La géopolitique pour comprendre le cyberespace

Frédérick Douzet[1]

Dès 1997, dans un article intitulé « Internet géopolitise le monde », *Hérodote* annonçait la couleur : « À défaut de temporiser les conflits géopolitiques, l'Internet semble au contraire les multiplier et les compliquer » [Douzet, 1997]. À contre-courant des voix optimistes qui annonçaient ni plus ni moins que la fin de la géographie, nous pointions déjà les enjeux géopolitiques de l'expansion irrésistible des systèmes d'information et de communication à travers le monde :

> Le réseau [Internet] est lui-même l'enjeu de nombreux conflits géopolitiques qui donnent lieu à des stratégies de domination de la part des nations aux intérêts divergents qui cherchent à en contrôler le contenu, le fonctionnement et le développement économique. Il est une arme hautement stratégique pour la sécurité des nations [...] et surtout un instrument extrêmement puissant dans les rivalités de pouvoir entre groupes, minorités, forces politiques, religieuses, économiques, au niveau local comme au niveau mondial.

S'il était encore permis d'en douter, les révélations d'Edward Snowden sur les programmes de surveillance massive de la National Security Agency des États-Unis ont démontré à quel point la géographie se porte bien et la géopolitique garde toute sa pertinence pour comprendre les conflits du monde moderne. C'est d'ailleurs l'argument de James A. Lewis, chercheur au Center for Strategic

Hérodote, n° 152-153, La Découverte, 2e trimestre 2014.

1. Professeure à l'Institut français de géopolitique de l'université Paris-VIII. Titulaire de la chaire Castex de cyberstratégie (Cercle des partenaires de l'IHEDN, avec le soutien de la fondation Airbus Group).

and International Studies (CSIS)[2], qui démontre que l'impact des révélations sur les négociations internationales diffère en fonction des pays mais que globalement, malgré la révolution numérique, les intérêts et objectifs stratégiques des États restent pour l'instant inchangés. La cartographie de la surveillance, réalisée par Louis Pétiniaud[3], est révélatrice de la signifiance des frontières politiques, même à l'heure où la technologie les traverse. Au début des années 1990 pourtant, l'accroissement fulgurant des communications libres de contraintes d'espace et de temps portait la promesse d'une démocratisation et d'une pacification du monde par la diffusion des idées et des valeurs démocratiques. L'émergence d'un cyberespace né de l'interconnexion des réseaux représenterait même l'avènement d'un « village global », à l'image du rêve formulé trente ans plus tôt par Marshall McLuhan [McLuhan, 1964]. L'expansion des réseaux de communication a de tout temps suscité l'utopie d'un monde meilleur [Musso, 2003 ; Mattelart, 2009] ; mais l'Internet a engendré autant de défis que de promesses.

La croissance exponentielle de l'Internet a révolutionné nos modes de vie, bouleversé notre économie, démultiplié nos moyens de communication et ouvert bien des horizons que nous commençons tout juste à explorer. Elle a aussi engendré de belles crispations territoriales, avec une prolifération des conflits entre une multitude d'acteurs à propos de son contrôle et sa régulation. Les tensions se cristallisent autour de l'émergence de nouvelles menaces liées à la cybercriminalité ou l'utilisation des réseaux informatiques dans le cadre de conflits politiques, de combats militaires, de guerre économique, de renseignement ou de politique d'influence diplomatique et culturelle. À l'heure du Big Data (ensemble de données très volumineuses) et de l'Open Data (mise à disposition des données publiques), les débats se multiplient autour des enjeux de respect de la vie privée, de protection de la liberté d'expression et autres libertés individuelles. L'affaire Snowden touche à tous ces enjeux à la fois, car dans le cyberespace, comme nous le verrons, ils sont inextricables.

Pendant longtemps, ces questions sont restées entre les mains d'une petite communauté d'experts de culture scientifique et technique. Elles entrent aujourd'hui avec fracas dans la sphère publique, parce qu'avec le développement massif de l'Internet (près de trois milliards d'utilisateurs) et son omniprésence dans nos vies quotidiennes, beaucoup de ces décisions techniques sont devenues politiques et stratégiques. Nombre d'acteurs (individus, groupes, start-up...) ont su tirer parti – et profit – de la croissance des réseaux avec une réactivité et une créativité

2. Basé à Washington DC, il est classé pour la troisième année consécutive premier *think tank* sur les questions « Défense et sécurité nationale » par le *Global Go To Think Tank Index*, rapport annuel de l'université de Pennsylvanie sur les *think tanks* aux États-Unis.

3. Étudiant en master à l'Institut français de géopolitique, université Paris-VIII.

Hérodote, n° 152-153, La Découverte, 2e trimestre 2014.

parfois époustouflantes, pour le meilleur comme pour le pire. Les gouvernements, les militaires, les entreprises, les citoyens ont désormais besoin de mieux comprendre ces enjeux pour veiller à leurs intérêts et développer des stratégies cohérentes, afin de saisir les nouvelles opportunités en gérant les risques qui leur sont liés. C'est notamment le cas des États, dont les pouvoirs régaliens sont mis au défi par de multiples acteurs dans le cyberespace, qu'il s'agisse de criminels, de hackers, de militants, de grandes entreprises privées, de dissidents, d'acteurs non étatiques ou d'autres États. Ces enjeux de pouvoir et de puissance se jouent hors des territoires classiques de la géopolitique ; et pourtant la géopolitique est un outil indispensable pour les analyser.

La géopolitique à la conquête du cyberespace

Comment la géopolitique peut-elle permettre de comprendre les conflits du cyberespace ? Le défi méthodologique est aussi important que stimulant. La géopolitique étudie les rivalités de pouvoir et d'influence sur un territoire, à différents niveaux d'analyse. Elle s'intéresse aux dynamiques d'un conflit sur ce territoire, aux représentations contradictoires et aux stratégies des acteurs pour son contrôle, son appropriation et la défense de leurs intérêts au sein de ce territoire. Le territoire est donc au cœur de l'analyse, ce qui à propos du cyberespace pose évidemment problème. Le cyberespace est-il une nouvelle forme de territoire ? Et, si oui, quelles en seraient les frontières ? Quelles en seraient les limites de souveraineté ?

