Éditorial. Du cyberespace à la datasphère. Enjeux stratégiques de la révolution numérique

Frédérick Douzet[1]

La révolution numérique provoquée par l'adoption massive des technologies de l'information et l'interconnexion mondiale des systèmes d'information et de communication a connu une accélération fulgurante au cours des deux dernières décennies. Elle a entraîné un bouleversement profond des pratiques sociales, économiques et politiques des sociétés humaines, plus important encore que les ruptures engendrées par l'invention de l'écriture et de l'imprimerie.

Des pans entiers de la connaissance et de l'activité humaine sont désormais transformés en données numériques dont le volume connaît une croissance exponentielle – pour ne pas dire une véritable explosion – qui oblige à développer de nouveaux types de statistiques. Le monde physique est ainsi truffé de capteurs disséminés dans l'espace public et privé, les smartphones, les objets connectés mais aussi les équipements de la vie quotidienne (automobiles, téléviseurs, appareils ménagers), de l'industrie, des armées, voire directement insérés dans le corps humain (pacemakers). Les traces numériques laissées par les usagers permettent alors d'observer et d'analyser en temps réel leurs déplacements, leurs activités et leurs interactions, et d'en tirer des analyses prédictives sur leurs besoins et leurs comportements à des fins commerciales, stratégiques, malveillantes ou d'intérêt public. Elles permettent l'essor de technologies disruptives et d'usages inédits qui révolutionnent les pratiques et ouvrent des perspectives d'évolution

1. Professeur à l'Institut français de géopolitique (université Paris 8), directrice de l'IFG Lab et de GEODE.

Hérodote, n° 177-178, La Découverte, 2e et 3e trimestres 2020.

jusqu'ici inimaginées, poussant ainsi les entreprises, les institutions et les États à entamer leur propre transformation numérique. La capacité à collecter, stocker, croiser et exploiter les données est désormais au cœur de l'innovation, moteur de la croissance économique, du pouvoir, mais aussi de multiples enjeux éthiques, démocratiques, de gouvernance et de légitimité.

Ces évolutions transforment également en profondeur l'environnement stratégique et la manière dont les grandes puissances se mesurent et s'affrontent désormais. Elles modifient les représentations de la menace mais aussi celles de la sécurité dans un environnement numérique où les interconnexions, les interactions et les interdépendances sont multiples mais ne sont pas toujours comprises, connues et maîtrisées. La transformation numérique met ainsi les gouvernements face à des choix technologiques, stratégiques et éthiques extrêmement complexes dont il est difficile d'évaluer *a priori* toutes les implications et qui mobilisent des représentations parfois contradictoires du risque et de la sécurité, selon que l'on se place du point de vue du militaire, du renseignement, des opérateurs d'importance vitale, de l'entreprise ou de la société civile. Or le champ des risques comme celui des opportunités n'a cessé de s'étendre et de se complexifier tout au long de la dernière décennie.

La transformation numérique s'est ainsi accompagnée d'une série de surprises stratégiques liées d'une part, à la sophistication croissante d'attaques de plus en plus ciblées émanant en large partie des États, et d'autre part, à la diversification des cibles, des acteurs malveillants, des modes opératoires et des conséquences, de plus en plus déstabilisatrices pour les sociétés. Les technologies numériques, par leur disponibilité et leur faible coût, rendent accessibles à une multiplicité d'acteurs de puissants outils de renseignement, d'expression, d'influence, mais aussi de redoutables vecteurs d'attaques dont les fonctions n'ont de limites que l'imagination des attaquants pour détourner ces technologies de leur usage initial. La décennie a été marquée par l'émergence du champ informationnel comme priorité stratégique (propagande djihadiste, manipulations de l'information) et d'attaques dévastatrices qui se sont propagées de manière incontrôlée à l'échelle mondiale (WannaCry et NotPetya[2]). Ces évolutions ont encouragé une course aux cyberarmes déjà bien engagée dans une dynamique de militarisation du cyberespace qui a conduit les États à en faire un champ d'affrontement privilégié.

2. Les attaques WannaCry et NotPetya de 2017 se sont propagées dans plus de 150 pays de manière incontrôlable, causant des centaines de millions d'euros de dégâts au sein d'entreprises et d'institutions de toute taille. Voir Andy Greenberg, « The untold story of NotPetya, the most devastating cyberattack in history », *Wired*, 22 août 2018.

