Études internationales

La route de la soie numérique, outil d'influence chinois, y compris dans l'Arctique?
The Digital Silk Road, Chinese Tool of Influence, Arctic Included?

Michael Delaunay

Volume 51, numéro 1, printemps 2020

Les politiques de l'Arctique

URI : https://id.erudit.org/iderudit/1079416ar
DOI : https://doi.org/10.7202/1079416ar

Aller au sommaire du numéro

Éditeur(s)

École supérieure d'études internationales

ISSN

1703-7891 (numérique)

Découvrir la revue

Citer cet article

Delaunay, M. (2020). La route de la soie numérique, outil d'influence chinois, y compris dans l'Arctique? *Études internationales*, *51*(1), 165–192. https://doi.org/10.7202/1079416ar

Résumé de l'article

L'Arctique n'échappe pas à l'extension du réseau physique d'Internet soutenu par les câbles sous-marins de fibre optique, dont plusieurs projets sont en cours ou réalisés. Cette possible nouvelle route des données est plus rapide et plus sûre que les routes habituelles reliant l'Amérique du Nord, l'Europe et l'Asie. La Chine, qui souhaite mettre en place une route de la soie numérique chinoise, est fortement intéressée par cette nouvelle route et pourrait y prendre pied par l'intermédiaire du projet de câble Arctic Connect. Dans un contexte de guerre commerciale et technologique entre la Chine et les États-Unis, on peut se poser des questions quant aux intentions réelles de la Chine pour ce qui est de ce projet de réseau Internet 100 % chinois. En effet, le financement et la construction par la Chine de ce genre d'infrastructure vitale pour l'économie mondiale ne sont-ils pas pour elle un moyen d'étendre son influence, dans la région mais aussi au niveau global?

La route de la soie numérique, outil d'influence chinois, y compris dans l'Arctique?

Michael DELAUNAY*

RÉSUMÉ : *L'Arctique n'échappe pas à l'extension du réseau physique d'Internet soutenu par les câbles sous-marins de fibre optique, dont plusieurs projets sont en cours ou réalisés. Cette possible nouvelle route des données est plus rapide et plus sûre que les routes habituelles reliant l'Amérique du Nord, l'Europe et l'Asie. La Chine, qui souhaite mettre en place une route de la soie numérique chinoise, est fortement intéressée par cette nouvelle route et pourrait y prendre pied par l'intermédiaire du projet de câble Arctic Connect. Dans un contexte de guerre commerciale et technologique entre la Chine et les États-Unis, on peut se poser des questions quant aux intentions réelles de la Chine pour ce qui est de ce projet de réseau Internet 100 % chinois. En effet, le financement et la construction par la Chine de ce genre d'infrastructure vitale pour l'économie mondiale ne sont-ils pas pour elle un moyen d'étendre son influence, dans la région mais aussi au niveau global?*

MOTS-CLÉS : Internet, câbles sous-marins, Arctique, Chine, route de la soie numérique

* Doctorant en Sciences politiques à l'Université de Versailles-Saint-Quentin (UVSQ) et chercheur à l'Observatoire de la Politique et la Sécurité de l'Arctique (OPSA). Nous souhaitons remercier les organisateurs de la conférence « Politiques de l'Arctique en perspectives. Approches multiscalaires et transdisciplinaires », qui s'est tenue à Sciences Po Paris les 18 et 19 décembre 2019, grâce notamment au Centre de recherches internationales (CERI) Sciences Po et au Groupe d'étude géopolitique (GEG) Nordiques et lors de laquelle ces recherches ont pu être présentées.

Abstract: *The Arctic do not elude the extension of the Internet network, supported by fibre optic submarine cables. Several submarine cable projects are in progress, or are already completed in the region. This new route promises a shorter distance, not for the containers this time, but for the transport of data between North America, Europe and Asia. China, which invests in a global Internet infrastructure, The Digital Silk Road, is very interested by this new route and could gain a foothold via the cable project Arctic Connect. In the context of a commercial and technological war between China and the United States, questions arise about the real intentions of China when it comes to this 100 % Chinese Internet network project. The financing and the construction by China of this type of infrastructure, vital for the global economy, might be a means to extend its regional and global influence.*

KEYWORDS: Internet, submarine cables, Arctic, China, Digital silk road, Huawei

Internet peut paraître lointain et surtout impalpable, mais l'infrastructure qui soutient le réseau et ses applications sont bien réelles, à tel point que l'on estime qu'Internet à lui seul consommerait entre 6 et 10 % de l'électricité produite dans le monde (Cailloce 2018). Cela est dû à la consommation d'énergie des ordinateurs, des serveurs, des centres de traitement de données (data centers), mais aussi de la transmission des paquets de données par les câbles sous-marins de fibre optique par lesquels transitent près de 99 % des données (Poole 2018), le reste voyageant via satellites et micro-ondes. Cette infrastructure sous-marine, telle une toile d'araignée (web en anglais), représente plus de 450 câbles sous-marins en service ou en projet (Telegeography 2020) dans le monde entier. Les câbles sous-marins de fibre optique, composants très discrets et essentiels de nos sociétés de l'information ultra-connectées et de plus en plus dépendantes d'Internet, sont (re) devenus d'intérêt public depuis 2015, avec les soupçons au sujet des intentions des navires et sous-marins russes qui patrouillaient à leurs abords. Pourtant, le caractère stratégique de ces câbles est loin d'être nouveau; il remonte au télégraphe, qui fut très utile pour le maintien et l'extension de l'Empire colonial britannique ainsi que pour son influence dans le monde (Headrick 1991). Ces câbles de fibre optique connectent pratiquement tous les pays de la planète et traversent presque tous les océans. Seul l'Antarctique n'est pas encore connecté par câble sous-marin de fibre optique, bien qu'un projet de câbles ait été envisagé pour connecter des bases de recherche scientifiques (*WFN Strategy* 2020; Pilot 2019). L'Arctique, quant à lui, voit des projets se concrétiser petit à petit, comme au Svalbard, au Groenland, en Alaska ou encore en Norvège. Mais ces câbles ne sont que des câbles régionaux. Faisant face à un gros problème de retour sur investissement en raison du peu de clients potentiels locaux et des conditions climatiques et géographiques difficiles, aucune grande réalisation transocéanique n'a encore vu le jour en Arctique; pourtant des projets existent et le rôle du financement par les États apparaît ici essentiel.

Il semble que dans l'Arctique nord-américain, les États-Unis et le Canada aient laissé passer plusieurs occasions d'investir, dans tous les sens du terme, cette possible nouvelle autoroute des données de l'Internet mondial, laissant d'autres puissances occuper le terrain. La Chine en effet semble fortement s'intéresser à au moins un de ces projets de câble dans l'Arctique (Arctic Connect). Cet intérêt tient au projet d'une route numérique de la soie 100 % chinoise, ce qui, pour les activités chinoises dans la région, pose évidemment la question de

l'influence chinoise, d'un possible espionnage des données, ainsi que de la souveraineté numérique et technologique pour les pays concernés. En conséquence, nous nous demanderons si le financement et la construction par la Chine de cette infrastructure stratégique, vitale pour l'économie mondiale, ne constitue pas un moyen pour elle d'étendre son influence globale tout comme l'ont fait (et continuent de le faire encore aujourd'hui) les États-Unis, grâce à leur mainmise sur le réseau physique d'Internet.

Afin de remettre en contexte cette question, nous étudierons la place stratégique qu'occupe Internet pour les entreprises et les gouvernements des grandes puissances, à travers notamment la guerre commerciale en cours entre les États-Unis et la Chine et la bataille pour la gouvernance de l'Internet mondial; puis nous verrons que la Chine place Internet au centre de ses stratégies de développement économique et de contrôle jusque dans l'Arctique; et enfin, nous nous interrogerons sur les risques que poserait un contrôle chinois sur cette nouvelle autoroute des données que représente potentiellement l'Arctique.

I – Internet, infrastructure d'importance vitale et objet d'une guerre d'influence entre États-Unis, Russie et Chine

A – Les câbles sous-marins : une infrastructure et une technologie stratégique et potentiellement vulnérable dominée par les Occidentaux

Une technologie dominée par les pays du Nord

Dans le paysage des câbles sous-marins de fibre optique, trois acteurs comptent, avec en premier lieu le Français Alcatel Submarine Networks (ASN) qui, selon les derniers chiffres vérifiés, était en 2014 leader du secteur, avec 47 % des parts de marché (Auchard 2016), pour plus de 600 000 km de câbles sous-marins posés avec 220 systèmes de câbles de fibre optique (Alcatel Submarine Networks 2020), dont un projet terminé dans l'Arctique (Quintillion) et un à venir (Eastern Arctic Undersea Fiber Optic Network – EAUFON). La deuxième entreprise la plus importante est l'américaine TE SubCom, et en troisième position la japonaise NEC.

Cette domination occidentale dans la pose et la fourniture de technologies n'est pas nouvelle; elle s'était exprimée dès les débuts du télégraphe avec l'hégémonie britannique sur cette technologie dès la

deuxième moitié du 19e siècle. Après la Deuxième Guerre mondiale, ce sont les États-Unis qui assureront cette hégémonie, sur les câbles téléphoniques puis les câbles de fibre optique (Headrick 1991). Aujourd'hui encore, l'infrastructure de l'Internet mondial suit les routes des câbles de télégraphe (même si certains projets annoncés tendent à prendre de nouvelles routes), faisant de l'Europe, l'Amérique du Nord et l'Asie des plaques tournantes (hubs) quasi incontournables de ces données.

