Câbles sous-marins de télécommunications et intérêts de puissance: les enjeux de sécurité des flux internationaux de données dans le cyberespace.

Brice Armel Simeu (UQAM)

Mai 2021

Sommaire Exécutif

Cette note politique produit une analyse sur la place saillante des câbles sous-marins intercontinentaux de télécommunications dans les rivalités de puissance au sein du cyberespace. Elle souligne l'importance des acteurs privés du numérique (*Big tech*) dans la maitrise de l'écosystème global du web. En outre, en examinant les enjeux de sécurité des infrastructures critiques d'internet, et les cyberconflictualités liées à la course au contrôle des flux internationaux de données, elle recommande au Canada et au Québec des pistes d'actions dans le cadre d'une stratégie pancanadienne et québécoise de cybersouveraineté. Enfin, elle explore les avenues d'initiatives possibles en matière de sécurité internationale pour le Canada et le Québec, face aux défis fluctuants que la globalisation numérique pose à la sécurité collective.

Introduction

En juin 2013, le programme de surveillance dénommé « PRISM » permettant au gouvernement américain via la *National Security Agency* (NSA) et le *Federal Bureau of Investigation* (FBI) de surveiller des millions d'utilisateurs d'internet était révélé par le *Washington Post*. Des portes d'entrées dissimulées dans des logiciels fabriqués par des entreprises américaines permettraient de pénétrer les serveurs des géants du web Google, Apple, Facebook et Yahoo (*Big tech*). Les services gouvernementaux américains auraient ainsi accès sans aucun contrôle, aux bases de données, aux comptes Facebook, aux boites mails et à des données de millions d'internautes à leur insu. La révélation de ce programme d'espionnage généralisé, qui faisait suite à une multitude d'affaires similaires est un indicateur d'une réalité : nous sommes pleinement entrés dans une société globale de l'intrusion, où l'interconnexion des espaces et des personnes par internet entraine l'immersion des géants du web et de leurs alliés de l'ombre dans nos espaces privés, grâce aux technologies numériques. Les câbles sous-marins intercontinentaux de télécommunications par lesquels transitent les milliards de communications quotidiennes et des mégadonnées à

l'échelle globale, constituent des infrastructures critiques dans cette société de l'information. Leur contrôle et leur surveillance sont au cœur de rivalités d'intérêts entre les puissances du cyberespace (Etats-Unis, Chine, Russie). De fait, l'ampleur de la globalisation numérique et les risques nouveaux qu'elle engendre, a transformé les flux internationaux de données en enjeux majeurs de sécurité internationale. Cette note politique explore les avenues d'actions possibles pour le Canada et le Québec face à ces problématiques aux complexités croissantes.

Le contrôle des câbles sous-marins de télécommunications : un impératif de sécurité et de souveraineté numériques

La globalisation des données avec les défis de sécurité et de régulation qu'elle soulève ne concernent pas que la captation et le contrôle des données (*Big data*) en circulation dans le cyberespace. Les infrastructures de transports des données et les « autoroutes » intercontinentales empruntées par les flux de données, constituent eux aussi des enjeux économiques et stratégiques au cœur des rivalités de puissance. Le marché de l'interconnexion et des câbles sous-marins intercontinentaux de télécommunications constitue ainsi l'un des aspects visibles du champ des affrontements économiques pour le contrôle de la gouvernance d'internet. Cependant, les États semblent en retrait ou replier derrière les acteurs privés du numérique pourtant, ils apparaissent comme les acteurs principaux des cyberconflits. Leurs souverainetés numériques semblent avoir été concédées aux firmes technologiques pour les États les plus faibles, ou « sous-traitées » par celles-ci pour les plus forts. En effet, les *Big tech* américaines Google, Facebook et Microsoft ont investi des sommes colossales pour financer la construction de leurs propres câbles sous-marins de télécommunication, avec l'appui du gouvernement américain, dans le but de limiter le contrôle des États étrangers sur leurs infrastructures critiques, et gagner en pouvoir de marché. Facebook et Microsoft ont par exemple tiré un câble de 6500 km entre l'Amérique du nord et l'Europe, offrant 169 térabytes par seconde. En termes comparatif, le câble permet de transférer 23.000 films de 7Go par seconde selon le site siecledigital.fr. A cela s'ajoute le projet 2Africa initié par Facebook, visant la construction d'un câble sous-marin de 37.000 km pour couvrir en internet haut débit 23 pays africains et du Moyen-Orient. Les investissements des géants du web dans la construction des infrastructures critiques ne se déploient pas sans interrogations. En effet, Les révélations d'Edward Snowden sur les programmes d'écoutes de la NSA ont dévoilé les rapports « incestueux » entre les services secrets américains et les infrastructures sous contrôle des *Big tech* américaines. Il prévaut une hégémonie de fait des Etats-Unis sur le marché des câbles sous-marins et autres infrastructures vitales de télécommunications. Une réalité économique et stratégique qui a poussé la