Du cyberespace à la datasphère

En 2014, *Hérodote* publiait son premier numéro entièrement consacré aux enjeux géopolitiques du cyberespace. Le concept de cyberespace est apparu dès la fin des années 2000 dans les stratégies et les doctrines de nombreux États comme un espace de menace à la sécurité nationale, un « territoire » à maîtriser et une priorité stratégique. À la faveur de la multiplication de cyberattaques de plus en plus ciblées et sophistiquées, il s'est progressivement imposé dans les discours des États comme un nouveau domaine de compétition stratégique, un champ d'affrontement et même un nouveau milieu militaire, à côté de la terre, la mer, l'air et l'espace.

Reconnu comme une priorité stratégique et nouveau domaine militaire par le *Livre blanc sur la défense et la sécurité nationale* (LBDSN) en France de 2013, le concept de cyberespace peine cependant à véhiculer l'ampleur des défis qui se posent aux États face à la révolution numérique. La France a d'ailleurs progressivement élargi sa vision du champ de l'action stratégique et emploie volontiers le concept d'espace numérique dans ses documents stratégiques, témoignant ainsi de l'évolution d'une approche initialement technico-militaire du cyberespace à une approche beaucoup plus globale, qui nécessite la mobilisation des sciences humaines et sociales pour appréhender les nouveaux enjeux dans toute leur complexité. En témoigne d'ailleurs la décision de la ministre des Armées de créer un comité d'éthique de la Défense, inauguré en janvier 2020, en charge notamment des questions posées par les technologies numériques émergentes et leur emploi dans le domaine de la défense[3].

Dans ce numéro, nous avons choisi d'introduire le concept de datasphère, notion tout juste émergente qui englobe dans un même concept les enjeux stratégiques liés au cyberespace et plus généralement à la révolution numérique. En mettant l'accent sur le lien entre la sphère du monde physique et les données, cette notion de datasphère permet de mieux appréhender les défis présents et à venir d'un monde à la dépendance croissante aux technologies et aux données numériques, et de plus en plus gouverné par les algorithmes et l'intelligence artificielle, dont la puissance promet d'être démultipliée par l'ordinateur quantique.

La notion de « sphère des données » a d'abord été théorisée par Stéphane Grumbach dans le cadre conceptuel de l'anthropocène, un concept qui fait l'objet de vigoureux débats dans la communauté scientifique et désigne une nouvelle ère géologique caractérisée par l'incidence déterminante des activités humaines sur l'écosystème terrestre, à l'origine notamment du changement climatique. Dans

3. « Florence Parly réunit le comité d'éthique du ministère des Armées pour sa première réunion », communiqué de presse, Ministère des Armées, 14 janvier 2020.

Hérodote, n° 177-178, La Découverte, 2e et 3e trimestres 2020.

un article intitulé « La sphère des données et le droit : nouvel espace, nouveaux rapports aux territoires », avec Jean-Sylvestre Bergé, une définition qui s'appuie sur une analogie avec l'hydrosphère est proposée :

> Afin d'être appréhendée comme un nouvel espace, la sphère des données doit être considérée de manière holistique, comme un système formé de l'ensemble des données, numériques bien sûr, à l'image de l'hydrosphère, reposant sur un constituant, le bit[4] de données, en place de la molécule d'eau avec ses réservoirs et ses flux, indépendamment du contrôle que différents acteurs exercent sur l'environnement, les nœuds du réseau, ou les services essentiels exploitant les données [Bergé et Grumbach, 2016].

La sphère des données, à l'instar de l'hydrosphère, interagit ainsi avec le monde physique. Elle est à la fois ancrée dans l'environnement physique, car elle repose sur une infrastructure physique et des acteurs économiques, mais aussi en grande partie indépendante du monde physique par sa fluidité et son ubiquité. Les auteurs prennent pour exemple les multiples questions et conflits juridiques complexes auxquels est soumis le droit international public face à des situations nouvelles, aux nouveaux rapports aux territoires institutionnels classiques, voire aux « nouveaux territoires » issus de sphère des données.