Encore faut-il comprendre ce que l'on entend par cyberespace. Il n'en existe pas de définition objective et consensuelle, on en compte de multiples, plus ou moins précises, qui reflètent les préoccupations et les intérêts des acteurs. Les Russes, comme les Chinois, utilisent peu le terme cyberespace – qui pourrait renvoyer à l'idée d'un espace à part, transfrontières – et préfèrent parler d'Internet ou de sécurisation de l'information, ramenant ainsi les discussions dans le champ de compétences des États. Dans un but pédagogique, on peut toutefois proposer une définition *a minima*. Le cyberespace, c'est à la fois l'Internet[4] et l'« espace » qu'il génère : un espace intangible dans lequel s'opèrent des échanges déterritorialisés entre des citoyens de toutes nations, à une vitesse instantanée qui abolit toute notion de distance. Si la définition de l'Internet est technique et communément

4. Ou plus précisément l'interconnexion mondiale d'équipements de traitement automatisé des données numériques, selon la définition de l'Agence nationale pour la sécurité des systèmes d'information, 2011. Les systèmes d'information et de communication ne se limitent pas à l'Internet, mais c'est bien l'Internet qui a donné naissance à ce que l'on conçoit aujourd'hui comme le cyberespace.

admise (voir lexique, à la fin de cet éditorial) – le réseau informatique mondial relie plus de 40 000 réseaux autonomes, utilisant un même langage –, la qualification de l'espace qu'il génère fait l'objet de représentations contradictoires, nourries d'images venues de la littérature de science-fiction, du militantisme, de la politique ou encore du marketing. Le fameux *Cloud* ne fait qu'ajouter au brouillard sémantique.

Une architecture en couches

Pour mieux comprendre, on évoque parfois sa structure en couches superposées, qui permet de décomposer le cyberespace comme un millefeuille dont les différentes couches pourraient interagir entre elles. Selon les auteurs, on les décompose en 3, 4, 5, voire 7 couches. Et à tous les étages de cette structure, on trouve des rivalités de pouvoir entre des acteurs sur des questions souvent très techniques, dont les enjeux sont pourtant très géopolitiques, comme nous allons le voir.

Pour simplifier, nous présenterons quatre couches. La première couche est physique. Composée de câbles sous-marins et terrestres, véritable épine dorsale de l'Internet (*backbone*), de relais radio, d'ordinateurs, elle est l'infrastructure physique de l'Internet : un ensemble de matériels installés sur le territoire, soumis aux contraintes de la géographie physique et politique, que l'on peut construire, modifier ou détruire, connecter ou déconnecter du réseau. L'article de Jérémy Robine et Kavé Salamatian montre l'importance et les enjeux stratégiques de cette infrastructure, qui, parce qu'elle est géolocalisable, est la moins difficile à cartographier lorsque l'on s'essaie à une cybergéographie. Kevin Limonier analyse, cartes à l'appui, le développement stratégique de l'infrastructure russe, et les représentations qui le sous-tendent. L'infrastructure physique a été conçue dans un esprit d'ouverture et de circulation maximale de l'information, sans aucune sécurité intégrée. L'un des pères fondateurs de l'Internet, Louis Pouzin, estime même que pour sécuriser l'Internet, il faudrait le reconstruire de fond en comble[5].

La deuxième couche est l'infrastructure logique. Elle comprend tous les services qui permettent d'assurer la transmission des données entre deux points du réseau et, donc, de faire voyager l'information, découpée en petits paquets de données, de son expéditeur à son destinataire. L'architecture logique repose sur une harmonisation essentielle, un langage commun qui permet à tous les ordinateurs du monde de communiquer entre eux, le protocole Internet (TCP/IP). Ces services sont le routage (choix de la route par laquelle voyagent des paquets de

5. N. Madelaine, « Louis Pouzin : "L'Internet doit être refait de fond en comble" », *Les Échos,* n° 21442 du 24 mai 2013, p. 23.

Hérodote, n° 152-153, La Découverte, 2e trimestre 2014.

données entre deux réseaux), le nommage (noms identifiant les éléments du réseau ou les utilisateurs) ou encore l'adressage (qui transforme les séries de chiffres représentant les adresses en mots intelligibles pour les utilisateurs). Là encore, certains aspects peuvent être géolocalisés au prix de quelques défis techniques (chemins empruntés, noms de domaines, adresses IP...). L'entretien accordé par Bertrand de La Chapelle rend compte des débats et des revendications autour de l'enjeu de l'adressage, en raison du contrôle symbolique fort qu'exercent encore les États-Unis par le pouvoir décisionnaire du secrétariat au Commerce. Dominique Lacroix montre, quant à elle, l'enjeu économique et politique de l'acquisition des noms de domaine.

La troisième couche est composée des applications, qui sont des programmes informatiques conviviaux permettant à tout un chacun d'utiliser l'Internet sans rien connaître à la programmation informatique (Web, e-mail, réseaux sociaux, moteurs de recherche, etc.). L'affaire Snowden a bien montré l'enjeu du succès planétaire des applications de quelques grandes entreprises (Google, Facebook, Amazon...), auxquelles les utilisateurs confient leurs données privées, exploitées ingénieusement par les équipes marketing ou les services de renseignement du pays, ce que Stéphane Frénot et Stéphane Grumbach considèrent comme le nouvel or noir de l'économie. Les données ne s'évaporent ainsi pas dans les nuages (le *Cloud*...) mais sont bien stockées sur des serveurs gérés par des acteurs privés ou publics.

Enfin, la quatrième couche est celle de l'information et de l'interaction sociale, que l'on nomme parfois cognitive ou sémantique. C'est celle des utilisateurs, des discussions et des échanges en temps réel à travers le monde, la plus difficile à appréhender et représenter d'un point de vue géographique. Ce n'est pourtant pas la moins pertinente d'un point de vue géopolitique, lorsqu'on arrive à déterminer qui sont les pays les plus « amis » sur Facebook, en quelles langues sont disponibles les contenus dans certaines régions de la planète, d'où partent les révoltes sur les réseaux sociaux ou les campagnes de désinformation contre un gouvernement ou une institution...