Russie à construire ses propres câbles sous-marins de télécommunication la reliant au reste du monde. Le gouvernement russe déploie ainsi ses câbles de fibre optique en passant par la Finlande, le Japon et la Géorgie, tout en apportant des aides gouvernementales en soutient à l'émergence des acteurs russes d'internet, à l'instar de la compagnie KOHTAKTE, leader russe des poses de câbles sous-marins. Le Brésil et l'Europe à la suite du scandale « Snowden » ont eux aussi décidé en février 2014 d'investir 135 millions d'euros dans le projet de construction d'un câble direct reliant l'Amérique latine à l'Europe, afin de contourner l'espionnage américain, selon les propos d'officiels brésiliens relayés par le journal *La Tribune.fr*. A l'occasion du lancement de ce projet au sommet UE-Brésil la Présidente du Brésil Dilma Rousseff affirmait :

« *Nous devons respecter la vie privée, les droits de l'homme et la souveraineté des nations. Nous ne voulons pas que les affaires et les entreprises soient espionnées. Internet est l'une des meilleurs choses que l'homme a inventé. Nous nous sommes donc mis d'accord pour garantir la neutralité du réseau, un espace démocratique où on peut protéger la liberté d'expression.* »

Les flux internationaux de données au cœur des rivalités de puissance

A la suite des américains et des russes, la Chine obsédée par le contrôle de son internet, s'est lancée dans des investissements majeurs afin d'avoir la maitrise sur les câbles sous-marins intercontinentaux de télécommunications. Ainsi, dans le cadre du volet numérique de son projet des nouvelles routes de la soie (*Belt and Road Initiative*), la Chine a financé la construction de son câble sous-marin à fibre optique SEA-ME-WE 5 avec un consortium de 20 opérateurs donc trois géants chinois des télécoms parmi lesquels Huawei. En 10 ans, Huawei c'est ainsi hissé parmi les plus imposants poseurs de câbles sous-marins de télécommunications au monde. Avec l'avènement de la 5G, le marché de l'interconnexion et des câbles de télécommunications va entrer dans une phase inédite de croissance, propulsé par le développement de l'intelligence artificielle et de l'internet des objets. La puissance des *Big tech* ne sera donc pas prête de s'amoindrir. De plus, l'accroissement de l'interopérabilité des outils et objets connectés va approfondir encore plus la transnationalisation des transactions et des échanges. L'amplification internationale du télétravail observée avec la Covid-19 en est un exemple. Les vidéoconférences, les facebook directs, Les réunions zoom entre collaborateurs dispersés dans les cinq continents, les villes intelligentes ou encore les robots intelligents au service d'une multitude de clients internationaux ne sont possibles et ne fonctionnent que du fait de l'interconnexion internet et d'un débit important de bande passante traversant les océans et accélérant la mobilité des données à l'échelle globale.