La datasphère peut se concevoir comme la représentation d'un nouvel ensemble spatial formé par la totalité des données numériques et des technologies qui la sous-tendent, ainsi que de leurs interactions avec le monde physique, humain et politique dans lequel elle est ancrée. Selon la définition d'Yves Lacoste, un ensemble spatial désigne un phénomène que l'on peut observer et cartographier par la représentation des différentes caractéristiques qui constituent un territoire [Lacoste, 1993, p. 31]. La datasphère n'est certes pas un territoire au sens classique du terme en géographie mais, avec l'expansion mondiale de l'Internet, le concept de cyberespace a émergé comme la représentation d'un territoire dans les discours des acteurs politiques, pour des raisons diamétralement opposées : un territoire indépendant de partage et de liberté pour les pionniers de l'Internet, puis un territoire de menaces à sécuriser et même un champ de bataille pour les États. La territorialisation du cyberespace se retrouve dans la stratégie des États qui cherchent à se le réapproprier et mieux le maîtriser, depuis les infrastructures physiques jusqu'à l'information qui y circule.

Cet ensemble spatial construit par la société est le nouvel environnement dans lequel nous évoluons par l'adoption des technologies, des services, des

4. Le terme bit est une contraction des mots *binary digit* qui désigne un chiffre binaire (c'est-à-dire 0 ou 1). Il est utilisé comme unité de mesure de base de l'information (un octet est une suite de 8 bits).

Hérodote, n° 177-178, La Découverte, 2e et 3e trimestres 2020.

infrastructures et des armes engendrés par la révolution numérique. Il peut être appréhendé comme une forme de représentation d'une mise en données du monde qui possède sa propre géographie dont on sait encore très peu de choses. Cette géographie nécessite de mener des recherches interdisciplinaires qui permettent, à partir d'un questionnement géopolitique, de faire émerger des problématiques informatiques permettant de récolter les données nécessaires à cette analyse. Inversement, ce dialogue interdisciplinaire permet, à partir d'un questionnement technique, de faire émerger des problématiques stratégiques dont les géographes peuvent se saisir [Robine et Salamatian, 2014].

Cette géographie peut être représentée en partie par des cartes géopolitiques classiques de répartition spatiale d'infrastructures physiques (câbles, serveurs, routeurs), de ressources numériques (centres de pouvoir, de formation, de calcul, d'hébergement de données ; industrie de confiance), d'affrontements entre acteurs (origine et cible connues de cyber-attaques) ou encore de flux géolocalisables (flux de données entre États). Mais elle mobilise aussi la théorie des graphes qui permet de représenter, à partir de nœuds et de liens, des relations et des interactions entre acteurs que l'on peut spatialiser afin de faire apparaître le degré de proximité entre acteurs en fonction de l'intensité de leurs échanges. Certains de ces acteurs peuvent parfois être géolocalisés, afin d'établir une correspondance entre le graphe et la carte géopolitique. Ces méthodes sont par exemple utilisées pour identifier des communautés à partir des échanges dans le réseau social Twitter, ou pour représenter les chemins que peuvent emprunter les données pour voyager d'un point à un autre de la datasphère. Nos travaux nous ont ainsi permis de mettre au jour la stratégie de l'Iran pour déconnecter son espace national de la datasphère mondiale[5] [Salamatian *et al*., 2019] ou encore les dynamiques de fragmentation qui s'opèrent au niveau topologique en Crimée et dans le Donbass, en conséquence des rivalités de pouvoir et des stratégies d'appropriation territoriale de la Russie en Ukraine [Douzet *et al*., à paraître].

La délimitation des ensembles spatiaux ne va pas toujours de soi et diffère en fonction de l'objet étudié et de ce que l'on cherche à démontrer [Loyer, 2019, p. 22]. Leurs limites ne coïncident pas. Au contraire, les ensembles spatiaux se recoupent et forment une série d'intersections qui engendrent des frictions pouvant conduire à des conflits géopolitiques. L'analyse de ces intersections est particulièrement complexe lorsqu'il s'agit d'articuler plusieurs niveaux d'analyse. Yves Lacoste distingue ainsi plusieurs ordres de grandeur, afin de systématiser la référence à la taille des ensembles spatiaux étudiés. Cette démarche est d'autant plus intéressante pour analyser la datasphère que, d'une part, elle forme un

5. Voir l'interview de Frédérick Douzet et Michaël Szadkowski, « Internet coupé en Iran : "Le niveau de sophistication de ce blocage est une première" », *Le Monde*, 20 novembre 2019.