Huawei s'allie avec Global Marine pour concurrencer les leaders occidentaux du câble

En face de ces leaders occidentaux du câble sous-marin, la Chine leur oppose Huawei Marine Networks (HMN), filiale du géant chinois des télécoms Huawei, qui a créé en 2008 une coentreprise (joint-venture) avec la société anglaise Global Marine, vestige de la domination anglaise sur les câbles sous-marins, qui a apporté au pot commun sa flotte de six câbliers, ce qui en fait la quatrième plus grosse entreprise sur le marché du câble sous-marin. HMN a posé depuis 45 câbles, pour une longueur de près de 60 000 km (Huawei Marine Networks), dont deux expériences en Arctique (Greenland Connect et Greenland Connect North). Cette coentreprise ne semble toutefois pas être encore en mesure de concurrencer ASN, TE Subcom et NEC, bien qu'elle soit présentée comme une joueuse avec qui il faudra compter dans les années à venir (Clark 2020).

Les câbles sous-marins : une infrastructure d'importance vitale, mais fragile

Bien qu'ils soient très peu connus et quasi invisibles, les câbles sous-marins de fibre optique constituent la colonne vertébrale de l'Internet mondial. Puisque Internet est devenu indispensable à quasiment toutes les activités, cela en fait une infrastructure d'importance vitale, susceptible d'être la cible d'actes malveillants – et donc une infrastructure vulnérable. En France, les entreprises comme ASN sont considérées comme des opérateurs d'importance vitale, leurs infrastructures étant définies comme stratégiques et indispensables au bon fonctionnement des activités dans le pays; elles sont donc encadrées et en partie protégées par la loi (Morel 2018). C'est certainement pour cette raison que l'État français cherche à ramener ASN dans le portefeuille d'entreprises françaises (Orange), après avoir pourtant accepté sa vente à Nokia dans un premier temps (*Les Échos - Investir* 2019).

La France n'est pas la seule à avoir adopté cette position. Les États-Unis considèrent que cette infrastructure touche à leurs intérêts vitaux; c'est pourquoi, à travers un comité interministériel appelé Team Telecom (Boulier 2014), ils se réservent le droit de refuser la réalisation d'un projet de câble sous-marin de fibre optique qui pourrait représenter un danger pour les intérêts américains, comme en 2013 (Powell 2013) et plus récemment en 2020 (Judge 2020).

Le caractère stratégique de cette infrastructure a également été mis en lumière en 2013 par les révélations d'Edward Snowden, qui ont permis de mettre au jour plusieurs programmes d'espionnage de masse, mis en œuvre par la National Security Agency (NSA), qui s'appuyaient sur les données transitant par les câbles sous-marins (Vaudano 2013) en profitant de la situation de plaque tournante des données qu'occupaient les États-Unis, de façon comparable (bien que de plus grande envergure) à la situation des Britanniques du temps du télégraphe (Headrick 1991).

Enfin, depuis 2015, consécutivement à la parution de plusieurs articles de presse alertant sur des activités douteuses de navires russes autour de ces câbles sous-marins de fibre optique (Martinage 2015; Starosielski 2015; Bridel 2015; Sanger David et Schmitt 2015), le caractère stratégique de cette infrastructure est revenu encore une fois sur le devant de la scène. À la suite de cette médiatisation et bien qu'elle soit protégée par des traités internationaux, tels que la Convention de Montego Bay, cette infrastructure vitale pour l'économie mondiale est à nouveau considérée comme vulnérable (Sunak 2017; MacAskill 2017; Morel 2016; Vuillemin 2019; Lartigue 2019; Barker 2018).

Contrôler ces technologies et cette infrastructure est donc essentiel pour les États qui veulent conserver une certaine souveraineté technologique et numérique à l'heure où l'espionnage des données est plus que répandu; de même, avoir la capacité d'influer sur le modèle de gouvernance de l'Internet mondial est un atout.

B – La bataille pour la gouvernance d'Internet : deux grands modèles s'affrontent

L'enjeu du modèle de gouvernance d'Internet

Le débat est animé autour de la gouvernance d'Internet au niveau international (Lepot 2014), alors que l'empreinte américaine reste encore aujourd'hui très forte, si l'on considère la prépondérance du

modèle de gouvernance dit *multi-stakeholder* ou multi-acteurs en français (Centre for International Governance Innovation – CIGI 2016). Ce modèle de gouvernance donne le pouvoir de décision à des acteurs privés et des organisations de contrôle et de développement de l'Internet à but non lucratif plutôt qu'aux États (Internet Society 2016). Certaines de ces organisations privées sont chargées d'établir les normes de l'Internet mondial, comme l'Internet Engineering Task Force (IETF) ou l'Internet Corporation for Assigned Names and Numbers (ICANN), créées par l'État américain et dont les sièges se trouvent encore en Californie. Bien que depuis quelques années l'influence américaine sur ces organisations se soit amoindrie, les États-Unis conservent encore une forte influence sur Internet, par l'intermédiaire notamment des grandes entreprises des nouvelles technologies que sont Google, Facebook, Apple, Microsoft et Amazon (GAFAM), ainsi que par un réseau physique majoritairement construit par des entreprises occidentales, en partie américaines. Les États-Unis ont donc plus d'influence que les autres pays sur le réseau en raison de la prépondérance de leur modèle de gouvernance (Stifel 2017), mais aussi de leurs technologies (incluant applications et logiciels) (Bloch 2017).

Cette influence américaine sur l'Internet mondial est fortement critiquée par de nombreux pays dits émergents tels que la Russie et la Chine, depuis plusieurs années (Nocetti 2015), ceux-ci accusant les États-Unis de vouloir contrôler Internet. Ces États tentent donc de promouvoir au sein des organisations internationales – dont l'Union internationale des télécommunications (UIT) – leur modèle de gouvernance dit cyber-souverain, où l'État régit le réseau, et donc son contenu, ainsi que les normes techniques découlant des technologies développées par leurs entreprises nationales. La volonté de ces pays (dont le Brésil, qui promeut lui aussi son propre modèle de gouvernance) de se départir de l'influence américaine sur Internet est très forte. La France a par ailleurs récemment elle aussi appelé à réguler Internet en proposant que sa gouvernance soit exercée, au sein des Nations Unies, par le Forum pour la gouvernance d'Internet (FGI) qui y serait intégré comme une agence de l'ONU (Loubière 2018).

Quels sont les enjeux de l'adoption de tel ou tel modèle de gouvernance?

De nombreux États considèrent qu'Internet, sa gouvernance, ses technologies, ainsi que son infrastructure touchent à leurs intérêts nationaux, les télécommunications étant une infrastructure vitale (SGDSN 2016), et cette infrastructure siégeant au cœur des économies

nationales qui en sont devenues dépendantes. Cela, les Chinois l'ont très bien compris, et c'est pour cette raison qu'ils poussent fortement à l'adoption de leur modèle d'Internet, qui pourrait faciliter l'entrée plus massive de leurs entreprises sur les marchés de fourniture des technologies soutenant le réseau physique et logiciel d'Internet. C'est notamment pour cela que Chinois et Américains se livrent une lutte d'influence à propos du contrôle de l'Internet mondial (Page *et al.* 2019).

En effet, pouvoir influer sur la gestion d'un réseau tout entier par l'imposition d'un modèle de gouvernance, de normes et de standards techniques est un atout important pour un État, car cela peut lui ouvrir des marchés potentiels pour telle technologie plutôt qu'une autre, et cela peut donc favoriser certaines entreprises nationales plutôt que d'autres, ce qui est l'enjeu central de la guerre commerciale entre les États-Unis et la Chine (Beattie 2019). Cette influence sur les normes peut également servir les intérêts de certaines agences de renseignements comme la NSA, celle-ci demandant à inclure des « portes dérobées » (backdoors) ou tout autre dispositif facilitant l'espionnage des données, comme l'a révélé l'affaire Snowden (Benhamou 2015). La présence sur leur territoire de grandes entreprises d'Internet qui détiennent un monopole ou du moins une position dominante ouvre des possibilités aux États qui, comme les États-Unis et la Chine, légifèrent pour avoir accès aux données générées.

La Chine, qui ne s'en cache pas, veut désormais être elle aussi faiseuse de normes et souhaite s'imposer dans tous les secteurs, en particulier dans les nouvelles technologies (Breznitz et Murphree 2013; Greene et Triolo 2020). En témoignent ses investissements et son avance dans la 5G par exemple. Pour la Chine, pouvoir imposer ses normes et standards dans le domaine des nouvelles technologies, et en particulier les technologies liées à Internet, constitue « une part critique des ambitions découlant de la planification d'État pour asseoir sa domination » (Beattie 2019).

C – Huawei « blacklisté » : guerre économique et technologique entre les États-Unis et la Chine

La guerre commerciale en cours entre Américains et Chinois est avant tout une guerre d'influence technologique (Bache 2019). Il semble que l'avance prise par Huawei – devenue tête de file du secteur des télécommunications, par rapport aux entreprises américaines concurrentes – dans le domaine de la 5G, fasse peur aux autorités

américaines, non seulement parce que cette technologie sera indispensable aux futures applications, notamment pour les objets connectés, mais aussi parce que cette nouvelle technologie pourrait également être un formidable outil d'espionnage des données, qui pourrait être cette fois-ci dominé par des entreprises chinoises et non américaines. Cette guerre a déjà fait une victime puisque Huawei a décidé de revendre la part de sa coentreprise Huawei Marine Networks peu après que la maison-mère se fut vu interdire d'acheter de l'équipement auprès des entreprises américaines, en raison d'accusations d'espionnage de la part de l'administration américaine (Jiang 2019). Pour faire oublier le nom de Huawei et ne plus subir d'interdictions d'achats de composants ou de pose de câble, HMN a été vendue à Hengtong Optic-Electric pour 149 millions de dollars (Clark 2020). Cette entreprise chinoise de pose de câbles va probablement devenir à terme le leader chinois des câbles de télécommunications et l'instrument privilégié du pouvoir chinois dans son projet de construction d'une infrastructure Internet chinoise d'envergure mondiale.