C'est un fait indiscutable que l'interconnexion des espaces économiques, le développement du commerce en réseau et l'expansion des services numériques ont été propulsés par le déploiement des câbles sous-marins intercontinentaux de télécommunications. Les réseaux de câblodistributions de la fibre optique, et les équipements de connexion internet, ont permis de connecter des territoires nationaux et des continents, d'accélérer la vitesse des communications, et d'amplifier l'échelle des échanges. Cette dimension matérielle de l'économie numérique est essentielle et constitue l'objet de cyberconflictualités et de rivalités géopolitiques particulièrement intenses. Là aussi, au-delà des intérêts de puissance des États, la volonté de contrôle des *Big tech* sur l'ensemble de la chaine de valeur du numérique s'affirme nettement. Des infrastructures et équipements critiques, aux contenus et algorithmes, en passant par les plateformes et les réseaux sociaux, les *Big tech* s'approprient les espaces de souveraineté numériques et servent de cheval de Troie aux rivalités de puissance notamment entre les Etats-Unis, la Chine et la Russie.

Conclusion

Le contrôle de l'écosystème numérique est au centre de jeux de concurrence géopolitique dans lesquels les intérêts économiques des firmes multinationales du numérique et les ambitions stratégiques des États s'imbriquent. Il faut dire que la sensibilité des enjeux de l'interconnexion et du contrôle des flux de données a été particulièrement exposée par le scandale des écoutes de la *NSA,* et notamment du programme d'espionnage américain ciblant les équipements informatiques à l'étranger et les câbles sous-marins intercontinentaux de télécommunications. De fait, à l'ère de l'interconnexion 3.0, où les hommes, les objets connectés et les machines intelligentes s'activent dans un écosystème intégré, contrôler les câbles sous-marins et les réseaux de télécommunications, c'est contrôlé non seulement les infrastructures vitales du capitalisme de l'information, et de l'économie algorithmique, mais aussi, les circuits de la mobilité des flux de données à l'échelle globale. Les acteurs privés du numérique l'ont tellement bien compris qu'ils se saisissent du marché de l'interconnexion globale et des câbles sous-marins intercontinentaux de télécommunications.

Implications et recommandations

La course au progrès en intelligence artificielle et aux mégadonnées ne doit baisser l'attention du Canada et du Québec sur la sensibilité de la question des infrastructures et des équipements matériels de connexion au reste du monde. Il est impératif que de nouveaux mécanismes de régulation et de gouvernance soient pensés à l'échelle des enjeux. Le caractère stratégique des câbles sous-marins

intercontinentaux de télécommunications exige de penser des dispositifs pour assurer leur sécurité physique face aux risques d'accidents, d'aléas climatiques ou de destruction à caractère criminel ou terroriste. Le Canada et le Québec devraient disposer d'une flotte de navires câbliers spécialement affrétée à la surveillance et la maintenance de l'intégrité des câbles dans le cadre d'opérations de contre-espionnage destinées à protéger les câbles ou les stations d'atterrissage qui sont les portes d'entrés des données sur le territoire canadien. Une autorité de surveillance de la neutralité d'internet pourrait se charger de cette mission. En effet, ces infrastructures critiques auront un rôle névralgique avec l'avènement de la 5G, et la sensibilité de ces enjeux sécuritaires nécessite de penser une stratégie pancanadienne et québécoise de cybersouveraineté. En outre, la croissance de la connectivité mondiale, exige de réfléchir rapidement aux réseaux de gouvernance transnationaux à mettre en place pour réguler et protéger l'intégrité et la neutralité des systèmes de communications internationaux. Le Canada et le Québec devraient par ailleurs prendre le leadership de la négociation d'un accord international sur la sécurité transfrontalière des réseaux et des données. Car la gouvernance des *Big data* ne se fera pas sans une gouvernance collective des réseaux globaux de télécommunications. Les dispositifs nationaux aussi puissants soient-ils ne pourront pas à eux seuls répondre efficacement à la multiplicité des risques auxquels l'interconnexion du monde est exposée.

Référence :

Cette note politique est tirée d'un travail de recherche effectué dans le cadre du volet Think Tank de l'Institut d'études internationales de Montréal (IEIM) avec pour titre : « *Enjeux de la souveraineté numérique face au pouvoir transnational des big tech : recommandations pour le Canada et le Québec* ». Publier en ligne sur https://www.ieim.uqam.ca/IMG/pdf/note_politique_ieim_-_souverainete_nume_rique.pdf