ensemble spatial à l'échelle planétaire et, d'autre part, elle peut s'étudier à différents niveaux d'analyse, depuis le niveau régional par l'ensemble des ressources numériques stockées ou accessibles sur un petit territoire jusqu'aux interactions à l'échelle planétaire. Ainsi la question de la « souveraineté numérique » peut-elle s'analyser comme une démarche de territorialisation de la datasphère qui nécessiterait de déterminer et cartographier les caractéristiques susceptibles de définir et délimiter cet ensemble spatial que les acteurs se représentent comme leur territoire souverain. La Russie, par exemple, en précise sa vision dans une série de lois élaborées depuis 2012 qui comprend, entre autres, localisation des données afférentes aux citoyens russes sur le territoire national, maîtrise des routes empruntées par les données et possibilité de couper leur réseau de l'Internet mondial, obligation aux constructeurs d'équipement informatique grand public de préinstaller des logiciels russes sur leurs produits, obligation pour les services de l'État d'utiliser des logiciels russes. Et avec la transformation numérique des sociétés et leur dépendance croissante aux technologies et données numériques, la datasphère se trouve à l'intersection de la plupart des autres ensembles spatiaux, depuis les villes – et même les parcelles agricoles – connectées jusqu'à l'espace extra-atmosphérique, dans lequel la prolifération des acteurs et objets spatiaux connectés importe les problématiques de la révolution numérique.

Cette géographie de la datasphère est éminemment stratégique et indispensable à la compréhension du monde contemporain et des rivalités de pouvoir géopolitiques. Elle inclut la géographie des flux et la maîtrise des données, la compréhension de l'espace informationnel, la cartographie des réseaux topologiques, ou encore la fusion de données géolocalisées et de données non spatialisées. Elle comprend aussi des dimensions juridiques complexes et l'analyse des représentations pour appréhender et caractériser des phénomènes en partie intangibles. Son étude peut révéler des déséquilibres et des rapports de force, des stratégies d'acteurs, des manœuvres voire des affrontements qui s'opèrent dans et hors de la datasphère.

Le projet GEODE

Ce numéro réunit – entre autres – un grand nombre d'auteurs issus de l'équipe du projet Géopolitique de la datasphère (<https://geode.science>), un centre de recherche et de formation dédié à l'étude des enjeux géopolitiques et stratégiques de la révolution numérique. Le projet GEODE, porté par l'université Paris 8, réunit autour de l'équipe de l'Institut français de géopolitique d'autres chercheurs de l'université Paris 8 (droit, philosophie, informatique), l'Inria, Saint-Cyr Coëtquidan, l'ENS, l'université de Savoie et l'université Paris Descartes.

Hérodote, n° 177-178, La Découverte, 2e et 3e trimestres 2020.

Présélectionné par le ministère des Armées, pour un label « Centre d'excellence » dans le cadre du Pacte Enseignement supérieur, le projet GEODE oriente ses recherches et ses formations dans deux directions principales. La première consiste à étudier la datasphère comme un objet géopolitique à part entière, avec une analyse des enjeux de défense, de sécurité, de diplomatie – et plus largement de société – qu'elle recouvre. Cette approche nécessite le développement d'une cartographie spécifique pour mieux appréhender, comprendre et représenter la géographie de la datasphère et ses enjeux. La deuxième consiste à utiliser les ressources de la datasphère pour faire de l'analyse géopolitique, c'est-à-dire développer des outils et des méthodologies d'enquête de terrain numérique. L'approche géopolitique combinée au maniement d'informations très techniques et de grands volumes de données en sources ouvertes permet, par le croisement d'immenses volumes de données spatialisées et non spatialisées, de comprendre les relations entre acteurs, les stratégies d'influence, les enjeux d'un conflit géopolitique ou d'un marché sensible. Ces recherches nécessitent une approche intrinsèquement interdisciplinaire entre les sciences humaines et sociales (géographie, droit, sciences politiques, philosophie) et les sciences informatiques et mathématiques.