II – La nouvelle route de la soie et Internet comme outil d'influence pour la Chine

A – Une infrastructure Internet très disparate dans l'Arctique nord américain

Dans l'Arctique, d'une région à l'autre, les infrastructures disponibles dans le domaine d'Internet varient énormément. Les pays nordiques, par exemple, bénéficient très souvent dans leurs territoires arctiques d'une très large couverture Internet mobile en 3G et en 4G, mais aussi de câbles terrestres et sous-marins. En Russie, la situation est très différente, avec une connexion parfois disponible par satellite en dehors des grandes villes, mais en général, seules les grandes villes disposent d'une bonne connexion par câble terrestre de fibre optique. En Amérique du Nord, d'un pays à l'autre, et même d'un territoire à l'autre, la qualité de l'accès à Internet, ainsi que les technologies offertes, varient énormément en fonction des contraintes géographiques et économiques.

L'Alaska, un État de mieux en mieux connecté mais toujours dernier en vitesse de connexion

L'Alaska est connecté au réseau de télécommunications international grâce à une association de plusieurs technologies : satellite, tours à micro-ondes, câbles terrestres et sous-marins de fibre optique, ces derniers le reliant au reste des États-Unis via les États de Washington et de l'Oregon. Ici aussi, en dehors des grandes villes et de certaines communautés, l'accès à Internet peut s'avérer compliqué. De plus, un rapport de 2019 fait état d'une vitesse de connexion moyenne de 17,03 Megabits par seconde pour l'Alaska, soit la plus lente des cinquante États américains.

L'arctique canadien, un patchwork de situations

Dans le Nord canadien, les deux territoires les plus mal desservis sont le Nunavut et le Nunavik, complètement dépendants du satellite pour leur connexion, du fait d'un choix technologique remontant aux débuts du satellite dans le pays, puis d'un manque chronique d'investissements dans les infrastructures du Nord ensuite. Par ailleurs, ces territoires cumulent de nombreux obstacles qui font monter la facture et rendent les différents gouvernements rétifs à investir dans ce secteur pour autre chose que le satellite : conditions météorologiques défavorables, perturbations électromagnétiques, isolement géographique, absence de routes, coûts de construction importants, faible population qui, de plus, est éparpillée sur un territoire immense, concurrence faible, voire inexistante... Toutefois, sans financement public, Internet ne serait pas disponible dans ces deux territoires. Viennent ensuite les Territoires du Nord-Ouest (TNO) qui bénéficient de connexions dans les grandes villes et dans de nombreuses communautés situées le long des axes routiers équipés de câbles terrestres de fibre optique ainsi que d'un réseau micro-ondes et d'une connexion satellite pour les communautés les plus éloignées. Au Yukon, une seule communauté est connectée par satellite; toutes les autres bénéficient d'un accès par câble terrestre de fibre optique, ce qui en fait le territoire arctique canadien le mieux connecté.

B – La route de la soie numérique et la place centrale d'Internet dans la stratégie économique chinoise

La nouvelle route de la soie « passe par le pôle Nord »

Le projet de nouvelle route de la soie a été lancé en 2013 par la Chine afin de connecter l'économie chinoise aux économies du reste du monde et surtout à l'Europe, par la construction de tous types d'infrastructures de transport terrestre et maritime. À ce projet s'est ajouté depuis un volet polaire, la route commerciale envisagée étant le Passage du Nord-Est, mais il semble pour le moment privilégier la route maritime du nord, le long des côtes russes, pour le volet maritime, et un parcours terrestre avec des lignes ferroviaires en Finlande et en Norvège pour transporter les marchandises depuis Kirkenes jusqu'au cœur de l'Europe au moyen d'investissements chinois (Quinn 2019).

Une route de la soie numérique : satellites, 4G–5G et câbles sous-marins chinois

Ce méga-projet inclut également une route numérique de la soie soutenue par les technologies satellitaires, 4G-5G, et surtout les câbles sous-marins et terrestres de fibre optique. Ces câbles et technologies chinoises semblent emprunter de nouvelles routes délaissées par les entreprises occidentales, dans ce qu'on pourrait appeler le ventre mou, c'est-à-dire les pays en voie de développement gouvernés par des régimes autoritaires, dans lesquels la Chine construit à crédit (crédits concédés par des banques d'investissement chinoises de la route de la soie). Ces infrastructures lui permettent à la fois d'asseoir son influence dans ces pays, mais aussi de bâtir son propre réseau Internet mondial distinct du réseau occidental – et cela tout en offrant des débouchés à ses entreprises qui en ont bien besoin, étant donné que le marché intérieur chinois ne suffit plus. Cette politique permet à 89 % des projets financés par des banques d'investissement chinoises dans le cadre de cette nouvelle route de la soie d'être attribués à des entreprises chinoises (*The Economist* 2018). Il semblerait qu'au moins un tiers des pays impliqués dans les projets des routes physiques de la soie soient également engagés dans des projets de la route numérique (Kurlantzick 2020). Enfin, bien que le méga-projet de route matérielle de la soie ait été lancé en 2013, ce n'est que depuis 2015 que le pouvoir chinois privilégie de plus en plus fortement la route numérique de la soie (RDS), soutenant des projets qui se faisaient auparavant sans l'aide des autorités chinoises (Greene et Triolo 2020) et dont

les coûts en 2020 sont déjà estimés à 79 milliards de dollars (Kurlantzick 2020).

Internet, central dans la stratégie chinoise de développement économique

Cette route numérique de la soie lancée en 2015 n'est pas un volet secondaire de la route de la soie, surtout quand on regarde la place centrale qu'occupe Internet dans une Chine qui tente de maintenir sa croissance économique – en faisant passer cette économie d'une économie industrielle à une économie de services et en devenant ainsi, grâce à Internet, un « *cyber-super power* » (Segal 2018). Le 13e plan quinquennal appelle le gouvernement à utiliser Internet pour promouvoir le *soft power* chinois (Livingston 2016), poursuivant la Stratégie de mondialisation (*Go Out Policy*) mise en œuvre au début des années 2000 (Hong 2018), appelant également les entreprises chinoises des nouvelles technologies à s'étendre en dehors des frontières chinoises comme le prévoit la stratégie *Internet Plus*, et à réduire leur dépendance envers les réseaux et technologies occidentales et ainsi offrir une alternative.

C – L'intérêt chinois pour l'Arctique et le mariage de circonstance entre la Chine et la Russie

La politique arctique chinoise et la connectivité

Nous ne nous attarderons pas sur l'intérêt évident que porte la Chine depuis plusieurs années à l'Arctique, ni à ses activités dans la zone; nombreuses sont les publications sur le sujet (Huang *et al.* 2014; Lasserre *et al.* 2015; Campbell 2012; Hong 2014; Lajeunesse et Lackenbauer 2016; Kopra 2013; Chen 2012). Cet intérêt non officiellement déclaré a été formalisé par la publication par l'État chinois, en janvier 2018, de sa très attendue politique arctique. La Chine s'y définit comme « un État quasi arctique et une partie prenante importante des affaires arctiques » (*a near arctic state and an important stakeholder in Arctic affairs*). Il est à noter par ailleurs que les mots « connectivité » et « câbles sous-marins » sont cités à trois reprises chacun dans ce court document, qui souligne aussi le fait que la Chine travaille déjà à « améliorer la connectivité numérique en Arctique » (*enhancing Arctic digital connectivity*) dans le cadre de coopérations en cours, ce qui montre à quel point cette infrastructure et cette route polaire numérique sont importantes pour la Chine.

Cet intérêt pour l'installation d'infrastructures de télécommunications dans l'Arctique s'est exprimé en 2019, Huawei Canada annonçant qu'elle avait obtenu, de la part du gouvernement canadien, l'autorisation de mettre en place des équipements 4G dans 70 communautés isolées de l'Arctique canadien et du Nord du Québec, qui dépendaient du satellite pour leur connexion (Radio-Canada 2019). Et cela alors que la directrice financière du groupe Huawei, Meng Wanzhou, avait été arrêtée sur demande de la justice américaine à Vancouver en décembre 2018. Ces équipements doivent être mis en place avant 2025 (Radio-Canada 2019) en partenariat avec des opérateurs locaux (ICE Wireless et Iristel). Alors que la connexion de ces communautés est assurée uniquement par satellite et qu'elle est très limitée en capacité (Bell 2019), installer des équipements plus rapides ne sert pour le moment à rien tant que le réseau n'augmente pas ses capacités – à moins que ces équipements 4G ne soient le moyen de préparer le futur, à savoir l'arrivée de la 5G de Huawei dans une zone pour laquelle la Chine ne dissimule plus son fort intérêt et où elle souhaite acquérir toujours plus d'influence. Avec son avance technologique sur la 5G, elle serait susceptible d'y acquérir une position de monopole.

