés et politiques des citoyens américains et d'autres pays par le Groupe des cinq n'ont pas diminué, elles ont été institutionnalisées et ont pris de l'expansion.

Un des principaux changements à la loi américaine depuis 2013 est que les fournisseurs d'accès à Internet ont maintenant l'obligation de divulguer les métadonnées de leurs clients, avec l'institution de ce qu'on appelle une « porte de derrière » qui donne accès aux mégadonnées. De leur côté, les fournisseurs d'accès Internet avaient fait campagne contre les intrusions illégales des agences d'État et demandé d'être protégés contre l'intimidation de ces agences.

Une des raisons d'être du Groupe des cinq est précisément d'espionner leurs propres citoyens en contournant les lois de leurs propres pays. Puisque le Canada, par exemple, ne peut espionner ses propres citoyens en toute légalité, l'espionnage se fait par les États-Unis et les résultats sont ensuite « partagés ». Entretemps, des mesures sont prises pour changer les lois dans chaque pays pour permettre l'espionnage et les récriminations au nom de nobles idéaux.

Le point commun des évaluations est qu'elles ne parlent pas des pratiques beaucoup plus documentées des États-Unis, d'Israël, de la France, de la Grande-Bretagne et d'autres agences qui s'ingèrent dans les affaires politiques d'autres pays au moyen de cyberattaques et de manipulations technologiques diverses. Il y a deux poids deux mesures lorsqu'il s'agit d'« ingérence étrangère ». Par exemple, l'ingérence flagrante des États-Unis dans les élections fédérales de 2019 au Canada au moyen de potins dans les grands médias n'a pas donné lieu à une enquête sur l'ingérence étrangère.

Les faits saillants du rapport du Centre pour la cybersécurité

Les « faits saillants » du rapport du Centre pour la cybersécurité sont :

« - Le nombre d'auteurs de cybermenace est en hausse et ceux-ci deviennent de plus en plus sophistiqués. La vente commerciale d'outils liés à la cybercriminalité, à laquelle s'ajoute un bassin mondial d'experts en la matière, a entraîné une hausse du nombre d'auteurs de cybermenace et donné lieu à des attaques plus sophistiquées. Les marchés en ligne servant à la vente d'outils et de services illicites ont également permis aux cybercriminels de mener des activités plus complexes et sophistiquées.

« - La cybercriminalité est l'activité de cybermenace la plus susceptible de toucher les Canadiens et les entreprises canadiennes. Nous estimons qu'au cours des deux prochaines années, les Canadiens et les entreprises canadiennes devraient continuer d'être visés par la fraude en ligne et des tentatives de vol de données personnelles, financières et commerciales.

« - Nous considérons que les activités malveillantes dirigées contre le Canada continueront fort probablement à cibler les grandes entreprises et les fournisseurs d'infrastructures essentielles. Comme ces derniers ne peuvent pas se permettre de subir des perturbations importantes, ils sont prêts à verser jusqu'à plusieurs millions de dollars pour rétablir leurs opérations. Il est probable que beaucoup de victimes canadiennes continueront de consentir à payer les rançons en raison des coûts élevés liés aux pertes commerciales et à la reconstruction de leurs réseaux, ainsi qu'aux conséquences potentiellement dévastatrices qui pourraient résulter advenant un refus.

« - Bien que la cybercriminalité représente la menace la plus importante, les programmes parrainés par la Chine, la Russie, l'Iran et la Corée du Nord posent les plus graves menaces stratégiques pour le Canada.

« - Il est fort probable que des auteurs de cybermenace parrainés par des États cherchent à développer des moyens pour perturber les infrastructures essentielles du Canada, comme l'approvisionnement en électricité, pour atteindre leurs buts. Nous croyons toutefois qu'il est fort improbable que des auteurs de cybermenace tentent de perturber volontairement les infrastructures essentielles du Canada et de causer de sérieux dommages ou des pertes de vie s'il n'y a aucun climat d'hostilité à l'échelle internationale. Néanmoins, les auteurs de cybermenace pourraient cibler des entreprises canadiennes essentielles dans l'objectif de recueillir des données, de se prépositionner en vue d'activités ultérieures, ou de les intimider.