Hérodote présente ici une partie des recherches menées au sein du projet GEODE ou en lien avec ses chercheurs. L'article de Stéphane Grumbach permet de plonger le lecteur d'emblée dans le grand bain numérique. Il démontre à quel point les questions numériques et climatiques sont intimement liées, alors que la révolution numérique avance dans le contexte d'une dégradation de l'environnement qui contraint nos sociétés à évoluer pour réduire l'empreinte des activités humaines sur la planète. Les données numériques reflètent à la fois le monde physique et les activités humaines. Associées à de puissants algorithmes, ces données au volume vertigineux permettent aussi bien d'observer et de comprendre les écosystèmes que de prédire les évolutions climatiques. Elles permettent aussi d'analyser dans les moindres détails nos déplacements, nos occupations, nos échanges sociaux, nos comportements commerciaux, et donc de mettre en place des formes de gouvernance numérique qui commencent à émerger dans certains pays d'Asie, en particulier la Chine. Sa mise en œuvre dans le cadre de l'épidémie du coronavirus illustre à la fois les bénéfices potentiels qu'elle offre mais aussi les risques éthiques et d'atteinte aux droits humains qu'elle entraîne. Ces initiatives confrontent les représentations occidentales des libertés individuelles à des représentations originales sur la nature et l'intérêt collectif, ancrées dans la philosophie ancienne chinoise, et mises en avant pour expérimenter de nouvelles formes de gouvernance numérique afin d'appréhender les défis de plus en plus complexes auxquels nos sociétés font face. L'enjeu politique majeur, comme l'explique Stéphane Grumbach, est de mettre le numérique au service du développement harmonieux et de la pérennité de nos sociétés. Or les transformations opérées par

Hérodote, n° 177-178, La Découverte, 2e et 3e trimestres 2020.

le numérique, si elles peuvent être source de solution, sont aussi un facteur de déstabilisation politique et d'aggravation des clivages partisans et sociaux dans nos démocraties.

Manipulations de l'information

Le piratage des messages électroniques du parti démocrate et leur publication par WikiLeaks au cours de la campagne présidentielle de 2016 ont pris l'administration américaine totalement par surprise. Prenant soudain conscience des vulnérabilités d'un système reposant sur des registres électoraux et des machines à voter peu sécurisées, l'administration a craint qu'une cyber opération porte atteinte à l'intégrité du processus électoral. Or, c'est sur le plan informationnel que l'opération d'ingérence s'est jouée, exploitant une vulnérabilité majeure – mais non informatique – de la société américaine, à savoir la forte polarisation politique et le ressentiment des laissés-pour-compte de la mondialisation à l'égard des élites. L'article de Camille François et Herbert Lin montre que cet angle mort dans l'analyse de la menace s'explique par une vision très occidentale et techno-centrée du cyberespace, dans laquelle les manipulations de l'information n'appartiennent pas au registre classique des opérations de « cyberguerre ». Leur appréhension nécessite de croiser trois champs différents de la littérature scientifique qui fonctionnent trop souvent en silos.

Or les démocraties occidentales se trouvent désormais confrontées au risque, décuplé par le Web et les réseaux sociaux, de manipulation à grande échelle de l'opinion publique dans un contexte de crise de confiance dans les institutions, de montée des populismes, voire de radicalisation. La liberté d'expression peut alors être instrumentalisée comme levier de déstabilisation lors d'une affaire politique, d'un débat public, d'un mouvement social ou d'un processus électoral. En Inde, cette instrumentalisation vient du parti au pouvoir et même de Narendra Modi en personne, comme le démontre Maya Mirchandani. Le gouvernement favorise le développement de la connectivité et la transformation numérique de l'État tout en exploitant les réseaux sociaux à des fins électorales, notamment en attisant les tensions entre les groupes ethniques et sociaux avec des conséquences dramatiques.

En Europe, la représentation de la menace est à la fois externe et interne. L'article de Martin Innes et son équipe analyse les méthodes et les objectifs respectifs des groupes d'extrême droite et des groupes proches de la Russie sur les réseaux sociaux au cours des campagnes électorales en Europe. Il démontre notamment l'impact des innovations associées aux techniques d'ingénierie de l'influence employées par ces groupes. Les opérations informationnelles peuvent

Hérodote, n° 177-178, La Découverte, 2e et 3e trimestres 2020.

aussi toucher des zones d'intérêt stratégique ou s'y étendre de manière opportuniste. La propagation des contenus produits par les agences russes et chinoises en Afrique francophone démontre l'influence croissante des narratifs de ces puissances, reprises de manière volontaire par des sites d'informations à travers le continent (voir l'article de Douzet, Limonier, Mihoubi et René). Le sujet suscite de vives inquiétudes mais aussi beaucoup de confusion. La prolifération de termes pour décrire ce phénomène (*fake news*, désinformation, manipulations de l'information) est révélatrice de la difficulté à le saisir et le caractériser, d'où l'importance de mener des études précises pour le comprendre. L'article de Colin Gérard et Guilhem Marotte permet ainsi de démythifier le rôle des comptes Twitter russes dans l'amplification de l'affaire Benalla et propose une méthodologie pour analyser et représenter les communautés sur ce réseau social.