Le mariage de circonstance entre la Chine et la Russie dans l'Arctique

Bien que voulant être présente dans la zone, la Chine ne possède aucun territoire en Arctique, alors pour faire avancer son influence et ses projets, elle se repose sur un allié de circonstance : la Russie. La Russie est un géant arctique de par ses ambitions dans la zone, ses moyens et l'étendue de sa région arctique; mais c'est un géant qui manque de financements pour développer cette région où reposent les ressources absolument indispensables à son économie. De son côté, la Chine dispose de moyens financiers dont la Russie est dépourvue, et elle veut peser dans la gouvernance de l'Arctique, région sur laquelle elle mise beaucoup dans le cadre des nouvelles routes de la soie pour en faire une nouvelle zone d'extraction de ressources, mais aussi une route de transport de marchandises et de données numériques. Ce serait une coopération gagnant-gagnant (win win), comme disent les Chinois, pour le moment.

Par ailleurs, il est à noter que dans le domaine d'Internet, il existe une certaine convergence de vues entre la Russie et la Chine, qui ont en commun un modèle de gouvernance d'Internet « cyber souverain » très similaire, ainsi qu'une infrastructure de contrôle du contenu d'Internet et la possibilité de couper leur Internet du reste de l'Internet

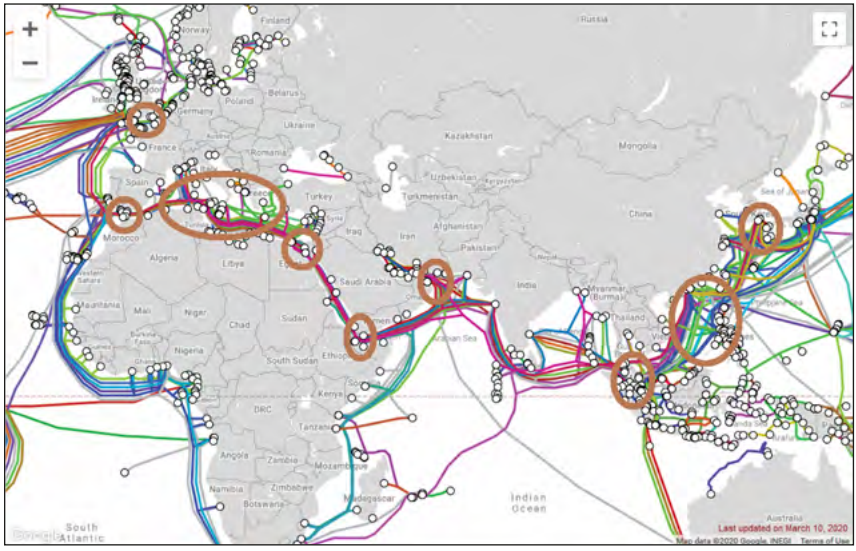
mondial. Les deux pays disposent également de tout un écosystème d'entreprises semblables aux GAFAM américaines qui leur permet de se dégager de l'influence occidentale et de promouvoir ainsi leur modèle de gouvernance comme une alternative. Ces deux pays ont la possibilité de créer un Internet distinct de celui qui est dominé par la gouvernance, les normes et les standards et technologies occidentales en général, et américaines en particulier.

III – L'Arctique, future autoroute des données chinoises?

A – L'Arctique : une nouvelle route de données

Pourquoi passer par l'Arctique?

Carte nº 1 : Les goulots d'étranglement de l'Internet mondial



Source : Telegeography

Avant d'aller plus loin, demandons-nous pourquoi vouloir passer par l'océan Arctique, alors que celui-ci reste difficile d'accès et que les routes actuelles de câbles sous-marins sont éprouvées depuis l'avènement du télégraphe dans la deuxième moitié du 19e siècle? Il suffit pour cela de regarder une carte actuelle des câbles sous-marins de fibre optique pour comprendre que les routes de l'Europe à l'Asie ne sont pas sans danger. Elles passent obligatoirement par les goulots

d'étranglement et les zones d'activités maritimes très denses que sont le détroit de Gibraltar, la mer Méditerranée, le canal de Suez ou encore les détroits de Bab-el-Mandeb, de Malacca et ceux de la mer de Chine. Cette carte nous montre que ces zones sont dangereuses pour les câbles (qui y sont nombreux) du fait du goulot d'étranglement qu'elles représentent, mais également parce que ce sont parfois des zones instables politiquement. De plus, la concentration des activités maritimes dans ces zones est la menace la plus importante pour ces câbles sous-marins, étant donné que les premières causes de ruptures ou de dommages faits aux câbles sont la pêche au chalut et les ancres des navires (Kordahi *et al.* 2014), et non pas les morsures des requins ou les vols de câbles, qui sont extrêmement rares.

Plusieurs projets ratés de pose de câbles

Comparativement à ces zones à risque que nous venons d'évoquer, l'Arctique, qui commence à s'ouvrir du fait du réchauffement climatique, offre une route plus courte, avec très peu d'activités maritimes et donc peu de risques d'endommagement ou de rupture des câbles, tout en présentant également une situation politique stable. Depuis 2000, plusieurs projets de câbles sous-marins de fibre optique passant à travers les passages arctiques ont été annoncés. Ce fut d'abord le projet russe ROTACS (Russian Optical Trans-Arctic Submarine Cable System) estimé à 1,9 milliard de dollars et qui devait connecter tout l'Arctique russe via le Passage du Nord-Est (PNE) en partenariat avec l'entreprise russe Transneft (Delaunay 2014). Bien que soutenu par l'État russe, ce projet ne vit jamais le jour, faute de financement. Il y eut aussi le projet américain Arctic Link, et le projet canadien Arctic Fibre, qui devaient tous deux relier l'Asie à l'Europe via le Passage du Nord-Ouest (PNO). Les deux projets n'ont jamais vu le jour, n'ayant pas réussi à obtenir assez de financements.

B – Des projets de pose de câbles fortement dépendants des financements publics

Les projets de câbles en cours

Malgré ces échecs, d'autres projets sont encore en cours en dépit des fortes contraintes imposées par les régions arctiques. C'est d'abord Arctic Connect qui depuis 2016 reprend en partie le principe de ROTACS, voulant connecter par un câble sous-marin de fibre optique long de 10 500 km, l'Europe du Nord au Japon et à la Chine, mais aussi à l'Alaska via le Passage du Nord-Est (PNE) pour un coût évalué

entre 700 millions et un milliard d'euros (Submarine Cable Networks 2020). Il est porté par la Finlande, avec l'entreprise Cinia, détenue à 70 % par l'État finlandais. Ce projet fait suite à un rapport de l'ancien premier ministre Paavo Lipponen sur la question et lancé sur proposition du ministère des Transports finlandais. Les pays d'Europe du Nord – Finlande, Suède et Norvège en tête (Nilsen 2016) – veulent devenir une plaque tournante de données et ils sont donc très impliqués dans ce projet.

Ce projet civil a un pendant militaire en Russie (Staalesen 2019), qui semble toutefois à l'arrêt, depuis que les deux brise-glaces poseurs de câbles prévus pour ce projet sont laissés à l'abandon en cale sèche dans leur chantier naval ukrainien. Ce câble doit relier toutes les bases militaires datant de la guerre froide en cours de réoccupation et de modernisation par l'armée russe, et créer ainsi un intranet militaire russe dans l'Arctique.

L'autre grand projet est celui de Quintillion, entreprise américaine qui a racheté le projet canadien Arctic Fibre et qui a posé un premier segment de câble en 2017 avec ASN le long de la côte de l'Alaska pour 270 millions de dollars, connectant ainsi cinq villages et la zone pétrolifère de Prudhoe Bay.

Dans l'Arctique canadien trois projets sont en cours. D'abord celui du gouvernement du Nunavut qui doit connecter seulement trois communautés (Iqaluit, Cape Dorset et Kimmirut) pour 209 millions de dollars canadiens, depuis Nuuk au Groenland (Brown 2020); le projet de l'administration du Nunavik, EAUFON, dont la première phase doit connecter cinq communautés pour 125 millions de dollars et dont le contrat a été attribué à ASN (Submarine Telecoms Forum 2020); et enfin le projet SednaLink de la société canadienne CanArctic Inuit Networks qui, pour 107 millions de dollars, prévoit de connecter Iqaluit à Internet via Terre-Neuve et le Labrador (Tranter Emma 2020).

Des projets impossibles à réaliser sans l'aide des États dans l'Arctique

À part Arctic Connect qui semble avoir trouvé des financements privés, les projets dans l'Arctique n'ont pu et ne semblent pas pouvoir se concrétiser sans financement public Seule exception à cette règle confirmée à ce jour, Quintillion. Elle est pour le moment la seule entreprise à avoir réussi à poser un câble sans financement public, cela, toutefois, en mentant à ses investisseurs sur les bénéfices escomptés (Cooper Investment Partner et Natixis) pour les amener à investir à

hauteur de 270 millions de dollars (Carr 2019). L'ancienne PDG, Elizabeth Pierce, a d'ailleurs été reconnue coupable de fraude par un tribunal de Manhattan et a été emprisonnée en juin 2019 pour cinq ans, pour avoir promis un retour sur investissement surévalué d'un milliard de dollars sur 25 ans et pour avoir falsifié des documents (Warwick 2019).