« - Les auteurs de cybermenace continueront probablement de mener des activités d'espionnage industriel contre les entreprises, le milieu universitaire et les gouvernements du Canada afin de voler la propriété intellectuelle et des renseignements canadiens de nature exclusive. Nous estimons que ces auteurs malveillants continueront à tenter de voler la propriété intellectuelle portant sur la lutte contre la COVID-19 pour appuyer leurs programmes de santé publique nationaux ou tirer profit de la reproduction illégale de cette propriété par leurs propres sociétés. La menace de cyberespionnage est certainement beaucoup plus grande pour les entreprises canadiennes qui font des affaires à l'étranger ou qui travaillent directement avec des sociétés détenues par des États étrangers.

« - Les campagnes d'influence étrangère en ligne sont pratique courante et ne se limitent pas à des événements politiques importants, comme des élections. Elles font maintenant partie de la nouvelle normalité, et les adversaires tentent non seulement d'influencer des événements à l'échelle nationale, mais ils veulent aussi avoir un impact sur les débats publics qui se tiennent sur la scène internationale. Nous estimons que, comparativement à d'autres pays, les Canadiens ne présentent pas une cible prioritaire en ce qui a trait à l'influence étrangère en ligne. Il faut toutefois noter qu'au Canada, l'écosystème des médias est étroitement lié à celui des États-Unis et d'autres alliés. Cela signifie que lorsque les populations de ces derniers sont ciblées, les Canadiens s'exposent à des dommages collatéraux en raison de l'influence en ligne. »

Les évaluations du Homeland Security

Le département américain du Homeland Security (DHS) a publié en octobre une évaluation de 26 pages des « menaces contre la patrie ». Les sept catégories de menaces générales sont identifiées dans la table des matières. Les citations suivantes tirées du rapport donnent un aperçu de ce que sont ces catégories.

Cybernétique : « Nous sommes préoccupés par les intentions, les capacités et les actions des États-nations tels que la Chine, la Russie, l'Iran et la Corée du nord. Le ciblage par des États-nations de nos biens a pour but de perturber l'infrastructure qui maintient notre économie américaine et représente un danger pour la sécurité nationale. En plus des menaces à l'infrastructure critique, les cybercriminels ciblent aussi nos réseaux pour voler de l'information, prendre des organisations en otage et endommager des compagnies américaines pour leur propre gain. »

Activités d'influence étrangère : « Les menaces contre nos élections sont une autre question qui évolue rapidement. Les États-nations comme la Chine, la Russie et l'Iran tenteront de se servir de leurs capacités cybernétiques ou de l'influence étrangère pour gêner ou perturber notre infrastructure liée aux élections américaines de 2020, exacerber les tensions sociales et raciales, ébranler la confiance dans les autorités américaines, et critiquer nos élus. Sans doute le plus alarmant est que nos adversaires tentent d'influencer les préférences et perceptions des électeurs américains par le biais de tactiques d'influence. »

Sécurité économique : « Le DHS est spécifiquement préoccupé par la menace directe et indirecte contre la patrie par la République populaire de Chine (RPC). La RPC dirigée par le Parti communiste de Chine (PCC) conteste le rôle de l'Amérique en tant que leader mondial et économique. Les menaces venant de la Chine incluent les dommages possibles à l'économie des États-Unis par le vol de propriété intellectuelle, la production et la distribution de produits contrefaits, et des pratiques commerciales inéquitables. Le mandat du DHS est de réduire ces menaces [...] pleinement conscient que la Chine est un compétiteur stratégique à long terme des États-Unis. »

Terrorisme : Le DHS prétend que ses préoccupations face au terrorisme sont à deux volets, l'un concernant l'extrémisme domestique violent. Il se dit « agnostique face aux menaces » tout en prétendant être « particulièrement préoccupé par les extrémistes suprémacistes blancs violents qui ont été exceptionnellement létaux dans leurs attaques ciblées abominables au cours des dernières années ».

L'autre volet est de cibler le mouvement de résistance populaire, qu'on dit une « exploitation de la prise de parole et de la contestation légales et protégées » et « de l'extrémisme antigouvernemental, anti-autorité et anarchiste violent ».