Le cyberespace serait donc tout cela à la fois, un ensemble de réseaux interconnectés d'ordinateurs – et de plus en plus d'objets mobiles (téléphones, tablettes et bientôt réfrigérateurs, bracelets, chaussures de sport...) –, de réseaux humains, de flux de données ; un espace d'information et d'échanges déterritorialisés, complexe à appréhender, constitué par une infrastructure matérielle installée sur le territoire physique, voire dans l'espace extra-atmosphérique pour les satellites. Selon qui l'utilise et pourquoi, le terme de cyberespace peut renvoyer à une infrastructure physique ou à des imaginaires complètement différents, dans un certain flou conceptuel.

La géopolitique apporte dès lors un outil indispensable à l'appréhension du cyberespace : les représentations. Une représentation est une construction, une

Hérodote, n° 152-153, La Découverte, 2e trimestre 2014.

façon de voir les choses, d'assembler des idées de façon plus ou moins logique et cohérente, qui a une fonction dans les conflits géopolitiques. Elle s'appuie sur des faits objectifs mais garde un caractère profondément subjectif. Les représentations ne sont pas neutres, elles influencent comme elles peuvent servir les stratégies des acteurs dans le but de convaincre, d'inquiéter, d'enthousiasmer ou de mobiliser des acteurs (électeurs, militants, investisseurs, militaires, internautes...).

« Planter son drapeau » dans le cyberespace

Le cyberespace n'est pas un territoire au sens géographique du terme, à savoir « une étendue sur laquelle vit un groupe humain qu'il considère comme sa propriété collective » [Lacoste, 2003], ou pour les États « une portion de l'espace terrestre délimitée par ses frontières et sur laquelle s'exercent son autorité et sa juridiction » [Lacoste, 2003]. Mais il est perçu comme un espace dans lequel interagissent des êtres humains, voire comme un territoire, ce que démontre Alix Desforges dans son article sur les représentations du cyberespace.

Le concept de cyberespace a paradoxalement émergé pour deux raisons radicalement opposées. D'abord apparu sous la plume du romancier de science-fiction William Gibson [984], il décrit un espace tridimensionnel d'une « infinie complexité », généré électroniquement, dans lequel ses personnages entrent en se connectant par ordinateur. Il offre ainsi une représentation mentale des données et de l'information stockées au cœur des systèmes informatiques de toute l'humanité, que s'approprieront des générations d'internautes.

Cette représentation imprègne l'imaginaire des pionniers de l'Internet, qui fondent en 1990, bien avant que l'Internet ne devienne grand public, l'Electronic Frontier Foundation (EFF), référence directe au front pionnier qui, selon la thèse de l'historien Frederick Jackson Turner, a forgé la démocratie américaine. John Perry Barlow, membre fondateur, ira même jusqu'à publier en 1996 une « déclaration d'indépendance du cyberespace », dans laquelle il affirme que le cyberespace possède sa propre souveraineté et que dans cette « civilisation de l'esprit », les lois des gouvernements du monde physique ne s'appliquent pas. Alix Desforges montre comment l'esprit de la contre-culture des années 1960 a inspiré jusqu'à l'architecture même du réseau, conçu dans un esprit d'ouverture, d'autogestion, de liberté des échanges et de l'expression. Fortement décentralisé, dénué de centre, il est pensé pour que l'information puisse toujours circuler, quels que soient les blocages. Ce souffle de liberté apporté par un monde où tout ce qui sort de l'esprit humain peut être « reproduit et distribué à l'infini sans que cela ne coûte rien » continue d'animer nombre d'hacktivistes, qui combattent toute tentative d'entraver la libre circulation de l'information sur l'Internet.

Hérodote, n° 152-153, La Découverte, 2e trimestre 2014.

Tombé quelque peu en désuétude, le terme cyberespace réapparaît à partir des années 2000 dans les discours des États, comme un territoire à conquérir, à contrôler, à surveiller, à se réapproprier. Un territoire sur lequel il faut faire respecter ses frontières, sa souveraineté, ses lois ; et surtout, une menace pour la sécurité nationale et les intérêts de la nation.

Les attaques de 2007 contre l'Estonie ont fait l'effet d'un électrochoc pour nombre de gouvernements, dont la France, qui ont pris brutalement conscience de leur manque de préparation face à de telles menaces. Le déplacement d'une statue à la gloire du régime soviétique à Tallinn a déclenché les hostilités. Les sites gouvernementaux, la défense nationale en particulier mais aussi les banques et autres services publics ont subi une attaque massive en déni de service (DDOS). Des botnets, réseaux de dizaines de milliers d'ordinateurs zombies – c'est-à-dire infectés par un logiciel malveillant qui permet de les piloter à distance à l'insu souvent de leurs utilisateurs –, ont inondé simultanément de requêtes les serveurs du pays jusqu'à la paralysie complète (écran noir), privant les habitants d'accès aux services publics en ligne pendant plusieurs jours pour certains. Le gouvernement russe a nié toute responsabilité malgré le faisceau d'indices techniques et politiques qui convergeait vers le pays. L'année suivante, les cyberattaques contre la Géorgie ont montré comment ces attaques pouvaient venir en appui des forces conventionnelles dans le cadre d'un conflit armé. À partir de là, nombre d'États ont sérieusement renforcé leurs capacités et cherché à accroître leur contrôle et leur puissance dans le cyberespace, à commencer par la France.

Stéphane Dossé, officier du ministère de la Défense, l'affirme on ne peut plus clairement : « Il apparaît donc nécessaire pour les États de "planter le drapeau" dans les espaces qu'ils occupent pour exercer toutes leurs fonctions régaliennes, de coloniser les espaces vierges et de se préparer à affronter des adversaires dans cet espace » [Dossé, 2010]. Le Livre blanc sur la défense 2013 est explicite, le cyberespace est une priorité stratégique et les armes cybernétiques font désormais partie de l'arsenal.

