(2) GEOPOLITIQUE D'INTERNET et du WEB. Souveraineté numérique, enjeu géopolitique, Internet sécessionniste. Par L. GAYARD

La souveraineté numérique, enjeu géopolitique. un internet sécessionniste ?

lundi 30 mars 2020, par GAYARD

DEUXIEME PARTIE - LA SOUVERAINETE NUMERIQUE, ENJEU GEOPOLITIQUE. UN INTERNET SECESSIONNISTE ?

I – La souveraineté numérique, enjeu géopolitique

Si la proposition de réforme chinoise du DNS n'a pas abouti en 2013, cela n'a pas empêché l'Empire du Milieu de se donner les moyens de cadenasser en partie le cyberespace chinois sans pour autant se couper d'Internet. Le « Grand Pare-feu national », ou encore « Grand Firewall » ou « Muraille de Chine virtuelle » sont autant de sobriquets désignant le projet « Bouclier doré », développé par le gouvernement chinois à partir de 1998 et mis en place à partir de 2003. L'arrivée d'Internet en Chine suscitait tout autant l'intérêt que les craintes des instances centrales du Parti Communiste chinois. Il s'agissait donc de créer un outil qui permette de contrôler l'accès des internautes chinois au réseau mondial sans pour autant s'en couper complètement. Le « Bouclier doré » est donc constitué de pare-feux (firewall) informatiques et de serveurs proxy [1] qui permettent de filtrer les flux de données en provenance de l'étranger, en particulier les sites d'informations et les réseaux sociaux non-chinois qui sont extrêmement surveillés, voire bloqués. Le « Grand Pare-feu » chinois a ses failles. Il peut même engendrer quelques conséquences contre-productives. Ainsi, le soudain blocage d'Instagram en Chine le 29 septembre 2014 a précipité l'usage des outils de contournement chez les utilisateurs du réseau social, une frange des internautes chinois pas vraiment politisés mais qui, en se mettant à utiliser massivement des VPN [2] pour accéder à nouveau à leur compte Instagram, ont pu au passage avoir accès à des sites et applications bannis depuis plus longtemps, comme Facebook, Youtube ou Twitter ou un grand nombre de pages Wikipédia [3]. En dépit de ses ratés, le gouvernement chinois a néanmoins réussi à établir son contrôle sur Internet, sans empêcher le secteur de l'économie numérique chinoise de devenir florissant. Comme l'a montré la chercheuse Margaret E. Roberts dans son ouvrage Censored, publié en 2018 chez Princeton, la stratégie chinoise ne consiste pas à interdire l'accès à Internet hors de Chine mais à le gêner le plus possible… et à développer des alternatives nationales qui permettent de dissuader les internautes d'aller voir ailleurs si l'herbe est plus verte [4].

C'est tout le paradoxe chinois : parvenir à instaurer – avec son « Grand pare-feu national » - un système de filtrage d'Internet à très grande échelle tout en devenant sur le plan mondial un acteur majeur de l'économie numérique, capable de concurrencer les GAFA avec ses propres géants que sont les BATX (Baidu, Alibaba, Tencent, Xiaomi… pour ne citer qu'eux). La République Populaire de Chine et les Etats-Unis se partagent maintenant quasi exclusivement une domination mondiale que les Européens sont bien en peine de leur contester. En 2017, parmi les vingt premières tech companies au monde, on ne comptait que des firmes américaines ou chinoises : Apple, Google, Microsoft, Amazon, Facebook pour les cinq premières et les Chinois Tencent, Alibaba et ICBC après elles, selon le rapport « Mary Meeker. "Internet Trends 2017" ». En 2019, les dix premières capitalisations boursières (toute activité confondue) sont celles d'Apple, Microsoft, Amazon, Alphabet, Berkshire Hathaway (un conglomérat d'investissement américain), Facebook, Alibaba, Tencent Holdings, JPMorgan Chase et Johnson&Johnson (entreprise pharmaceutique américaine). On notera cependant que, parmi les dix plus importantes entreprises d'informatique et producteurs de logiciels au monde, aux côtés des inévitables Microsoft et IBM en première place, on trouve aussi les géants indiens Infosys et Tata Consultancy Services et le français Cap Gemini.