Organisations criminelles transnationales (OCT) : Le DHS dit que ces groupes « continuent de profiter aux dépens des Américains, des cartels mexicains et d'autres OCT continueront de passer clandestinement des drogues dures comme le fentanyl, l'héroïne et les méthamphétamines dans nos

communautés, contribuant au niveau alarmant de surdoses aux États-Unis. »

Immigration illégale : Le DHS prétend que « la migration illégale et de masse aux États-Unis [...] pendant la pandémie [...] constitue une menace plus spécifique aux migrants, aux communautés où ils passent, aux communautés frontalières des États-Unis, et à nos agents et policiers qui transigent avec les migrants lorsque ceux-ci entrent aux États-Unis ».

Catastrophes naturelles : Le DHS mentionne ici la menace que représentent des événements comme les tempêtes, les feux de forêt ainsi que la pandémie de la COVID-19.

Les prédictions de menaces de Kaspersky Lab pour 2021

Kaspersky Lab est une compagnie de sécurité cybernétique mondiale dont le siège social se trouve en Russie. Elle a publié ses prédictions de menaces avancées pour 2021 le 16 novembre. Un communiqué de presse de Kaspersky identifie les secteurs suivants de « menaces avancées persistantes » (APT) :

« - Les auteurs de menaces APT achèteront à d'autres cybercriminels les accès aux réseaux de leurs cibles. L'une des tendances majeures – et potentiellement la plus dangereuse – anticipées par les chercheurs de Kaspersky est un changement d'approche dans l'exécution des attaques. L'année dernière, les attaques ciblées par rançongiciels ont franchi un nouveau palier avec l'utilisation de logiciels génériques malveillants qui permettent d'intégrer des réseaux ciblés. En effet, des connexions entre ces derniers et des réseaux parallèles clandestins bien établis, tels que Genesis – au sein desquels la revente de données personnelles dérobées est monnaie courante – ont été observées. Les chercheurs de Kaspersky pensent que les auteurs de menaces APT utiliseront à l'avenir une méthode similaire pour attaquer leurs cibles. [...]

« - L'utilisation croissante des actions en justice par les États dans le cadre de leur stratégie de cybersécurité. Les précédentes prédictions formulées par Kaspersky en ce qui a trait à dénoncer et stigmatiser les attaques APT se sont confirmées, et il faut s'attendre à voir de nouvelles organisations adopter cette stratégie. L'exposition de la gamme d'outils utilisés par les groupes APT au niveau des gouvernements encouragera d'autres États à faire de même, ce qui contribuera à freiner les activités et le développement de gamme d'outils des cybercriminels.

« - Davantage d'entreprises de Silicon Valley prendront des mesures à l'égard des failles « au jour zéro ». À la suite des récents scandales ayant dévoilé, dans des applications populaires, la présence de vulnérabilités de type « au jour zéro » [des failles non connues du vendeur de logiciels lors de la date de sortie] utilisées par des organisations à des fins d'espionnage, un nombre plus important d'entreprises technologiques pourraient prendre des mesures contre les failles « au jour zéro » et les acteurs qui les exploitent afin de protéger leurs clients et leur réputation.

« - Un ciblage accru des équipements réseau. Avec l'augmentation du travail à distance, assurer la sécurité des réseaux de l'entreprise est plus que jamais prioritaire. En conséquence, Kaspersky prévoit une augmentation de l'intérêt des attaquants à cibler les appareils en réseau et les passerelles de réseau privé virtuel (VPN), ainsi que la hausse des pratiques visant à collecter les identifiants VPN des entreprises par le biais de faux salariés et de procédés de 'vishing' (hameçonnage vocal).

« - Exiger de l'argent sous menace. Des gangs opérant des rançongiciels sont devenus plus précis dans leurs attaques et ont plus souvent menacé de divulguer des données volées. Grâce à l'argent dérobé, ces groupes clandestins vont être en mesure d'investir d'importantes sommes dans l'acquisition de nouveaux outils avancés, avec des budgets comparables à ceux de groupes APT soutenus par des États. Ces changements de stratégies pourraient aussi engendrer une plus grande consolidation de l'écosystème de rançongiciels.