Cet épisode montre bien que la question du financement de ces projets dans l'Arctique est centrale et que les États ont un rôle considérable à jouer pour leur permettre de voir le jour, que ce soit à travers le financement et/ou l'impulsion politique (qui est très forte du côté du projet Arctic Connect par exemple), le retour sur investissement pour les entreprises privées étant quasi nul pour des projets qui ne desserviraient que la région arctique. Dans un tel cas, les anglophones utilisent l'expression *no business case* : les opportunités d'investissement permettant de gagner de l'argent pour les entreprises privées sont absentes, et les sommes à investir sont bien trop élevées comparativement au retour sur investissement possible. Les projets transarctiques ont quant à eux plus de perspectives de retour sur investissement, mais ils exigent des sommes de départ importantes. Jusque-là, les marchés américains, européens et asiatiques se sont montrés très frileux à l'idée d'investir dans ces projets, qui sont pourtant utiles pour la connectivité mondiale et la rapidité de transmission des données. Alors, sans aides publiques et sans le soutien des États qui pourraient faire en sorte que ces infrastructures restent aux mains d'entreprises nationales, ces projets ne verront pas le jour ou seront financés par d'autres pays, comme peut-être la Chine.

C – La Chine, futur investisseur de cette nouvelle route des données?

Les pays concernés par le projet de câble Arctic Connect, la Norvège, la Finlande, la Russie le Japon et la Chine, ont été associés au projet depuis au moins mars 2017 (Saunavaara 2018). Notamment la Chine, avec qui la Finlande a eu des discussions au niveau ministériel, lors desquelles les officiels chinois ont été décrits comme extrêmement intéressés (Murdoch-Gibson 2018), tout comme certaines entreprises chinoises qui se sont dites ouvertes à une coopération de type gagnant-gagnant, notamment China Telecom (Suokas 2017). Cet intérêt chinois pour le projet de câble Arctic Connect se manifeste également par l'attention que lui porte la presse chinoise qui suit de près les avancées du projet (Xinhua 2019b).

Certains experts ont même déclaré que Cinia et China Telecom seraient les deux principales entreprises derrière le projet Arctic Connect (Buchanan 2018), et que la Chine souhaite en être un partenaire majeur (Shi 2017; Burkitt-Gray 2018; Pearce 2017; *The Arctic* 2017; Xinhua 2019a) sur les plans politiques, techniques et financiers. Par ailleurs, un conseiller de Cinia a annoncé qu'il serait possible que ce projet soit financé par les banques d'investissement chinoises qui soutiennent les projets des nouvelles routes de la soie (Murdoch-Gibson 2018).

Mais ces prêts chinois, au-delà des taux d'intérêt, ne sont pas « gratuits » comme nous l'avons vu plus haut, la majorité des projets financés par la Chine dans le cadre des nouvelles routes de la soie étant attribuée à des entreprises chinoises telles que Huawei ou China Telecom. Il se pourrait donc que Huawei puis Hengtong puissent elles aussi entrer dans ce projet – sachant qu'en plus Cinia et Huawei ont déjà travaillé ensemble sur le premier câble de l'entreprise finlandaise, le C-lion, posé en 2016, en vendant des équipements pour ce câble ainsi que des équipements pour connecter des fermes de serveurs entre l'Europe et l'Asie (Huawei 2016).

De plus, les liens bilatéraux entre la Finlande et la Chine se sont renforcés ces dernières années avec la visite en avril 2017 de Xi Jinping (une première depuis 1995), ainsi que l'ouverture d'une ligne de transport ferroviaire entre Kouvola (Finlande), Xi'an et Zhengzhou (centre de la Chine) et une augmentation des investissements chinois dans le pays.

D – Quels risques que la Chine investisse dans les télécommunications dans l'Arctique?

Alors qu'une bataille pour la gouvernance de l'Internet mondial et l'imposition d'une nouvelle architecture et des technologies, normes et standards qui vont avec, fait rage entre les grandes puissances sur la scène internationale, l'Arctique pourrait devenir une nouvelle autoroute des données dans un avenir proche et ainsi peser dans ce rapport de force. La volonté clairement affichée de la Chine de devenir une cyber superpuissance, notamment en proposant une alternative au modèle d'Internet occidental, pourrait donc bénéficier d'un investissement majeur dans cette potentielle nouvelle route des données qui passe par l'Arctique, tout en représentant des risques pour d'autres.

Un investissement chinois dans l'Arctique qui pourrait avoir des effets bien au-delà de la région

En investissant dans le projet Arctic Connect et en imposant ses entreprises et ses technologies sur un projet visant à connecter la majeure partie des internautes de la planète, faisant d'Arctic Connect un projet structurant pour l'Internet mondial, la Chine mettrait en valeur sa proposition d'un nouveau modèle de gouvernance et d'architecture de l'Internet dit « cyber souverain ». Mais il s'agit d'un modèle de gouvernance beaucoup moins ouvert et plus autoritaire, où l'État est capable de contrôler jusqu'au contenu d'Internet, et cela ne pourrait qu'aller à l'encontre des libertés des utilisateurs, comme c'est déjà le cas en Chine qui est en train de construire une société de surveillance (avec le système de crédit social, par exemple).

Par ailleurs, en étendant son réseau au-delà de ses frontières, la Chine pourrait avoir accès, comme les États-Unis aujourd'hui, à un flux de données important et avoir ainsi la possibilité (comme ses lois le lui permettent) d'espionner ces données à son profit.

Enfin, le risque de voir naître un Internet parallèle à l'Internet mondial n'est pas à exclure. Avec la « route numérique de la soie », la Chine impose déjà son modèle d'Internet dans les pays de la route de la soie par des infrastructures Internet installées par des entreprises chinoises dans des pays autoritaires, ce qui donne les moyens à ces derniers d'installer un Internet de surveillance chinois. Plusieurs pays le long de la route de la soie ont déjà été séduits par les technologies et applications de surveillance chinoises. C'est le cas par exemple de l'Égypte, qui a adopté en 2018 une loi sur les crimes cyber proche de la législation chinoise, qui lui donne le droit de censurer le contenu sur Internet, tandis que d'autres pays utilisent les technologies de surveillance de Huawei (Kurlantzick 2020).

Le projet Arctic Connect qui bénéficiera à la Chine mais aussi à la Russie, qui a la même conception de la gouvernance d'Internet, ne pourrait que renforcer leur position dans les organisations internationales en faveur de leur modèle de gouvernance en connectant ainsi de plus en plus d'internautes.

Quels risques pour le Canada?

Le risque d'une plus grande influence chinoise sur cette infrastructure d'importance vitale de manière globale existe donc. Mais il existe également dans la région arctique. Le Canada, lui, n'investit que dans des petits bouts de câble, sans vision globale du réseau et sans réelle

stratégie de connectivité (Bureau du vérificateur général du Canada 2018). Cette politique laisse le champ libre à d'autres acteurs étatiques qui réfléchissent à plus long terme, comme la Chine, et qui ont une stratégie affirmée d'influence sur les nouvelles technologies, dont Internet. Cela ouvre donc la possibilité pour d'autres acteurs de financer, installer puis contrôler cette nouvelle route des données – comme Huawei, qui investit dans l'Arctique canadien, avec le risque d'une situation de monopole si la Chine est la seule à investir dans des projets structurants tels qu'Arctic Connect ou la 4G et la 5G. Cette situation dominante, voire de monopole, par défaut d'investissements occidentaux dans la région, pourrait selon certains être utilisée dans le cas d'une (hypothétique) crise géopolitique entre la Chine et le Canada dans la zone (Levinson-King 2019). De ce fait, certains observateurs canadiens alertent sur les risques liés aux investissements chinois dans l'Arctique canadien (Luedi 2020; Blanchfield 2019; Levinson-King 2019). Mais il faut néanmoins considérer que les entreprises qui investissent dans le Nord canadien dans le domaine des télécommunications ne sont pas légion, car cela est peu rentable. Par ailleurs, Huawei est déjà présente dans le Nord canadien puisqu'elle a fourni des équipements 3G dans les trois territoires arctiques canadiens en 2013 (Capacity Media 2012). Évincer Huawei de l'Arctique canadien pourrait avoir comme conséquence de retarder encore la mise à niveau du service (très insatisfaisant) offert aux habitants du Nord (Luedi 2020). L'équation n'est donc pas si simple.

Quelle réponse des États-Unis?

Les États-Unis considèrent qu'Internet et son infrastructure font partie de leurs intérêts vitaux. Aussi, laisser la Chine peser sur la gouvernance mondiale d'Internet et imposer ses technologies leur ferait possiblement perdre leur position dominante.

Depuis peu, on constate à travers des programmes militaires un début de réponse à la politique chinoise. L'Armée de l'air et la Force de l'espace américaine ont, en 2020, élaboré une stratégie arctique dont l'un des quatre piliers est la connectivité. En conséquence, des financements ont été débloqués pour soutenir de nouvelles alternatives afin d'améliorer la connectivité des Forces armées américaines en Arctique à travers la technologie LEO, et peut-être dans le futur à travers la fibre optique. En effet, Quintillion a publié une nouvelle route de son câble (Quintillion 2020), montrant un nouveau segment de câble allant connecter la base américaine de Thulé au Groenland, tandis que dans le même temps, elle embauchait d'anciens militaires

américains. De plus, Quintillion axe depuis peu sa communication en grande partie sur l'aspect sécuritaire de son projet de câble, ce qui est inédit et qui pourrait laisser présager un financement du gouvernement fédéral pour la suite de son projet (Delaunay 2020).