Cyberespace : les États contre-attaquent

Peu d'États avaient anticipé l'enjeu stratégique que pourraient représenter, à terme, l'expansion fulgurante et l'interconnexion des systèmes d'information et de communication. Seuls quelques-uns comme la Russie et la Chine, dont la conscience de l'importance de l'information est historiquement aiguisée, ou encore les États-Unis, à la pointe des avancées technologiques, ont amorcé très tôt une réflexion stratégique. Dans un premier temps, l'innovation est arrivée par des individus et petits groupes entreprenants, astucieux et réactifs, qui ont su

Hérodote, n° 152-153, La Découverte, 2e trimestre 2014.

tirer le meilleur parti de la puissance et la distributivité de ces nouveaux moyens, faiblement régulés. Des individus, des start-up sont à la source de réussites exceptionnelles qui ont profondément transformé nos modes de vie (loisirs, financements collectifs de projets, militantisme, marketing...) et ouvert d'immenses opportunités. Mais des hackers, des criminels, des mercenaires ont tout aussi bien su se saisir très vite et efficacement de ces outils, qui entraînent aujourd'hui la réaction des pouvoirs politiques et institutionnels. Bruce Schneier, expert en sécurité informatique, explique très bien la tension entre pouvoir « distribué » (militants, dissidents, hackers, criminels) et pouvoir « traditionnel » (gouvernements, grandes entreprises, institutions) dans le cyberespace[6]. Il montre comment la forte accessibilité et la décentralisation du système ont initialement privilégié les petits acteurs – y compris malintentionnés –, en leur offrant des capacités de coordination et une efficacité qui semblaient les rendre imbattables. Mais les acteurs traditionnels prennent aujourd'hui leur revanche, avec des moyens et une puissance sans commune mesure, et surtout une solide détermination étant donné les enjeux.

Au nom de la sécurité...

Les États reviennent en force dans le cyberespace au nom de la défense de leurs pouvoirs régaliens. Premièrement, la difficulté à stopper les cyberattaques est susceptible d'affecter leur capacité à assurer la sécurité de la nation et la défense du territoire. Les inquiétudes portent particulièrement sur la protection des infrastructures dites vitales, dont la perturbation ou le sabotage pourrait mettre en danger les populations civiles. La représentation de cette menace alimente les discours les plus catastrophistes, et les débats d'experts sur la possibilité – peu probable, non démontrée mais impossible à exclure – qu'une cyberattaque puisse causer des millions de morts, voire faire tomber un pays. Olivier Kempf interroge la notion de cyberterrorisme, montrant que le rapprochement entre terrorisme et cyberespace n'est pas aussi évident que ce que le discours dominant laisse à penser et masque en partie ce que pourrait être le terrorisme dans le cyberespace. Rodrigo Nieto Gomez analyse la construction de cette représentation américaine et le rôle qu'elle joue dans les politiques sécuritaires, qui tendent à criminaliser le hacker et encourager une culture du secret dans un domaine où, pourtant, l'innovation fait la force.

6. « The battle for power on the Internet : Bruce Schneier at TEDxCambridge 2013 », vidéo publiée le 25 septembre 2013 par TEDxTalks, consultée le 16 février 2013, <www.youtube.com>.

Hérodote, n° 152-153, La Découverte, 2e trimestre 2014.

Au-delà des actes terroristes, l'enjeu de la maîtrise de l'information est crucial. La capacité à collecter, analyser, manipuler l'information peut offrir un avantage stratégique à l'ennemi et le faire douter de la fiabilité de sa propre information. Les cyberattaques peuvent plus directement perturber les communications, désorienter l'ennemi et même affecter ses capacités opérationnelles qui dépendent de plus en plus des réseaux pour leur coordination et leur fonctionnement. Les stratégies classiques de dissuasion et de défense rencontrent des limites, en raison des difficultés d'attribution des attaques – c'est-à-dire la capacité d'identifier à coup sûr qui est derrière une attaque et pourquoi –, mais aussi le faible coût et la forte accessibilité de la technologie, qui renforce le pouvoir de petits acteurs face aux grandes puissances. Les pays les plus dépendants aux réseaux sont à la fois les plus vulnérables aux attaques, mais aussi les plus à même de développer la résilience de leurs réseaux, construire des capacités offensives et saisir les nouvelles opportunités offertes par les réseaux pour accroître leur efficacité et leur puissance.

La guerre idéologique se mène aussi sur les réseaux sociaux alors que, dans nos démocraties, les gouvernements ne peuvent pas toujours ignorer une vive opposition de l'opinion publique avant de s'engager dans un conflit armé ; le djihad offre par ailleurs de véritables kits de radicalisation rapide en ligne et les recettes pratiques du terrorisme individualisé, qui prennent parfois de court les plus grandes puissances.

Deuxièmement, le maintien de la sécurité intérieure et de l'ordre public est mis au défi par la criminalité, organisée ou non, qui opère *via* les réseaux. Il peut s'agir d'intrusions illicites dans les systèmes, de vol ou destruction de données et même, au sens large, de tout acte criminel perpétré *via* les réseaux (braquage de banque, arnaques, usurpation d'identité, etc.). Le problème de l'attribution est renforcé par la volatilité de la preuve. En l'absence d'une intervention rapide, les pièces à conviction peuvent disparaître des écrans. Or la possibilité d'opérer à distance complique le processus d'investigation, d'appréhension et de mise en examen d'un suspect. La criminalité traverse aisément les frontières, *via* les réseaux, ce qui n'est pas le cas des forces de l'ordre. Si le criminel et la victime sont situés dans le même pays, les autorités peuvent agir rapidement. Lorsque le criminel, la victime et/ou les systèmes utilisés sont localisés dans des pays différents, il faut des procédures de coopération internationale au niveau des forces de police et de justice qui sont souvent trop lentes pour être efficaces. Il y a des frontières de juridiction dans le cyberespace et la police ou la gendarmerie ne peuvent s'introduire dans les réseaux étrangers sans autorisation officielle, même pour attraper un criminel.

Les enjeux de sécurité conduisent les gouvernements à surveiller activement ce qui se passe dans le cyberespace, avec les risques de dérives et d'atteinte aux libertés individuelles que l'affaire Snowden a révélés. Pour les États autoritaires, la surveillance et le contrôle du cyberespace sont essentiels à la protection de leur régime car la menace principale est susceptible de venir de l'intérieur. La

Hérodote, n° 152-153, La Découverte, 2e trimestre 2014.

circulation accrue de l'information peut affaiblir les régimes autoritaires, mais les réseaux sont aussi de formidables outils pour détecter, identifier, surveiller les dissidents ou les éventuelles brebis galeuses du régime. L'article sur la Chine (Frédérick Douzet, *infra*) montre comment le régime a su, jusqu'ici, faire preuve de créativité pour s'adapter à ces nouveaux défis.