« - Des attaques à l'impact grandissant. Nous sommes toujours plus dépendants de la technologie et

les périmètres d'attaques ne cessent de s'agrandir. De ce fait, l'impact des attaques perpétrées sur nos sociétés et nos infrastructures – notamment nos infrastructures critiques – deviendra de plus en plus conséquent.

« L'émergence des vulnérabilités 5G. À mesure que l'adoption de la technologie 5G augmentera et que de plus en plus de dispositifs deviendront dépendants de la connectivité qu'elle offre, les attaquants seront davantage incités à rechercher les vulnérabilités qu'ils peuvent exploiter.

« - Les attaquants continueront à exploiter la pandémie de la COVID-19. Bien qu'il n'ait pas entraîné de changements dans les tactiques, les techniques et les procédures des auteurs de la menace, le virus est devenu un sujet d'intérêt constant. Comme la pandémie devrait se poursuivre jusqu'en 2021, les pirates ne cesseront pas d'exploiter ce sujet pour prendre pied dans les systèmes qu'ils ciblent. »

Les propos alarmistes au sujet de la chaîne d'approvisionnement du Canada

Peu avant que des doses du vaccin contre la COVID-19 aient été expédiées partout au pays, le Service canadien du renseignement de sécurité (SCRS) a organisé une séance d'information pour les compagnies participant à la chaîne d'approvisionnement du vaccin. Les divers reportages indiquent que le SCRS prédit de soi-disant menaces à la chaîne d'approvisionnement du Canada, par des « acteurs étrangers malveillants » qui pourraient exploiter les vulnérabilités des compagnies qui font partie de la chaîne d'approvisionnement et de leurs travailleurs.

« Le SCRS observe des activités de menace persistantes et sophistiquées parrainées par un l'État, y compris des dommages à des entreprises canadiennes individuelles, ainsi que le péage croissant sur les actifs vitaux du Canada et l'économie du savoir », a dit un porte-parole de l'agence.

« Par conséquent, le SCRS travaille en étroite collaboration avec des partenaires gouvernementaux pour veiller à ce que le plus grand nombre d'entreprises canadiennes et de différents paliers de gouvernement soient conscients de l'environnement de la menace et qu'ils disposent de l'information dont ils ont besoin pour mettre en oeuvre des mesures de sécurité préventives. »

Lorsqu'on lui a demandé de quels pays il s'agissait, le porte-parole a mentionné une séance d'information en juillet à l'intention de la Chambre de commerce du Canada où on avait mentionné la Chine et la Russie comme étant des pays engagés activement dans l'espionnage.

Dans un article du 17 décembre de CBC News, on cite différentes personnes qui se disent « analystes du renseignement » qui reprennent la campagne de peur du SCRS et donnent libre cours à leurs propres fabulations sur les « menaces à la sécurité ».

Une de ces analystes laisse entendre que la chaîne d'approvisionnement du vaccin serait « peut-être » une cible parce que les adversaires du Canada sortiraient gagnants si le Canada n'avait pas accès aux vaccins ou si sa population n'était pas entièrement vaccinée, ou pour miner la confiance dans le système de distribution. Elle suggère même qu'une faction terroriste militante opposée au vaccin pourrait tenter d'en perturber sa distribution. Elle déclare en terminant que si les agences de sécurité de l'État et la police se donnent la peine d'informer les acteurs de la chaîne d'approvisionnement, c'est que la menace doit être réelle. Elle tient ces propos même s'il est bien connu que les tactiques alarmistes, les activités occultes et terroristes organisées par l'État et effectuées par la police et les agences de la sécurité pour miner et criminaliser le mouvement du peuple et ses organisations sont chose courante.

L'ancien directeur du SCRS Ward Elcock aurait dit que le crime organisé lui-même constitue une menace. « Si vous êtes une organisation criminelle, vous pouvez gagner de l'argent avec n'importe quoi. Les gens gagnent de l'argent avec la cigarette. Ils gagnent de l'argent avec la drogue. Ce n'est pas différent de tout autre produit. » Bien sûr, les nouveaux vaccins sont instables et difficiles à transporter, car il requiert une infrastructure frigorifique spécialisée qui n'est pas accessible à tout le monde. À quoi peut servir le système de sécurité d'un pays qui sème le doute sur la capacité d'une société moderne à transporter des vaccins en toute sécurité, sauf si ce n'est de justifier une augmentation du financement et du déploiement de ce système de sécurité ?