La lutte contre ce phénomène est d'autant plus complexe que les acteurs s'appuient, d'une part, sur la liberté d'expression, valeur fondamentale des démocraties, et, d'autre part, sur des plateformes aux activités transfrontalières sur lesquelles la plupart des États n'ont pas autorité. Ces plateformes s'imposent ainsi sur la scène internationale comme un défi à la souveraineté des États mais aussi comme un partenaire essentiel dans l'exercice de leurs pouvoirs régaliens. L'enjeu de la puissance et de la souveraineté est d'ailleurs au cœur de la politisation croissante des questions de technologies numériques.

Enjeux stratégiques des technologies numériques

La question du *cloud computing* – qui permet le stockage et l'utilisation à distance de données et de services numériques – en est l'illustration même. L'article de Clotilde Bômont et Amaël Cattaruzza montre le glissement, dans les représentations stratégiques françaises, d'une question d'abord de compétitivité économique à une question de sécurité et de souveraineté nationale. Or le *cloud* totalement souverain reste un mythe en raison des interdépendances technologiques mais aussi de la réalité du marché et des moyens européens. La technologie du *cloud computing* est pourtant devenue indispensable à la transformation numérique des entreprises et des institutions et même des armées, comme le démontre l'amiral Arnaud Coustillière. La donnée numérique est au centre des enjeux de la transformation numérique du ministère des Armées, qui vise à s'approprier rapidement les technologies émergentes au travers de nouveaux usages, à provoquer des ruptures dans les pratiques, l'organisation du travail et l'action globale des armées. Il faut donc apprendre à mieux la traiter et la partager, mais aussi la stocker et la sécuriser. L'ambition numérique du ministère est aussi une ambition de souveraineté numérique, qui se décline dans le langage militaire en autonomie stratégique.

Hérodote, n° 177-178, La Découverte, 2e et 3e trimestres 2020.

Ces concepts présentent les deux faces d'une même pièce, celle de la capacité de l'État à exercer ses pouvoirs régaliens et à conserver la maîtrise de son destin à l'ère numérique. Le concept de souveraineté numérique s'est imposé dans le débat public à la suite des révélations d'Edward Snowden sur la surveillance de masse des États-Unis, alors que l'Europe prenait brutalement conscience des enjeux de sa dépendance aux technologies numériques américaines. Alix Desforges et Didier Danet démontrent les difficultés à définir les contours de ce concept très médiatique qui recouvre un grand nombre d'enjeux d'ordre différent, d'où la préférence pour le concept d'autonomie stratégique dans la littérature officielle. Sa mise en œuvre reste toutefois complexe, à l'échelle nationale et européenne, aussi bien dans sa dimension politique qu'industrielle. La transition de la technologie mobile 4G vers la 5G en est le parfait exemple.

Kavé Salamatian explore les enjeux à la fois économiques, technologiques et géopolitiques d'un déploiement hautement stratégique de la 5G, alors que Donald Trump fait pression sur ses alliés pour bannir l'entreprise Huawei, très en avance sur les autres entreprises y compris américaines, des marchés européens. En focalisant toute l'attention sur l'entreprise chinoise, le président américain tend à imputer tous les problèmes de sécurité et les risques pourtant inhérents à toute technologie numérique à un fournisseur en particulier – parmi une liste noire d'entreprises technologiques chinoises –, une stratégie qui en dit plus long sur la compétitivité de la Chine et le contexte de compétition stratégique exacerbée entre les deux pays que sur la technologie elle-même. Donald Trump n'hésite d'ailleurs pas à politiser les questions technologiques. Alors que l'administration Obama avait longuement consulté les experts et mûri sa réflexion sur la neutralité du Net avant de trancher en sa faveur, Donald Trump à peine arrivé au pouvoir a choisi de la faire supprimer. Ce principe fondateur de l'Internet garantit l'égalité de traitement de tous les flux de l'Internet, et interdit donc aux fournisseurs d'accès à l'Internet de favoriser ou ralentir certains contenus. Charlotte Escorne démontre le lobbying politique exercé par ces puissants acteurs auprès de l'instance fédérale de régulation des communications pour supprimer ce principe populaire auprès de l'opinion publique et ardemment défendu par les entreprises de la Silicon Valley bien décidées à se battre pour le rétablir. Elle montre aussi l'enjeu, pour les opérateurs, de dégager de nouveaux revenus à des fins d'investissements dans un contexte où l'essentiel de la valeur est capté par les plateformes d'intermédiation.