Enjeux de souveraineté

L'entretien avec Bertrand de La Chapelle, fondateur du projet Internet et Juridiction, souligne à quel point l'exercice de la souveraineté est devenu plus complexe pour les États, car les limites de juridictions sont plus floues et plus entremêlées dans le cyberespace. Les activités sont transfrontières dans le cyberespace, et il est parfois difficile pour un État de faire respecter ses lois et régulations, même sur son territoire et par ses citoyens, particulièrement lorsque le service utilisé est fourni par une entreprise étrangère. Ce qui constitue une juridiction dans le cyberespace est bien souvent le produit de rivalités de pouvoir plutôt que d'une définition juridique consensuelle. Un conflit récurrent touche à la protection de la liberté d'expression, qui connaît des restrictions en France irrecevables au regard de la loi américaine. En 2012 par exemple, des commentaires antisémites postés en français sur Twitter, dans un concours de blagues nauséabondes sous le mot clé (*hashtag* dans le jargon) #UnBonJuif, a conduit à un véritable bras de fer entre la justice française et l'entreprise américaine. Il a fallu dix mois de procédure pour que Twitter accepte de livrer à la justice française les données pouvant permettre l'identification de certains auteurs. Les grandes entreprises de l'Internet – les fameux GAFA (Google, Amazon, Facebook, Apple) – ont acquis une telle puissance économique qu'elles peuvent se permettre de jouer le rapport de force et ne se soumettent pas si facilement à la justice d'un État qui réclame la suppression de contenus ou des informations sur les utilisateurs. Face à des régimes autoritaires, la protection des utilisateurs peut s'avérer salutaire mais coûter à l'entreprise l'accès à un marché profitable.

Enfin, la souveraineté économique et financière des États est mise à rude épreuve. Les réseaux accélèrent considérablement la circulation des biens et des flux financiers, ce qui facilite l'évasion fiscale et la propagation de crises financières internationales. L'article de Dominique Lacroix montre par ailleurs la concentration dans des paradis fiscaux d'entreprises candidates aux nouveaux noms de domaines. La réorganisation des activités de Yahoo ! en Europe autour de l'entité irlandaise (où l'impôt sur les sociétés s'élève à 12,5 %[7]) pourrait conduire à

7. À titre de comparaison, l'impôt sur les sociétés dont le capital est détenu à moins de 75 % par des personnes physiques est de 33,1 % pour l'ensemble de ses bénéfices (<impots.gouv.fr>).

Hérodote, n° 152-153, La Découverte, 2e trimestre 2014.

un transfert de la base imposable de différentes entités européennes de l'entreprise. Les réseaux augmentent aussi le risque et l'ampleur de l'espionnage économique, du vol de propriété intellectuelle et industrielle, ou encore des secrets d'affaires. Danilo D'Elia analyse ces risques et montre le potentiel de conflits géopolitiques qu'ils recèlent. Il en va de la puissance économique et financière des nations, au point que les intérêts du secteur privé rejoignent ceux de la nation et que la cybersécurité des entreprises puisse relever de l'intérêt national. Il va sans dire que le marché de la cybersécurité est aussi sensible que florissant, ce qui encourage également les gouvernements à s'impliquer.

Des menaces nouvelles ?

Nombre de ces menaces ne sont pas nouvelles mais elles se propagent dans le cyberespace de façon plus diffuse, rapide, puissante et à une échelle inédite. Qu'il s'agisse des quantités d'informations dérobées aux entreprises par les hackers chinois (selon le rapport Mandiant), des 1,7 million de fichiers emportés par Snowden, des masses invraisemblables de données collectées par la NSA ou des 30 000 ordinateurs de la société Aramco sabotés d'un coup en 2012... les conséquences arrivent plus vite, plus fort et sont parfois d'une ampleur sans précédent.

Certains défis, en revanche, sont propres au cyberespace : la difficulté à identifier et prouver l'origine d'une attaque ; la difficulté à l'anticiper, à la prévenir ou la stopper ; l'enchevêtrement de souveraineté et de juridictions ; l'évolution rapide de la technologie et la reconfiguration permanente des réseaux, qui nécessitent une adaptation rapide et constante à l'évolution du milieu ; la possibilité de développer des armes cyberexpérimentales ; la difficulté à tester ces armes en grandeur nature ; l'incertitude quant à leurs effets, qui dépendent aussi de la capacité de la cible à résister ; le fait que la meilleure attaque reste celle que l'on ne détecte pas... Le cyberespace est défini par plusieurs pays comme un nouveau domaine (ou milieu) militaire, à côté de la terre, la mer, l'air et l'espace. Mais contrairement aux autres, ce n'est pas un milieu naturel – tout ce qui s'y passe est le produit de l'action humaine – et il est transverse à tous les autres domaines.

Dès lors, les stratégies développées par les États pour défendre leurs pouvoirs régaliens et maximiser leur puissance dans le cyberespace ont des conséquences géopolitiques dont il faut se préoccuper. Elles soulèvent en retour de sérieuses questions, voire de nouvelles menaces.

Pourquoi faire de la géopolitique du cyberespace

Les ramifications techniques des conflits du cyberespace ont de quoi décourager les citoyens – et les chercheurs en sciences humaines et sociales –, et ce n'est pas un hasard si ces questions sont longtemps restées aux mains d'une petite communauté d'experts. Pourquoi s'y intéresser malgré tout ? Parce qu'il s'agit du monde dans lequel on a envie de vivre. Parce qu'en raison de l'omniprésence des systèmes d'information et de communication dans nos vies quotidiennes, les décisions qui seront prises affecteront tous les aspects de notre vie. Parce qu'un certain nombre de pouvoirs se sont développés sans que soient discutés les contre-pouvoirs, les garde-fous, les processus de contrôle démocratique.

Nous sommes à un tournant et beaucoup d'entre nous, y compris nombre de nos élus, découvrent les outils, les programmes, les politiques que les grandes entreprises, les gouvernements ou encore les criminels ont développés pour défendre leurs intérêts et maximiser leur puissance ou leurs profits dans le cyberespace. Les anciens paradigmes stratégiques et règles du jeu internationales semblent inadaptés, mais les nouveaux restent à écrire. La vitesse des évolutions technologiques dépasse largement celle de l'élaboration d'un consensus international, d'un nouveau cadre juridique ou de l'adaptation des lois. La culture du secret et le manque de confiance entre les partenaires ralentissent ces efforts. Nous sommes à la croisée des chemins et celui que nous choisirons de suivre est susceptible d'avoir des implications majeures pour notre futur. Trois domaines en particulier méritent notre attention.