Un participant à la séance d'information a commenté que la chaîne d'approvisionnement est « riche en données », ce qui en ferait une cible. Un porte-parole du Centre de la sécurité des télécommunications Canada (CST) a dit : « Le CST et le Centre canadien pour la cybersécurité continuent de travailler avec nos partenaires nationaux et internationaux pour soutenir la réponse du gouvernement du Canada à la pandémie du COVID-19, y compris la recherche et la distribution de vaccins. Il est toujours important de noter que nous continuons de surveiller les cybermenaces dans le cadre de notre mandat de renseignement étranger. Nous travaillons avec nos partenaires canadiens en matière de sécurité et de renseignement, y compris le ministère de la Défense nationale et les Forces armées canadiennes, pour contrer les cybermenaces envers le Canada. »

Le major général Dany Fortin, le commandant militaire responsable de la distribution des vaccins à l'Agence canadienne de la Santé publique, a dit que « je pense que le problème sous-jacent que vous soulevez ici est que nous devons nous assurer que certaines informations ne sont pas divulguées, pour des raisons évidentes. Donc, en ce qui concerne le routage exact [des expéditions du vaccin], nous préférons ne pas divulguer l'acheminement, l'emplacement exact ou les points de transfert dans la chaîne du froid pour protéger l'intégrité de la chaîne d'approvisionnement. »

Tout indique que ceux qui prétendent être responsables et conscients des « menaces à la sécurité » du Canada et de sa chaîne d'approvisionnement du vaccin font partie de la conception du monde axée sur la prémisse que tous les pays doivent se soumettre à la domination des États-Unis et que ceux qui refusent de le faire sont des menaces à la sécurité.

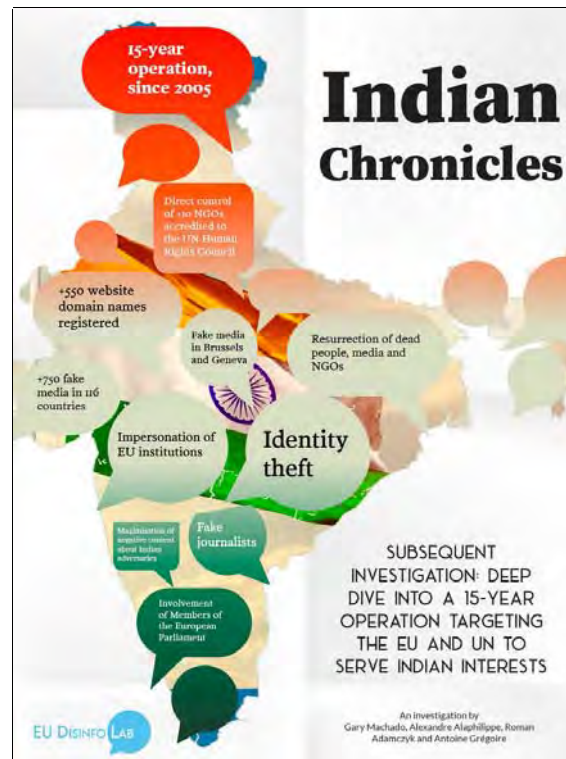
Ils visent à exploiter l'anxiété de gens face à la COVID-19 pour justifier les pouvoirs accrus des agences de sécurité de l'État au lieu d'encourager une unité de pensée en des actions à la défense des droits. Au nom de défendre le Canada contre « des acteurs étrangers malveillants », les Canadiens devraient s'appuyer sur des acteurs étrangers malveillants (par exemple, les impérialistes américains, l'OTAN, etc.), car les agences au service de ces acteurs étrangers très malveillants disent qu'on peut leur faire confiance. Cela n'a aucun sens.