Conclusion

Il semble donc bien que la Chine se positionne fortement sur le secteur de la connectivité dans la région et dans le monde et qu'elle voie l'Arctique comme une possible route stratégique, aussi bien pour ses porte-conteneurs que pour les données. La Chine agit sur le long terme, une temporalité qui fait défaut aux autres pays, comme le Canada ou les États-Unis, et qui pourrait leur faire perdre de vue l'importance de participer au financement de ces infrastructures qui durent 25 ans et ainsi les garder entre les mains d'intérêts nationaux, au lieu de les laisser financer et manufacturer par des intérêts étrangers et notamment chinois. Le problème est que ces infrastructures sont bien trop coûteuses dans l'Arctique pour les seuls investisseurs privés; l'apport de capitaux publics est donc indispensable à la réalisation de ces infrastructures. Sans engagement clair et massif des gouvernements pour financer au moins en partie ces infrastructures stratégiques, il est fortement probable qu'aucun projet ne pourra aller de l'avant dans l'Arctique dans le domaine de la connectivité. Par l'investissement massif dans l'infrastructure Internet, la Chine pourrait acquérir plus de poids et d'influence, ce qui lui permettrait à terme de tenter d'imposer son modèle de gouvernance, ses technologies et ses standards Internet, opposés à ceux des pays occidentaux et en premier lieu à ceux des États-Unis. Une guerre d'influence se joue actuellement entre les différents modèles, normes et standards américains et occidentaux, d'une part, et ceux de la Chine, d'autre part. Si bien que laisser la Chine investir seule dans des projets structurants tels qu'Arctic Connect reviendrait à lui laisser plus d'influence sur l'Internet mondial.

Pouvoir financer et contribuer à la construction d'un système tel qu'Arctic Connect, qui pourrait ouvrir une nouvelle autoroute d'Internet, complètement distincte des routes traditionnelles empruntées depuis le télégraphe, serait un atout précieux pour la Chine dans sa quête d'influence dans l'Arctique et sur l'Internet mondial. La Chine utilise clairement le financement d'infrastructures à travers le monde, et notamment dans les pays en voie de développement, comme un outil de *soft power*, afin d'étendre son influence (Hillman 2019). De

plus, de nombreuses questions se posent sur la sécurité des données et les possibilités d'espionnage par les services de renseignements chinois. Il se pourrait que le financement et la fourniture de technologies pour le câble Arctic Connect puisse être une brique importante dans la construction d'une infrastructure Internet dénuée d'influence américaine, au profit des pays impliqués et notamment la Chine. Il se peut qu'à l'avenir l'Arctique devienne la nouvelle autoroute de l'Internet mondial, et une route concurrente au réseau dominé par les États-Unis et plus largement, par les Occidentaux. L'enjeu pour le futur de l'Internet mondial pourrait donc se jouer en partie sous les glaces de l'Arctique, sans les États-Unis et le Canada, qui refusent de financer des infrastructures pourtant vitales et touchant à leurs intérêts nationaux, laissant ainsi le champ libre à d'autres pays, comme la Chine, pour ouvrir et contrôler cette nouvelle route des données.

Michael Delaunay
Université de Versailles-Saint-Quentin-en-Yvelines,
France

michaeldelaunay10@gmail.com

Bibliographie

Alcatel Submarine Networks, 2020, *At a Glance*. Consulté sur Internet (https://web.asn.com/en/about-asn/who-we-are/) le 15 mars 2020.

Auchard, Eric, 2016, « Nokia Sets New Record for Submarine Cable Capacity as Demand Jumps. » *Reuters.* Consulté sur Internet (https://www.reuters.com/article/us-nokia-submarine/nokia-sets-new-record-for-submarine-cable-capacity-as-demand-jumps-idUSKCN12C0M9) le 10 septembre 2019.

Bache David, 2019, « Chine-États-Unis : guerre commerciale, technologique et stratégique », *RFI*. Consulté sur Internet (http://www.rfi.fr/economie/20190510-etats-unis-chine-commerce-guerre-nouvelles-technologies-espionnage-industrie) le 10 juin 2019.

Barker Pete, 2018, « The Challenge of Defending Subsea Cables », *The Maritime Executive*. Consulté sur Internet (https://www.maritime-executive.com/editorials/the-challenge-of-defending-subsea-cables) le 25 février 2020.

Beattie Alan, 2019, « Technology: How the US, EU and China Compete to Set Industry Standards », *Financial Times*. Consulté sur Internet (https://www.ft.com/content/0c91b884-92bb-11e9-aea1-2b1d33ac3271) 16 février 2020.

Bell Jim, 2019, « The Connected Territory? Nunavut Still Waits », *Nunatsiaq*. Consulté sur Internet (https://nunatsiaq.com/stories/article/the-connected-territory-nunavut-still-waits/) le 15 avril 2019.

Benhamou Bernard, 2015, « La gouvernance mondiale de l'Internet après Snowden », *Hommes & Libertés*, septembre, n° 17 : 50-53. Consulté sur Internet (https://www.ldh-france.org/wp-content/uploads/2015/10/HL171-Dossier-9.-La-gouvernance-mondiale-de-lInternet-apr%c3%a8s-Snowden.pdf) le 12 février 2020.

BLANCHFIELD Mike, 2019, « Huawei déploiera un service Internet dans l'Arctique », *Le Devoir*, 23 juillet. Consulté sur Internet (https://www.ledevoir.com/economie/559231/huawei-deploiera-les-services-4g-dans-le-grand-nord-canadien) le 23 juillet 2019.

BLOCH Laurent, 2017, *Internet, vecteur de puissance. Géopolitique du cyberespace, nouvel espace stratégique*, Paris, Diploweb.

BOULIER Dominique, 2014, « Internet est maritime : les enjeux des câbles sous-marins », *Revue internationale et stratégique*, n° 95 : 149-158. Consulté sur Internet (https://www.cairn.info/revue-internationale-et-strategique-2014-3-page-149.htm) le 1er février 2020.

BREZNITZ Dan et Michael MURPHREE, 2013, *The Rise of China in Technology Standards: New Norms in Old Institutions*, Rapport de recherche, US-China Economic and Security Review Commission. Consulté sur Internet (https://www.uscc.gov/sites/default/files/Research/RiseofChinainTechnologyStandards.pdf) le 24 février 2020.

BRIDEL Bernard, 2015, « Moscou s'intéresse de très près aux câbles sous-marins et à leurs données », *Tribune de Genève*. Consulté sur Internet (https://www.tdg.ch/monde/moscou-s-interesse-tres-cbles-sousmarins-donnees/story/25004822) le 24 février 2020.

BROWN Beth, 2019, « MLAs Shocked at $80 Million Cost Increase to Nunavut-Greenland Fibre Cable », *CBC News*. Consulté sur Internet (https://www.cbc.ca/news/canada/north/nunavut-fibre-link-cost-1.5334784) le 12 janvier 2021.

BUCHANAN Elizabeth, 2018, « Sea Cables in a Thawing Arctic », *The Lowy Institute*. Consulté sur Internet (https://www.lowyinstitute.org/the-interpreter/sea-cables-thawing-arctic) le 15 mars 2018.

BUREAU DU VÉRIFICATEUR GÉNÉRAL DU CANADA, 2018, « La connectivité des régions rurales et éloignées », Rapport 1, automne, Bureau du vérificateur général du Canada. Consulté sur Internet (https://www.oag-bvg.gc.ca/internet/Francais/parl_oag_201811_01_f_43199.html) le 11 décembre 2019.

BURKITT-GRAY Alan, 2018, « €700m Arctic Cable "to Get Backing" to Speed Asia-Europe Links », *Capacity Media.* Consulté sur Internet (https://www.capacitymedia.com/articles/3814531/EXCLUSIVE-700m-Arctic-cable-to-get-backing-next-week-to-speed-Asia-Europe-links) le 7 juin 2019.

CAMPBELL Caitlin, 2012, « China and the Arctic: Objectives and Obstacles », US-*China Economic and Security Review Commission*, Staff Research Report. Consulté sur Internet (https://uscc-dev.usa-ctc.com/sites/default/files/Research/China-and-the-Arctic_Apr2012.pdf) le 4 juin 2019.

CAILLOCE Laure, 2018, « Numérique : le grand gâchis énergétique », dans *CNRS- Le Journal*. Consulté sur Internet (https://lejournal.cnrs.fr/articles/numerique-le-grand-gachis-energetique) le 6 décembre 2019.

CAPACITY MEDIA, 2012, « Ice Wireless and Iristel Partner with Huawei for 3G Deployment in North West Canada », *Capacity Media*. Consulté sur Internet (https://www.capacitymedia.com/articles/3092625/Ice-Wireless-and-Iristel-partner-with-Huawei-for-3G-deployment-in-North-West-Canada) le 9 mars 2020.

CARR Austin, 2019, « The Billion-Dollar High-Speed Internet Scam », *Bloomberg*. Consulté sur Internet (https://www.bloomberg.com/news/features/2019-10-08/quintillion-ceo-s-promise-to-wire-the-arctic-was-1-billion-scam) le 8 octobre 2019.

CHEN Gang, 2012, « China's emerging Arctic strategy », *The Polar Journal*, vol. 2, no 2 : 358-371. Consulté sur Internet (https://www.tandfonline.com/doi/abs/10.1080/2154896X.2012.735039) le 15 janvier 2020.