La souveraineté numérique, pour la Russie, n'est pas un concept ou une ambition mais bien une politique publique qui vise à assurer l'autonomie stratégique et l'indépendance numérique de la Russie contre la dépendance à des entités extérieures. Marie-Gabrielle Bertran montre que les révélations de Snowden ont servi de catalyseur à des ambitions de développement numérique qui misent en priorité sur le logiciel libre et open-source, qui cumulent les avantages d'un faible

Hérodote, n° 177-178, La Découverte, 2e et 3e trimestres 2020.

coût d'exploitation et de la possibilité de favoriser le contrôle des infrastructures numériques par les autorités étatiques, une pratique aux antipodes de l'esprit qui les avait fait naître pour permettre aux utilisateurs de choisir et contrôler eux-mêmes le fonctionnement de leurs logiciels. La stratégie russe passe aussi par le développement de territoires stratégiques du numérique. L'article de Kévin Limonier et Hugo Estecahandy s'intéresse au minage de cryptomonnaies en Sibérie, région où l'abondance d'électricité à prix attractif, le climat froid et les nombreux centres d'hébergement de données créent un contexte favorable au développement de cette activité qui à son tour contribue à façonner le territoire.

Stratégies de puissance dans le cyberespace

L'Estonie a d'ailleurs complètement misé sur le numérique pour développer son territoire et s'émanciper de la puissance russe pour se construire une identité nationale forte, au lendemain de la chute de l'Union soviétique. Léa Ronzaud montre qu'en incluant l'innovation technologique, la cybersécurité et la cyberdéfense dans sa stratégie de « nation-branding », l'Estonie a pu prendre une avance considérable sur les autres pays en matière de développement numérique et assurer son rayonnement international. Le pays, paralysé par des cyberattaques en 2007 qui suscitèrent une véritable prise de conscience à l'échelle internationale, a su tirer parti de sa visibilité médiatique pour conserver sa place de leader mondial dans le domaine de l'innovation numérique, même si cette stratégie commence à montrer ses limites.

Israël, en revanche, ne semble pas connaître de limites. L'innovation est en plein essor et s'inscrit dans une stratégie plus globale de puissance au sein de laquelle le numérique occupe une place de choix. David Amsellem montre comment l'État hébreu a réussi à développer une industrie de pointe dans le domaine numérique et s'est pleinement investi dans le développement de capacités cyber au service de son influence et de sa puissance. Dans l'espace numérique comme dans les autres domaines militaires, Israël privilégie sa rapidité d'action, son agilité et sa force de frappe pour établir un rapport de force favorable face à ses ennemis, quel qu'en soit le coût politique ou juridique, participant ainsi pleinement à la militarisation du cyberespace dénoncée par la Chine.

Et pourtant la Chine a pour ambition de devenir la « cyber-puissance majeure », un objectif élevé au rang de priorité absolue par les autorités chinoises. Rogier Creemers montre que cette stratégie de puissance s'inscrit dans l'objectif plus large du président Xi Jinping d'accomplir le « rêve chinois » et répond d'abord à des objectifs de politique intérieure, même si elle comprend un volet diplomatique de plus en plus important. Les investissements massifs consacrés à l'éducation,

Hérodote, n° 177-178, La Découverte, 2e et 3e trimestres 2020.

la recherche et le développement pour faire progresser l'économie numérique et l'intelligence artificielle doivent servir d'abord à mieux développer et gouverner le pays, et lui permettre d'accomplir son programme politique tout en assurant sa stabilité politique. L'essor du numérique s'accompagne ainsi d'une indissociable politique de cybersécurité, qui inclut aussi le contrôle des contenus informationnels qui circulent sur le Web et les réseaux. Rogier Creemers montre aussi que cette politique s'est construite en opposition au rôle joué dans le paysage numérique mondial par les États-Unis, puissance qu'elle perçoit comme son seul réel homologue et un potentiel danger en raison de la supériorité de ses ressources.