Grande opération de désinformation de l'Inde

Un organisme sans but lucratif de l'Union européenne appelé EU DisinfoLab, dont la mission est de débusquer les campagnes de désinformation, a déclaré avoir mis au jour une campagne de désinformation indienne aux proportions massives et qui dure depuis 15 ans. DinsinfoLab dit que la campagne est une opération d'influence qui « cible les institutions internationales et sert les intérêts indiens ». Le rapport DinsinfoLab s'intitule « Indian Chronicles : deep dive into a 15-year operation

targeting the EU and UN to serve Indian interests » (Chroniques indiennes : un examen approfondi d'une opération de 15 ans qui vise l'UE et l'ONU pour servir les intérêts indiens). L'avant-propos du rapport dit :

« 'Chroniques indiennes – le nom que nous avons donné à cette opération – des médias disparus, des groupes de réflexion et des ONG disparus ressuscités, de même que des personnes décédées ressuscitées. Les acteurs à l'origine de cette opération ont piraté les noms d'autres personnes, ont tenté de se faire passer pour des médias et des agences de presse réguliers telles que EU Observer, *The Economist* et Voice of America, utilisé l'en-tête officiel du Parlement européen, enregistré des sites Web sous des avatars avec de faux numéros de téléphone, fourni de fausses adresses aux Nations unies, créé des maisons d'édition pour imprimer les livres des groupes de réflexion qu'ils possédaient. Ils ont organisé des événements soi-disant multipartites où, essentiellement, tout le monde qui parlait était lié aux « Chroniques indiennes ». Ils se sont appropriés de manière frauduleuse la photo d'un ancien ministre du gouvernement britannique et directeur de la BBC sur Facebook, ont enregistré les noms de personnes décédées pour qu'elles assistent à des événements cinq ans après leur mort, inventé des dizaines d'identités de journalistes. Ils ont utilisé des pages de faux médias qui se citaient et se republiaient entre eux. Ils ont utilisé des politiciens qui voulaient vraiment défendre les droits des femmes ou des minorités pour servir en fin de compte des intérêts géopolitiques et ont donné une plate-forme aux politiciens d'extrême droite lorsque des objectifs convergents pouvaient être atteints. »



La publication en ligne *The Wire* a rapporté le 10 décembre :

« En 2019, EU DisinfoLab avait publié une étude qui prétendait avoir découvert un réseau d'influence indien qui couvre '265 faux sites d'information locaux dans plus de 65 pays'.

« Cette étude a commencé comme une enquête sur une possible désinformation russe lorsque des articles publiés sur Russia Today ont été republiés sur un site Web, 'EP Today', qui a conduit les enquêteurs vers le réseau de sites et d'ONG, largement liés au groupe Srivastava basé à New Delhi.

« Cette entreprise était apparemment le principal bailleur de fonds du 'think tank' basé à Delhi, l'Institut international d'études non alignées (IINS) qui avait parrainé un groupe de membres de droite du Parlement européen (MPE) pour visiter le Cachemire en octobre 2019 – la première fois que des politiciens (y compris des Indiens) ont été autorisés à visiter l'ancien État après qu'il a été placé en confinement à la suite de la suppression de l'article 370 [de la Constitution indienne] en août de cette année.

« Dans le prolongement de son étude antérieure, le groupe dit maintenant avoir trouvé des preuves d'une opération d'influence menée par le groupe Srivastava qui a débuté il y a 15 ans de cela.

« Dans le dernier rapport d'enquête - 'Indian Chronicles', publié mercredi [9 décembre] - le DisinfoLab de l'UE affirme avoir identifié plus de 10 ONG accréditées auprès du Conseil des droits de l'homme des Nations unies (CDH), qui sont apparemment gérées par le groupe Srivastava. La plupart d'entre elles semblent avoir été de véritables ONG en déclin et dont l'identité a été 'piratée',

selon les auteurs du rapport.

« Par exemple, en mai 1938, le Comité international permanent de la conserve a été fondé pour promouvoir la 'consommation de produits en conserve' et a cessé d'exister en 2007. Cependant, le nom de domaine de l'organisation a été enregistré le 10 janvier 2016, 'le même jour comme l'enregistrement des noms de domaine d'autres ONG accréditées, et il est hébergé sur l'adresse IP avec plusieurs autres sites Web appartenant à Srivastava '.