Paix et sécurité collective

Le premier enjeu est celui de la paix et de la sécurité collective. Plusieurs articles de ce numéro montrent à quel point l'inflation de la représentation de la menace domine le débat. L'approche des États-Unis, en particulier, est caractérisée par une escalade des discours et des moyens, dont l'un des moteurs est la rivalité avec la Chine. Dans une stratégie claire d'acquisition d'une suprématie informationnelle, le régime chinois collecte par tous les moyens – licites et illicites – l'information technologique, industrielle, économique, politique et militaire, ce qui suscite de vives inquiétudes aux États-Unis (voir l'article F. Douzet).

Au cours des deux dernières années, une avalanche de révélations dans la presse, de déclarations d'experts, de membres du Congrès et même de la Maison-Blanche a exposé les risques liés aux cybermenaces pour la sécurité et la prospérité de la nation, avec des accusations de plus en plus directes à l'égard de la Chine. Le directeur du renseignement, Jim Clapper, a même déclaré devant une commission

Hérodote, n° 152-153, La Découverte, 2e trimestre 2014.

du Sénat que la menace cyber était sur le point devenir plus importante que la menace terroriste pour la nation.

Malgré les restrictions fédérales généralisées, le budget de la cyberdéfense a augmenté de 800 millions de dollars en 2013 et le UC Cyber Command[8], créé en 2010, devrait voir ses effectifs passer de 900 à 4 900 employés dans les années à venir. L'affaire Snowden a montré à quel point les États-Unis ont agressivement collecté des masses d'information par les réseaux, au péril de la confiance et de la coopération qu'ils avaient construites avec d'autres nations. James Lewis relativise toutefois la portée des révélations, qui n'étaient pas une surprise pour les Chinois ou les Russes, et qui ne remettraient pas en question fondamentalement les négociations internationales. La question de la confiance reste épineuse, alors que beaucoup d'officiels aiment à répéter l'adage selon lequel « il n'y a pas d'amis dans le cyberespace ».

Les États-Unis seraient aussi à l'initiative de ce que beaucoup considèrent comme le premier acte de « cyberguerre », une attaque expérimentale, sorte de troisième voie entre la diplomatie coercitive et l'attaque armée. En 2012, David Sanger dans le *New York Times* a révélé comment le virus Stuxnet, élaboré en collaboration avec les services israéliens, aurait infecté les centrifugeuses de Natanz, afin de ralentir le programme nucléaire de l'Iran.

Les révélations de ces deux dernières années et des déclarations récentes laissent à penser que la course aux cyberarmes a commencé. Plusieurs pays ont récemment mis l'accent sur le développement de leur cyberdéfense et de leurs cybercapacités. La France et la Grande-Bretagne ont annoncé courant 2013 le développement de capacités offensives. En 2011, les États-Unis – et la France en 2013 – ont clairement affirmé qu'une cyberattaque de grande ampleur pourrait être considérée comme un acte de guerre et qu'ils se réserveraient le droit de répliquer par tous les moyens. Les Russes dénoncent la militarisation du cyberespace tout en développant leurs propres capacités.

L'article de Martin Libicki, chercheur à la RAND Corporation et auteur de travaux pionniers sur la dissuasion dans le cyberespace, pointe le potentiel d'escalade des conflits en cas de réponse conventionnelle à une cyberattaque. Les dégâts seraient selon lui plus limités si les représailles restaient dans le cyberespace, ce qui serait certes moins dissuasif. Oriane Barat-Ginies, docteure en droit international, présente au contraire les arguments des experts auteurs du *Manuel de Tallinn*, une série de recommandations juridiques sur l'applicabilité du droit international au cyberespace, qui justifie la légitime défense et le recours aux armes conventionnelles en réponse à une cyberattaque qui constituerait une agression armée.

8. Unité militaire de cyberopérations et de la NSA.

Le risque d'escalade est à prendre au sérieux car, comme le montrent ces deux articles, il n'y a aucune garantie qu'un conflit qui commence dans le cyberespace reste dans le cyberespace. On connaît par ailleurs mal les effets collatéraux des cyberarmes et l'idée de « frappes chirurgicales » dans le cyberespace, énoncée par des officiels américains, est préoccupante.

Dans ce contexte, les analogies avec l'ambiance de la guerre froide se multiplient. Dans *Foreign Policy*, David Rothkopf avance même l'idée d'une guerre « cool », un peu plus chaude et plus « branchée » que la guerre froide : « Le but de la guerre *cool* serait de pouvoir frapper constamment sans déclencher de guerre chaude tout en rendant les guerres chaudes moins désirables [...] ou même nécessaires » [Rothkopf, 2013].

Faut-il recréer des alliances de type guerre froide (ou *cool*) ? Faut-il partager la vision pessimiste des relations internationales comme un jeu à somme nulle et monter en capacités ? Ou bien est-ce une nouvelle opportunité de repenser les cadres de la sécurité collective, en impliquant des pays comme la Russie et la Chine ? Les deux pays ont montré la volonté de coopérer dans l'élaboration de règles internationales mais de fortes divergences de vues persistent, comme le montre James Lewis. L'article de Martin Libicki montre que la réflexion stratégique pour prévenir l'escalade est indispensable mais complexe et que le débat est loin d'être tranché.

La question est aussi quel cadre de sécurité collective est-on capable de construire ? L'Europe de la défense était déjà difficile, celle de la cyberdéfense l'est plus encore. Le partage des capacités est perçu d'abord comme un abandon de souveraineté, étant donné le caractère sensible de la technologie et ce qu'elle peut révéler des forces et des vulnérabilités. Jean-Loup Samaan et Vincent Joubert montrent que l'Union européenne et l'Otan ont intégré ces questions dans leurs priorités stratégiques et pris des initiatives parallèles. Mais la répartition des rôles et des compétences reste floue, il n'y a pour l'instant guère de coordination entre les deux institutions et la limite de souveraineté semble bien difficile à dépasser. Les disparités sont très importantes en termes de capacités entre les pays alliés et les nations qui disposent des moyens les plus avancés considèrent qu'il s'agit d'un domaine de souveraineté nationale et cultivent en priorité leurs relations bilatérales dans le domaine, en particulier avec les États-Unis.