La puissance américaine est en effet incontournable dans le cyberespace. Or, la stratégie de l'administration Trump en la matière a pris un tournant particulièrement offensif qui suscite beaucoup de débats et de questionnements outre-Atlantique. Stéphane Taillat analyse la doctrine du *Persistent Engagement* et le concept *Defend Forward* de la vision du Cyber Command qui favorise la reconnaissance des cyber opérations offensives et constitue ainsi une inflexion des représentations et des dispositifs dans ce nouveau domaine militaire. Stéphane Taillat questionne la pertinence de cette posture de projection de puissance aux accents dissuasifs pour atteindre les objectifs de sécurité des États-Unis et de stabilité internationale dans le cyberespace. En légitimant le recours à l'action offensive dans l'espace numérique, cette stratégie contribue directement à l'accélération de la course aux cyberarmes.

Comme quoi le cyberespace, ça sert, d'abord, à faire la guerre. C'est le titre – certes provocateur – que nous avons choisi avec Aude Géry pour résumer les enjeux des discussions internationales qui se déroulent depuis l'automne 2019 au Nations unies visant à assurer la sécurité et la stabilité du cyberespace. La notion de cyberespace est ici étroitement liée à sa territorialisation et sa militarisation, autrement dit la constitution de l'espace numérique en objet de sécurité que les géographes critiques appellent sécuritisation. Les États se retrouvent cependant pris entre deux impératifs de sécurité qui créent une tension contradictoire : d'une part, assurer leur puissance numérique pour conserver leur autonomie stratégique et leur supériorité opérationnelle vis-à-vis de leurs ennemis et adversaires ; et, d'autre part, juguler le risque systémique lié à la prolifération des outils offensifs qui peuvent se retourner contre eux, se propager de manière incontrôlée, provoquer des dommages sévères et déstabiliser le cyberespace et les sociétés.

In fine, le débat rejoint les préoccupations soulevées il y a plus de cinquante ans par le débat sur la dissuasion nucléaire. Sauf que le numérique est partout, les outils offensifs à portée de tous, et les interconnexions et interactions entre domaines multiples, mal connues et donc difficilement maîtrisables. Les États se retrouvent ainsi à la croisée des chemins. Et même dans la datasphère, il y a des chemins qui mènent là où l'on ne voudrait pas se retrouver.

Hérodote, n° 177-178, La Découverte, 2e et 3e trimestres 2020.

Bibliographie

BERGÉ J. S. et GRUMBACH S. (2016), « La sphère des données : objet du droit international et européen », *Journal du droit international (Clunet)*.

CATTARUZZA A. (2019), *Géopolitique des données numériques. Pouvoir et conflits à l'heure du big data*, Paris, Le Cavalier Bleu.

DOUZET F., PÉTINIAUD L., SALAMATIAN L., LIMONIER K., SALAMATIAN K. et ALCHUS T. (à paraître), « Measuring the fragmentation of the Internet : the case of the Border Gateway Protocol (BGP) during the Ukrainian crisis », *CyberConflict (CyCon) 2020 12th Conference on Cyber Conflict IEEE*.

Hérodote (2014), « Cyberespace : enjeux géopolitiques », n° 152-153.

LACOSTE Y. (1993), *Dictionnaire de géopolitique*, Paris, Flammarion.

LIMONIER K. (2018), *Ru.net. Géopolitique du cyberespace russophone*, Paris, L'Inventaire, « Les Carnets de l'Observatoire ».

LOYER B. (2019), *Géopolitique. Méthodes et concepts*, Paris, Armand Colin.

ROBINE J. et SALAMATIAN K. (2014), « Peut-on penser une cybergéographie ? », *Hérodote*, n° 152-153, p. 123-139.

SALAMATIAN L., DOUZET F., SALAMATIAN K. et LIMONIER K. (2019), « The geopolitics behind the routes of data travel : the case of Iran », <https://arxiv.org/abs/1911.07723>.