« Accréditée auprès du CDH, l'organisation a fait des interventions orales 'pro-indiennes et anti-pakistanaïses'. Le thème central de l'ONG originale – 'conserves' – a été totalement détourné pour nuire à l'image du Pakistan au Conseil des droits de l'homme, dit le rapport.

« Une autre ONG accréditée par l'ONU à avoir une présence sur les serveurs utilisés par le groupe de Srivastava, selon le rapport, est la Commission d'étude de l'organisation de la paix (CSOP).

« Cette organisation était inactive depuis la fin des années 1970, avant d'être relancée en 2005. 'Chose choquante, nous avons découvert que l'organisation n'avait pas seulement été relancée. Son ancien président et 'grand-père du droit international aux États-Unis », Louis B. Sohn, décédé en 2006, a apparemment assisté à une réunion du Conseil des droits de l'homme des Nations unies en 2007 et a participé à un événement organisé par les 'Amis du Gilgit-Baltistan' à Washington, DC en 2011', indique le rapport.

« Ces groupes organisaient des événements parallèles au Parlement européen ou dans les bureaux de l'ONU, qui ont été utilisés pour faire venir des députés européens 'en utilisant des causes telles que les droits des minorités et les droits des femmes comme point d'entrée'. »

En outre, le rapport affirme que les « acteurs » derrière les opérations ont enregistré plus de 550 noms de domaine d'ONG, de groupes de réflexion, de médias, de groupes informels du Parlement européen, des organisations religieuses et imams, de sociétés d'édition obscures et de huit personnalités publiques.

« EU DisinfoLab prétend avoir trouvé un nouveau faux média – 'EU Chronicle' – qui est en grande partie une plate-forme pour que les eurodéputés signent des articles pro-indiens. 'En moins de 6 mois d'existence, déjà 11 députés du Parlement européen, la plupart déjà impliqués avec EP Today, ont écrit ou approuvé pour EU Chronicle des articles d'opinion à un rythme remarquablement élevé'.

« Ces articles dans EU Chronicle ont ensuite été reconditionnés par l'agence de presse ANI. 'À part *Times of Geneva* et *4 News*, qui ont arrêté leurs activités à la suite de notre enquête précédente, ANI reste la seule agence de presse à couvrir largement les activités des ONG douteuses à Genève ».

« Cette couverture médiatique, observe le rapport, visait principalement les ressortissants indiens' avec une large couverture de ces 'médias', députés européens et 'ONG' à peine connus en Europe '.

« Résumant ses conclusions, EU DisinfoLab a déclaré que son enquête examine 'les activités d'une fausse ONG zombie et celles d'un faux média spécialisé qui peuvent ensuite être reconditionnées, déformées et amplifiées par des acteurs malveillants pour influencer ou désinformer à l'échelle mondiale, en utilisant des failles dans les institutions internationales et les moteurs de recherche en ligne. »

« Les chercheurs ont précisé qu'ils savaient que les conclusions du rapport seraient utilisées par des intérêts particuliers, dans une référence aux autorités pakistanaïses. 'Gardons à l'esprit que ce n'est pas parce qu'une partie utilise des campagnes d'influence douteuses que l'autre ne le fait pas – et une simple recherche sur Google vous amènera à découvrir les comportements non authentiques qui appuient les intérêts pakistanaïses', ajoutent-ils. »

« Ce rapport, ont-ils noté, n'était pas un jugement sur la situation des droits humains au Pakistan et ne portait pas atteinte à la crédibilité des mouvements minoritaires.

« Affirmant qu'il n'existe pas de 'bonne désinformation', les auteurs ont affirmé que 'le rapport met simplement en lumière la manière dont les parties prenantes indiennes ont utilisé ces luttes pour servir leurs propres intérêts'.

« Bien que le rapport n'ait pas pointé du doigt les agences de renseignement indiennes, il a noté qu'il y avait 'plusieurs éléments suggérant la possible implication d'autres parties prenantes' dans les opérations d'influence. Ces éléments ont été identifiés dans le rapport comme étant la relation étroite entre l'ANI et le gouvernement indien, l'implication présumée d'une entreprise du groupe Srivastava dans l'offre de services de la guerre de l'information uniquement aux agences indiennes et les menaces apparentes faites à un orateur à l'ONU par un membre du groupe Srivastava, suivies d'un interrogatoire par les agences de sécurité indiennes. »

Pour le rapport au complet (en anglais), cliquer [ici](#).