La discussion transatlantique est compliquée par les enjeux économiques, qui sont indissociables. L'affaire Snowden a jeté une lumière crue sur la dépendance des États européens à l'égard des grandes entreprises américaines pour leurs données (accessibles par le gouvernement), et leurs équipements, pour lesquels la principale alternative – bien plus problématique – est la Chine. Certains pointent la naïveté des Européens, qui se posent aujourd'hui la question de leur souveraineté dans le cadre de l'ouverture des marchés économiques. Peut-on construire la

Hérodote, n° 152-153, La Découverte, 2e trimestre 2014.

cybersécurité pour la prospérité économique de l'Europe indépendamment de la cyberdéfense ? Que peut l'Europe à travers les régulations, les normes techniques, les politiques industrielles pour améliorer sa cybersécurité ? Quelle alternative aux équipements chinois ou américains ? Les marchés nationaux semblent trop restreints pour être compétitifs mais comment construire la confiance entre les nations pour développer des solutions politiques et industrielles communes ? Peut-on et doit-on développer une offre souveraine ?

Ces questions sont pressantes car – au-delà des menaces sécuritaires – la masse de données numériques est en expansion continue. Comment les protéger ? Et de qui ?

Démocratie et libertés individuelles

De plus en plus de données personnelles seront accessibles en ligne, plus ou moins ouvertement. Avec l'Open Data (« ouverture des données »), toutes sortes de données publiques, issues des administrations, deviendront à terme accessibles, offrant de nouveaux outils d'information et de transparence susceptibles d'améliorer le fonctionnement de la démocratie. On peut espérer que la France, en particulier, où la communication des données publiques est loin d'être un acquis, bénéficie de ce mouvement d'ouverture. Mais, à côté des risques de divulgation criminelle ou accidentelle des données personnelles, se pose la question de l'accès des entreprises et des gouvernements.

S'il y a au moins une chose sur laquelle tout le monde s'accorde à propos d'Edward Snowden, c'est qu'il a lancé un débat qui n'aurait sinon probablement pas eu lieu. Les lanceurs d'alerte qui avaient précédemment tenté d'attirer l'attention sur les pratiques de la NSA n'avaient pas reçu beaucoup d'échos. Il a fallu cette déflagration d'ampleur planétaire pour que la prise de conscience du public en fasse une question politique et que le traumatisme des attentats du 11 septembre 2001 ne suffise plus à occulter le débat. La question est désormais posée : comment concilier démocratie et surveillance ?

Les processus de contrôle démocratique en la matière sont largement inconnus de la plupart des citoyens – voire des élus – et visiblement, aux États-Unis, malgré des procédures très encadrées (au moins sur le papier), ils ont dysfonctionné. Beaucoup considèrent, et les débats juridiques font rage, que le gouvernement a outrepassé ses droits et empiété sur les libertés civiles des citoyens. Si la fatalité semble l'emporter dans les réactions françaises, l'opinion publique allemande est très mobilisée. Les souvenirs de la Stasi ne sont pas si lointains. Le secret est souvent revendiqué par les acteurs du renseignement pour préserver l'efficacité des investigations mais, dans nos sociétés actuelles, il devient de plus en plus difficile

Hérodote, n° 152-153, La Découverte, 2e trimestre 2014.

de garder des secrets, même pour les gouvernements, et Snowden risque bien de faire des émules...

Penser les garde-fous, débattre des procédures de contrôle démocratiques (qui décide, où, de quoi, quand ?), mettre en place des procédures d'évaluation de ces programmes de surveillance (financés avec de l'argent public) permet non seulement de préserver les libertés individuelles, les valeurs mêmes de la démocratie, mais participe aussi à leur assurer plus de légitimité.

L'enjeu est de taille. Notre dossier médical, nos opinions politiques, nos résultats scolaires, notre orientation sexuelle, nos achats, nos déplacements, nos amis, les amis de nos amis, les amis des amis de nos amis... toutes ces informations et bien d'autres peuvent faire l'objet d'investigations, de recoupements et permettre d'établir un profil d'une précision redoutable. Et beaucoup de ces informations sont déjà accessibles, souvent même mises à disposition volontairement par les utilisateurs des réseaux sociaux et des blogs.

La question des garde-fous se pose clairement pour les entreprises, qui ne sont pas soumises au contrôle démocratique mais seulement à la loi, et parfois à la collaboration forcée avec leur gouvernement. Là encore le compromis mérite réflexion entre les avantages indéniables de l'exploitation des données par les entreprises, qui analysent nos goûts, mémorisent nos choix et nous proposent des services sur mesure, et les atteintes potentielles aux libertés.

Ces débats se jouent sur fond d'énormes enjeux économiques. L'article de Stéphane Grumbach et Stéphane Frénot, chercheurs à l'Inria, montre à quel point la capacité à collecter mais aussi croiser, analyser, exploiter les données est devenue le moteur de l'économie de nos sociétés. La domination des entreprises américaines dans les services en ligne, alliée à leur savoir-faire dans le traitement des données et à la puissance américaine pour imposer des normes techniques, leur offre un avantage stratégique indéniable pour les marchés d'ouverture des données publiques à venir. Là encore, les enjeux de souveraineté sont palpables et l'affaire Snowden risque de compliquer les négociations des accords de libre-échange. Pour autant, ils ne seront pas remis fondamentalement en question et la balle est dans le camp des Européens qui, contrairement à certains émergents, n'ont pas produit de champions de l'Internet.

Là encore se pose la question de l'Europe et de la capacité des États membres à s'unir pour créer un levier économique et politique face aux géants de l'Internet. La réforme de la loi européenne de protection des données personnelles permettrait d'harmoniser le patchwork de législations nationales européennes, favorisant la mobilité des entreprises en Europe, et permettrait de renfoncer la protection des citoyens. Elle prévoit par exemple d'imposer aux entreprises qui collectent des données personnelles le consentement explicite des utilisateurs, le droit à l'oubli (la possibilité d'effacer les données) ou encore une agence unique pour gérer les

litiges. Malgré l'affaire Snowden, la proposition de réforme a été renvoyée en 2015, suite à un lobbying particulièrement intensif des grandes entreprises américaines et de sérieuses divergences entre les États membres. Le chantier est encore vaste...