CIGI, 2016, *Who Runs the Internet? The Global Multi-Stakeholder Model of Internet Governance*, Centre for International Governance Innovation and the Royal Institute of International Affairs, décembre. Consulté sur Internet (https://www.cigionline.org/sites/default/files/documents/GCIG%20Volume%202.pdf) le 12 février 2020.

CLARK Robert, 2020, « Hengtong Set to Shape the Global Subsea Market », *LightReading*. Consulté sur Internet (https://www.lightreading.com/hengtong-set-to-shape-the-global-subsea-market-/d/d-id/757055) le 25 janvier 2020.

DELAUNAY Michael, 2014, « The Arctic: A New Internet Highway? », dans Lassi HEININEN, Heather EXNER-PIROT et Joël PLOUFFE, *Arctic Yearbook 2014*, Northern Research Forum. Consulté sur Internet (https://arcticyearbook.com/images/yearbook/2014/Briefing_Notes/2.Delaunay.pdf) le 15 février 2020.

DELAUNAY Michael, 2020, « Internet, plus que jamais vital dans l'Arctique en 2020 », *L'année arctique 2020. Revue annuelle*, Observatoire de la Politique et la Sécurité de l'Arctique (OPSA). Consulté sur Internet (https://cirricq.org/wp-content/uploads/2020/12/Connectivite.pdf) le 10 janvier 2021.

GREENE Robert et Paul TRIOLO, 2020, « Will China Control the Global Internet Via its Digital Silk Road? » *Carnegie*. Consulté sur Internet (https://carnegieendowment.org/2020/05/08/will-china-control-global-internet-via-its-digital-silk-road-pub-81857) le 12 janvier 2021.

HEADRICK Daniel, 1991, *The Invisible Weapon. Telecommunications and International Politics 1851-1945*, Oxford, Oxford University Press.

HILLMAN Jonathan E., 2019, *Influence and Infrastructure: The Strategic Stakes of Foreign Projects*, Rapport, Center for Strategic and International Studies, Reconnecting Asia Project. Consulté sur Internet (https://csis-prod.s3.amazonaws.com/s3fs-public/publication/190123_Hillman_InfluenceandInfrastructure_WEB_v3.pdf) le 17 septembre 2019.

HONG Nong, 2014, « Emerging Interests of Non-Arctic Countries in the Arctic: a Chinese Perspective », *The Polar Journal*, vol. 4, nº 2 : 271-286. Consulté sur Internet (https://www.tandfonline.com/doi/abs/10.1080/2154896X.2014.954888) le 15 novembre 2019.

HONG Shen, 2018, « Building a Digital Silk Road? Situating the Internet in China's Belt and Road Initiative », *International Journal of Communication*, nº 12 : 2683-2701, Carnegie Mellon University. Consulté sur Internet (https://ijoc.org/index.php/ijoc/article/view/8405) le 12 novembre 2019.

HUANG Linyan, Frédéric LASSERRE et Olga V. ALEXEEVA, 2014, « Is China's Interest for the Arctic Driven by Arctic Shipping Potential? » *Asian Geographer*, vol. 32, nº 1 : 59-71. Consulté sur Internet (https://www.tandfonline.com/doi/abs/10.1080/10225706.2014.928785) le 25 février 2020.

HUAWEI, 2016, *Cinia Selects Huawei to Build Direct Digital Silk Road between Asia and Europe*, Huawei. Consulté sur Internet (https://carrier.huawei.com/en/relevant-information/all-cloud-network/build-direct-digital-silk-road) le 24 mai 2019.

HUAWEI MARINE NETWORKS, 2020, *Timeline*. Consulté sur Internet (http://www.huaweimarine.com/en/Company/timeline) le 2 mars 2020.

INTERNET SOCIETY, 2016, « Gouvernance de l'Internet. Pourquoi l'approche multi-acteurs fonctionne », *The Internet Society*. Consulté sur Internet (https://www.internetsociety.org/fr/resources/doc/2016/gouvernance-de-linternet-pourquoi-lapproche-multi-acteurs-fonctionne/) le 4 mars 2020.

JUDGE Peter, 2020, « Google and Facebook Abandon US-China Cable Plan over Security Fears », *Data Center Dynamics*. Consulté sur Internet (https://www.datacenterdynamics.com/en/news/report-google-and-facebook-abandon-us-china-cable-plan-over-security-fears/) le 6 mars 2020.

JIANG Sijia, 2019, « China's Huawei to Sell Undersea Cable Business, Buyer's Exchange Filing Shows », *Reuters*. Consulté sur Internet (https://www.reuters.com/article/us-huawei-tech-usa-cable/chinas-huawei-to-sell-undersea-cable-business-buyers-exchange-filing-shows-idUSKCN1T40BS) le 4 juin 2019.

KOPRA Sanna, 2013, « China's Arctic Interests », dans Lassi HEININEN, Heather EXNER-PIROT et Joël PLOUFFE, *Arctic Yearbook 2013*, Northern Research Forum, The Arctic of Regions vs. The Globalized Arctic. Consulté sur Internet (https://arcticyearbook.com/images/yearbook/2013/Scholarly_Papers/5.KOPRA.pdf) le 25 février 2020.

KORDAHI Maurice E., Seymour SHAPIRO et Gordon LUCAS, 2014, *Trends In Submarine Cable System Faults*, Suboptic Conference 2014. Consulté sur Internet (https://www.suboptic.org/wp-content/uploads/2014/10/WeA1.2.pdf) le 15 mars 2020.

KURLANTZICK Joshua, 2020, « China's Digital Silk Road Initiative: A Boon for Developing Countries or a Danger to Freedom? » *The Diplomat*. Consulté sur Internet (https://thediplomat.com/2020/12/chinas-digital-silk-road-initiative-a-boon-for-developing-countries-or-a-danger-to-freedom/) le 12 janvier 2021.

LAJEUNESSE Adam et Whitney P. LACKENBAUER, 2016, « Chinese Mining Interests and the Arctic », in Dawn Alexandrea BERRY, Nigel BOWLES et Halbert JONES, *Governing the North American Arctic: Sovereignty, Security, and Institutions*, Palgrave Macmillan : 74-99. Consulté sur Internet (https://link.springer.com/chapter/10.1057/9781137493910_4) le 26 février 2020.

LARTIGUE Aurore, 2019, « Un océan de câbles. Menaces sous les mers, panique dans le cyberspace », RFI. Consulté sur Internet (http://webdoc.rfi.fr/ocean-cables-sous-marins-internet/chapitre-2.html) le 6 décembre 2019.

LASSERRE Frédéric, Olga V. ALEXEEVA et Linyan HUANG, 2015, « La stratégie de la Chine en Arctique : agressive ou opportuniste? » *Norois*, vol. 3, n° 236 : 7-24. Consulté sur Internet (https://journals.openedition.org/norois/5681#xd_co_f=ZmU4YWU5ZTQtNTQ1OC00Nzk4LTkzNTEtMGQxOWIwMDc0NTQz) le 25 février 2020.

LEPOT Julien, 2014, « Netmundial, un pas décisif dans l'évolution de la gouvernance internet? » CEIS, *Les notes stratégiques*, décembre. Consulté sur Internet (https://observatoire-fic.com/wp-content/uploads/2015/01/Policy_paper_NetMundial_Gouvernance_CEIS.pdf) 15 novembre 2019.

LES ÉCHOS – INVESTIR, 2019, « Orange est prêt à envisager la reprise d'ASN avec Nokia et Bpifrance », *Les Échos-Investir*. Consulté sur Internet (https://investir.lesechos.fr/actions/actualites/orange-est-pret-a-envisager-la-reprise-d-asn-avec-nokia-et-bpifrance-pdg-1845484.php) le 4 juin 2019.

LEVINSON-KING Robin, 2019, « Huawei Heats up the Battle for Internet in Canada's North Robin », *BBC News*. Consulté sur Internet (https://www.bbc.co.uk/news/world-us-canada-49415867) le 9 septembre 2019.

LIVINGSTON D., 2016, « Scott, Assessing China's Plan to Build Internet Power », *China File*. Consulté sur Internet (https://www.chinafile.com/reporting-opinion/media/assessing-chinas-plan-build-internet-power) le 14 novembre 2019.

LOUBIÈRE Paul, 2018, « Emmanuel Macron veut confier à l'ONU la gouvernance de l'internet », *Challenges.fr*. Consulté sur Internet (https://www.challenges.fr/high-tech/la-gouvernance-de-l-internet-peut-elle-etre-confiee-a-l-onu_625833) le 16 février 2020.

Luedi Jeremy, 2020, « Northern Canada Could Be Left out in the Cold if Ottawa Passes Huawei 5G Ban », *cbc*. Consulté sur Internet (https://www.cbc.ca/news/canada/north/opinion-huawei-northern-telecom-1.5479193) le 3 mars 2020.

Macaskill Ewen, 2017, « Russia Could Cut off Internet to Nato Countries, British Military Chief Warns », *The Guardian*. Consulté sur Internet (https://www.theguardian.com/world/2017/dec/14/russia-could-cut-off-internet-to-nato-countries-british-military-chief-warns) le 25 février 2020.

Martinage Robert, 2015, « Under the Sea: The Vulnerability of the Commons », *Foreign Affairs*, Janvier-février. Consulté sur Internet (https://www.foreignaffairs.com/articles/global-commons/under-sea) le 25 février 2020.

Morel Camille, 2016, « Menace sous les mers. Les vulnérabilités du système câblier mondial », *Hérodote*, vol. 4, n° 163 : 33-43, La Découverte. Consulté sur Internet (https://www.herodote.org/IMG/pdf/her_163_0033.pdf) le 20 juin 2019.