(Traduit de l'anglais par LML)

Un deuxième juge bloque la tentative de Trump d'interdire une application chinoise des médias sociaux

Le 8 décembre, le juge Carl Nichols de la Cour de district des États-Unis à Washington, DC, a décidé que le département américain du Commerce « avait vraisemblablement outrepassé » ses pouvoirs d'urgence présidentiels « et a agi de façon arbitraire et non réfléchie en omettant de considérer des alternatives évidentes » face aux tentatives du président Donald Trump d'interdire TikTok, une application des médias sociaux utilisée pour partager de courtes vidéos créées par les utilisateurs. La société mère chinoise de TikTok, ByteDance, a intenté le 18 septembre un procès contre l'interdiction, plaçant que l'interdiction viole le droit à la liberté de parole et aux droits reconnus en vertu de la loi.

ByteDance a proposé que les opérations de TikTok aux États-Unis soient prises en main par des compagnies américaines. L'administration Trump avait provisoirement accepté en septembre que le géant des logiciels Oracle et Walmart investissent dans TikTok, et qu'Oracle gèrerait les données des utilisateurs. Cette entente devait être finalisée le 6 décembre. Le département américain du Trésor, qui gère l'agence responsable de cet arrangement, a dit que l'agence « participe avec ByteDance dans le parachèvement du processus de désengagement et d'autres étapes nécessaires pour surmonter les risques à la sécurité nationale liés à la transaction ».

Précédemment, le 27 septembre, un jugement du juge Nichols avait temporairement bloqué l'interdiction présidentielle. Ensuite, la juge de district des États-Unis, Wendy Beetlestone, du district est de la Pennsylvanie, s'est prononcée contre l'interdiction, le 30 octobre, lors d'un procès intenté par trois utilisateurs de TikTok s'opposant à l'interdiction présidentielle sur la base qu'elle nuisait à leur droit de parole.

Selon ByteDance, TikTok a 100 millions d'utilisateurs aux États-Unis et 700 millions à l'échelle mondiale. L'administration Trump prétend que TikTok est une menace à la sécurité, disant que le gouvernement chinois pourrait s'en servir pour espionner les données personnelles des utilisateurs. Trump a signé un arrêté présidentiel le 6 août dans le but d'interdire les transactions de TikTok aux États-Unis avant le 20 septembre à moins que la société mère chinoise ByteDance ne vende ses

opérations américaines. Cet arrêté a été suivi d'un autre le 14 août, accordant à ByteDance 90 jours pour vendre ou céder les opérations américaines de TikTok.

Les péripéties de TikTok se déroulent dans le contexte des tentatives des impérialistes américains d'isoler la Chine en ayant recours à la rhétorique de la peur et de l'anticommunisme, avec le danger que l'escalade des sanctions et des guerres commerciales n'éclatent en agression militaire ouverte. Il n'y a pas de preuves pour appuyer les accusations de l'administration Trump contre TikTok, mais les pratiques d'espionnage cybernétique ou de guerre cybernétique de longue date du gouvernement américain contre son propre peuple et ceux d'autres pays sont notoires.

Dans cette situation, les cercles dirigeants du Canada ont entraîné le pays dans les intrigues contre la Chine au service des intérêts impérialistes américains, ce qui comprend l'arrestation par la GRC de la directrice de Huawei, Meng Wanzhou, en vertu d'une demande d'extradition des États-Unis. Soulignons aussi le choix méprisable de Halifax comme endroit pour la tenue de la conférence de sécurité de Halifax, où, en grande partie, les conférenciers ont attaqué la Chine, en opposition aux souhaits des Canadiens que le Canada soit une zone de paix.

(Sources : Associated Press, Washington Post, CNBC)

(Pour voir les articles individuellement, cliquer sur le titre de l'article.)

Lisez *Le Marxiste-Léniniste*
Site web : www.pccml.ca Courriel : redaction@cpcml.ca