Le futur de l'Internet

Enfin, les stratégies nationales contribuent à façonner l'Internet et là encore les enjeux sont importants. Suite aux révélations sur la surveillance massive, y compris de son propre téléphone, la présidente du Brésil Dilma Rousseff a exprimé le souhait de se séparer de cet Internet trop américain (*U.S. Centric-Internet*) et appelé à l'organisation d'un Sommet sur la gouvernance de l'Internet au Brésil, en avril 2014. Bertrand de La Chapelle en évoque les enjeux dans son entretien. Ebert Hannes et Tim Maurer montrent que les pays émergents, dont le nombre d'utilisateurs d'Internet est en forte croissance, vivent mal la suprématie américaine sur l'architecture et la gouvernance de l'Internet – et la domination dans les équipements, les services, les contenus et la gestion des données – et développent des stratégies pour accroître leur influence. Les BRICS, en partenariat une vingtaine d'États africains, ont même lancé le projet de leur propre câble sous-marin de 32 000 km, reliant la Russie, Chine, Inde, Afrique du Sud, Brésil (les BRICS) et États-Unis. Mais les BRICS ne sont pas un groupe homogène et ne partagent pas tous les mêmes traditions démocratiques, comme le montre l'article d'Hannes Ebert et Tim Maurer.

Nombre d'États démocratiques s'inquiètent des enjeux de la « balkanisation de l'Internet », une fragmentation physique et politique du réseau qui lui ferait perdre son caractère libre et ouvert à l'origine de son succès. La Chine, la Russie, l'Iran, l'Arabie saoudite, la Corée du Nord ont mis en place des stratégies pour contrôler leurs réseaux, de l'infrastructure physique jusqu'aux contenus en circulation. L'article de Kevin Limonier montre très bien les représentations et les stratégies mises en œuvre par la Russie pour défendre la conception d'un Internet souverain. Ces États font la promotion d'un contrôle de l'Internet par les États au sein de l'Union internationale des télécommunications. Les négociations internationales achoppent régulièrement sur deux points cruciaux, que les États occidentaux mettent en avant : le respect des droits de l'homme (liberté d'expression, accès à l'information, respect de la vie privée) et l'implication d'acteurs non étatiques dans un modèle de gouvernance multipartite, comme l'explique Bertrand de La Chapelle. Pour la Chine, la Russie et d'autres, ces questions relèvent exclusivement de la souveraineté des États. Et l'intérêt économique et politique à rester connectés est suffisamment fort pour que, jusqu'ici, la structure commune de base ne soit pas remise en question.

Les révélations sur les programmes de la NSA, la montée au créneau de pays démocratiques émergents comme le Brésil et l'Inde et les efforts de l'Icann[9] pour prendre en compte les revendications régionales font désormais bouger les lignes. L'enjeu est celui du futur de l'Internet. Comment faire de la place pour toutes les nations et créer un environnement suffisamment sûr pour maintenir le caractère libre et ouvert des réseaux ?

Conclusion

Le cyberespace est ainsi devenu à la fois un enjeu de rivalités de pouvoir entre acteurs, un théâtre d'affrontement et une arme redoutable dans les conflits géopolitiques. Les conflits pour le cyberespace ou dans le cyberespace ne sont pas dissociables des rivalités de pouvoir géopolitiques classiques. Ils en sont, au contraire, à la fois l'expression et une nouvelle dimension, présente à tous les niveaux d'analyse, à prendre en compte dans une approche multiscalaire.

Les enjeux géopolitiques du cyberespace sont intimement mêlés à des considérations politiques, économiques, sociales et culturelles. Par son approche multiscalaire et sa transdisciplinarité, qui de fait s'ouvre à l'informatique, voire aux mathématiques, la géopolitique permet d'aborder ces questions dans toute leur complexité.

La dimension technique des débats demandera sans aucun doute un effort particulier au lecteur. Mais le jeu en vaut la chandelle. Car il ne s'agit pas seulement d'enjeux de puissance et de sécurité dans le cyberespace, mais aussi des valeurs que nous défendons en tant que nation démocratique ; les valeurs que nous voulons voir gouverner le monde que nous construisons.

Bibliographie

CATTARUZZA A. et DOUZET F. (2013), « Le cyberespace au cœur de tensions géopolitiques internationales », *DSI,* hors-série n° 32.

DESFORGES A. (2013), « Les frontières du cyberspace », *in* DOUZET F. et GIBLIN B. (dir.), *Des frontières indépassables ?*, Armand Colin, Paris.

DOSSÉ S. (2010), « Vers une stratégie de milieu pour préparer les conflits dans le cyberespace ? », *DSI*, n° 59, mai.

DOUZET F. (1997), « Internet géopolitise le monde », *Hérodote,* n° 86/87, p. 222-233.

–, (2007), « Les frontières chinoises de l'Internet », *Hérodote,* n° 125, p. 127-142.

9. L'Internet Corporation for Assigned Names and Numbers (Icann) est l'organisation qui coordonne le système d'addresses Internet et de noms de domaine (<www.icann.org>).

–, (2013), « Chine, États-Unis : la course aux cyberarmes a commencé », *Sécurité globale*, n° 23.
–, (2013), « Chine : cyberstratégie, l'art de la guerre revisité », *Diploweb,* 12 septembre (<www.diploweb.com>)
GIBSON W. (1984), *Neuromancer,* Ace, New Jersey.
KEMPF O. (2012), *Introduction à la cyberestratégie*, Economica, Paris.
LACOSTE Y. (dir.) (1993), *Dictionnaire de géopolitique*, Flammarion, Paris.
LACOSTE Y. (2003), *De la géopolitique aux paysages, dictionnaire de la géographie*, Armand Colin, Paris.
MATTELART A. (2009), *Histoire de l'utopie planétaire. De la cité prophétique à la société globale*, La Découverte, Paris.
MCLUHAN M. (1964), *Understanding Media. The Extensions of a Man*, McGraw-Hill, New York.
MUSSO P. (2003), *Critique des réseaux*, PUF, Paris.
ROTHKOPF D. (2013), « The cool war », *Foreign Policy*, 20 février.
SANGER D. (2013), « In cyberspace, new cold war », *New York Times,* 24 février.
VIRILIO P. (1997), « Un monde surexposé », *Le Monde diplomatique,* août.