Morel Camille, 2018, « Protéger nos infrastructures vitales pour assurer notre résilience : les câbles sous-marins, entre invisibilité et vulnérabilité », *Les Champs de Mars*, vol. 1, n° 30 : 419-426. Consulté sur Internet (https://www.cairn.info/revue-les-champs-de-mars-2018-1-page-419.htm) le 21 juin 2019.

Murdoch-Gibson Sebastian, 2018, « Finland's Arctic Data Cable Set to Disrupt Global Connectivity », *Asia Pacific Foundation of Canada*. Consulté sur Internet (https://www.asiapacific.ca/blog/finlands-arctic-data-cable-set-disrupt-global-connectivity) le 5 mai 2019.

Nilsen Thomas, 2016, « Trans-Arctic Fiber Cable Can Make Kirkenes to High-tech Hub », *The Independent Barents Observer*. Consulté sur Internet (https://thebarentsobserver.com/en/industry-and-energy/2016/12/trans-arctic-fiber-cable-can-make-kirkenes-high-tech-hub) le 2 décembre 2019.

Nocetti Julien, 2015, « Internet et sa gouvernance : la rivalité entre États-Unis et grands émergents », *Observatoire fic.com*. Consulté sur Internet (https://observatoire-fic.com/contribution-internet-et-sa-gouvernance-la-rivalite-entre-etats-unis-et-grands-emergents/) le 12 février 2020.

Page Jeremy, Kate O'Keefe et Rob Taylorin, 2019, « America's Undersea Battle with China for Control of the Global Internet Grid », *The Wall Street Journal*. Consulté sur Internet (https://www.wsj.com/articles/u-s-takes-on-chinas-huawei-in-undersea-battle-over-the-global-internet-grid-11552407466) le 10 mars 2020.

Pearce James, 2017, « China Telecom Linked to Plans for Arctic Subsea Cable », *Capacity Media*. Consulté sur Internet (https://www.capacitymedia.com/articles/3775858/China-Telecom-linked-to-plans-for-arctic-subsea-cable) le 15 novembre 2019.

Pilot, 2019, « How The Internet Reaches Antarctica ». Consulté sur Internet (https://www.pilotfiber.com/blog/how-the-internet-reaches-antarctica) le 21 février 2020.

Poole Jim, 2018, « Submarine Cable Boom Fueled by New Tech, Soaring Demand », *Equinix*. Consulté sur Internet (https://blog.equinix.com/blog/2018/03/21/submarine-cable-boom-fueled-by-new-tech-soaring-demand/) le 4 novembre 2019.

Powell Rob, 2013, « Hibernia's Express Buildout Suspended Due to Huawei's US Problems », *Telecom Ramblings*. Consulté sur Internet (https://www.telecomramblings.com/2013/02/hibernias-express-buildout-suspended-due-to-huaweis-us-problems/) le 22 janvier 2020.

Quinn Eilis, 2019, « The Arctic Railway, Building a Future… or Destroying a Culture? » *Eye on the Arctic*. Consulté sur Internet (https://newsinteractives.cbc.ca/longform/the-arctic-railway) le 15 mars 2020.

QUINTILLION, 2020, *System Specifications*. Consulté sur Internet (http://qexpressnet.com/system/), le 28 janvier 2020 et le 17 mars 2020.

RADIO-CANADA, 2019, « Huawei sous les projecteurs alors qu'elle déploiera le 4G dans le Grand Nord », *Radio-Canada*. Consulté sur Internet (https://ici.radio-canada.ca/nouvelle/1232106/telecommunications-huawei-canada-reseau-securite-autochtones) le 22 juillet 2019.

SEGAL Adam, 2018, « When China Rules the Web », *Foreign Affairs*, septembre-octobre. Consulté sur Internet (https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web) le 25 novembre 2019.

SANGER David E. et Eric SCHMITT, 2015, « Russian Ships Near Data Cables Are Too Close for U.S. comfort », *The New York Times*. Consulté sur Internet (https://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html) le 11 décembre 2019.

SAUNAVAARA Juha, 2018, « Arctic Subsea Communication Cables and the Regional Development of Northern Peripheries », *Arctic and North*, n° 32 : 51-67. Consulté sur Internet (http://www.arcticandnorth.ru/upload/iblock/298/05_Saunavaara.pdf) le 15 novembre 2019.

SGDSN, 2016, « La sécurité des activités d'importance vitale », Secrétariat général de la Défense et de la Sécurité nationale. Consulté sur Internet (http://www.sgdsn.gouv.fr/uploads/2016/10/plaquette-saiv.pdf) le 26 février 2020.

SHI Ting, 2017, « 10,000 Kilometers of Fiber-Optic Cable Show China's Interest in Warming Arctic », *Bloomberg*. Consulté sur Internet (https://www.bloombergquint.com/business/undersea-cable-project-shows-china-s-interest-in-warming-arctic) le 10 juin 2019.

STAALESEN Atle, 2019, « Russia's New Military Internet to be Supported by Arctic Cable », *The Barents Observer*. Consulté sur Internet (https://thebarentsobserver.com/en/civil-society-and-media/2019/03/russias-new-military-internet-be-supported-arctic-cable) le 17 février 2020.

STAROSIELSKI Nicole, 2015, « How Can We Protect the Internet's Undersea Cables? » *World Economic Forum*. Consulté sur Internet (https://www.weforum.org/agenda/2015/11/how-can-we-protect-the-internets-undersea-cables/) le 8 janvier 2020.

STIFEL Megan, 2017, « Maintaining U.S. Leadership on Internet Governance », *Council on Foreign Relations*. Consulté sur Internet (https://cdn.cfr.org/sites/default/files/pdf/2017/02/CyberBrief_Stifel_Governance_OR.pdf) le 12 février 2020.

SUBMARINE CABLE NETWORKS, 2020, « Arctic Connect, Submarine Cable Networks ». Consulté sur Internet (https://www.submarinenetworks.com/en/systems/asia-europe-africa/arctic-connect) le 30 août 2020.

SUBMARINE TELECOMS FORUM, 2020, « ASN Announces It Has Been Awarded the Eastern Arctic Undersea Fiber Optic Network (EAUFON) Contract, Submarine Telecoms Forum ». Consulté sur Internet (https://subtelforum.com/eaufon-submarine-cable-contract-awarded-to-asn/) le 12 janvier 2021.

SUNAK Rishi, 2017, « Undersea Cables Indispensable, Insecure », *Policy Exchange*. Consulté sur Internet (https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf) le 10 décembre 2019.

SUOKAS Janne, 2017, « China, Finland in Talks about Arctic Telecom Cable », *GBTimes*. Consulté sur Internet (https://gbtimes.com/china-finland-in-talks-about-arctic-telecom-cable) le 14 novembre 2019.

TELEGEOGRAPHY, 2020, *The Submarine Cable Map*. Consulté sur Internet (https://www.submarinecablemap.com/) le 16 mars 2020.

THE ARCTIC, 2017, « China Interested in Project to Lay Submarine Cable Line along Russian Arctic Coast », *Arctic.ru*. Consulté sur Internet (https://arctic.ru/international/20170731/650577.html) le 11 juin 2019.

The Economist, 2018, « China Has a Vastly Ambitious Plan to Connect the World ». Consulté sur Internet (https://www.economist.com/briefing/2018/07/26/china-has-a-vastly-ambitious-plan-to-connect-the-world) le 19 novembre 2019.

Tranter Emma, 2020, « Company Plans to Build $107M Fibre-optic Cable from Newfoundland to Nunavut », *CTV News*. Consulté sur Internet (https://www.ctvnews.ca/business/company-plans-to-build-107m-fibre-optic-cable-from-newfoundland-to-nunavut-1.5243445) le 12 janvier 2021.

Vaudano Maxime, 2013, « Les câbles sous-marins, clé de voûte de la cybersurveillance », *Le Monde*. Consulté sur Internet (https://www.lemonde.fr/technologies/article/2013/08/23/les-cables-sous-marins-cle-de-voute-de-la-cybersurveillance_3465101_651865.html) le 4 décembre 2019.

Vuillemin Jean-Luc, 2019, « Les câbles sous-marins, talon d'Achille de l'Internet mondial », *Atlantico*. Consulté sur Internet (https://www.atlantico.fr/decryptage/3577287/les-cables-sous-marins-talon-d-achille-de-l-internet-mondial-jean-luc-vuillemin) le 10 décembre 2019.

Warwick Martyn, 2019, « CEO of Alaskan Telco Jailed for US$1 Billion Fraud », *Telecom TV*. Consulté sur Internet (https://www.telecomtv.com/content/telco-and-csp/ceo-of-alaskan-telco-jailed-for-us-1-billion-fraud-35611/) le 10 mars 2020.

WFN Strategy, 2020, *South Pole Broadband*. Consulté sur Internet (https://wfnstrategies.com/portfolio-items/south-pole-broadband-study/?portfolioCats=55) le 14 mars 2020.

Xinhua, 2019a, « Arctic Connect Data Cable Project Delayed », *Xinhua*. Consulté sur Internet (http://www.xinhuanet.com/english/europe/2019-03/23/c_137916543.htm) le 15 avril 2019.

Xinhua, 2019b, « Plan to Build Arctic Northeast Cable Gets Boost », *Xinhua*. Consulté sur Internet (http://www.xinhuanet.com/english/europe/2019-06/07/c_138122903.htm) le 16 juillet 2019.