Il n'en reste pas moins que les Etats-Unis, patrie d'Internet, restent largement en avance dans le domaine de l'économie numérique, s'appuyant sur l'attractivité et les capacités d'innovation de la Silicon Valley et sur la puissance d'entreprises telles que Google. Comme le remarque Shoshanna Zuboff dans son ouvrage The Age of Surveillance Capitalism [5], Google joue au XXIe siècle le rôle qui était celui de Ford au début du XXe siècle, celui d'un acteur capable d'imposer les règles du jeu dans une révolution technologique aux innombrables conséquences. Mais à cette différence près que Google n'a, dans son secteur, pas de concurrent réel et a colonisé un marché immense à la manière « d'une espèce invasive dans un environnement libre de tout prédateur naturel. » A l'heure actuelle, 92% des requêtes effectuées sur un moteur de recherche dans le monde le sont sur Google [6]. Le géant chinois Baidu arrive encore loin derrière avec 1,5%, suivi par le Russe Yandex avec 0,6%. Quant au français Qwant, sa part de marché est tellement infime qu'elle n'est pas comptabilisée dans les dix premiers mondiaux. En France, le moteur de recherche français représente en 2019 0,84% des parts de marchés. On peut aussi mettre en avant le fait que le développement historique d'Internet aux États-Unis a doté la première puissance mondiale d'infrastructures physiques – réseaux de serveurs, câblage et centres de données – lui permettant d'assurer largement sa souveraineté numérique.

Le continent européen se trouve, lui, dans une situation de dépendance encore importante en la matière. Pour combler ce retard, l'Union Européenne a lancé en 2014 le « Projet Horizon 2020 », auquel elle compte allouer 80 milliards d'euros sur une période de sept ans, afin de financer la recherche et le développement dans les secteurs de pointe et notamment celui de l'économie numérique. Cela peut-il suffire pour autant à combler le retard européen dans ce domaine ? L'Europe reste une terre d'innovation mais les investissements dans le secteur du numérique font encore pâle figure face à ceux des États-Unis et aux géants du numérique que sont Google ou Apple. Si Emmanuel Macron considérait en 2015 le moteur de recherche Qwant comme le « Google français », il faut rappeler que le moteur de recherche tricolore lancé en 2013 annonçait avoir dépassé les dix milliards de requêtes en 2017 quand Google revendiquait la même année 3,3 milliards de requêtes… par jour [7]. L'entrée en vigueur du Règlement Européen sur la Protection des Données (RGPD) le 25 juillet 2018 illustre la volonté de l'Union Européenne de défendre un peu mieux sa souveraineté numérique. Les Européens ont beau avoir inventé le world wide web, la supériorité américaine reste écrasante dans les trois dimensions d'Internet : 1) la couche logicielle évidemment, visible à travers le monopole exercé par des sociétés comme Google ou Facebook, 2) la dimension physique ensuite, avec la géopolitique des câbles, mais aussi celle des centres de

données, puisque avec 1 252 centres de données sur leur territoire, les Etats-Unis disposent, selon le centre d'étude privé Xerfi, de plus de 45% du parc de centres de données dans le monde, trois fois plus à eux seuls que les trois suivant – le Royaume-Uni, l'Allemagne et la France – totalisant à eux trois 512 centres de données, 3) la dimension logique enfin. Internet est surnommé le « réseau des réseaux » pour une bonne raison. Il est divisé en un certain nombre de sous-réseaux qui orientent les flux de connexions mondiaux. Comme le note une étude du MIT publiée en 2009, « la véritable histoire de l'infrastructure de routage d'Internet est que ce service est fourni par un grand nombre d'organisations commerciales, généralement en compétition les unes avec les autres. (…) , les fournisseurs d'accès à Internet coopèrent afin d'assurer une connectivité globale pour leurs réseaux de clients respectifs. Un aspect important est que ces fournisseurs d'accès ne sont pas égaux ; ils présentent une grande variété de tailles et de structures internes. » [8] Ces fournisseurs d'accès garantissent l'accès à Internet pour les particuliers mais également pour de larges sous-réseaux qui représentent des entités commerciales, des institutions publiques et différents types d'organisations. Pour reprendre les termes du spécialiste Laurent Bloch : « L'Internet n'est pas un réseau unique, mais, comme son nom l'indique, un réseau de réseaux. Chacun de ces réseaux est la propriété d'un opérateur (ou FAI, pour Fournisseur d'accès à l'Internet, en anglais ISP, pour Internet Service Provider) différent, qui l'administre à sa façon. Un réseau administré de façon unique par un FAI est un AS (Autonomous System). Si l'on compare l'Internet à un continent, les AS en sont les pays, séparés par des frontières, avec chacun sa législation. » [9] En général ces AS ou « systèmes autonomes » font appel à des sociétés spécialisées dans l'hébergement de données et le cloud computing [10] pour stocker leurs données. Le Massachussetts Institute of Technologies américain représente par exemple un énorme système autonome fait appel pour stocker et rendre accessibles ses données en ligne aux services de la multinationale Akamai (« intelligent » en hawaïen) qui dispose de 100 000 serveurs répartis dans plus d'une centaine de pays différents. Nous sommes ici à une autre échelle qu'OVHCloud cité précédemment. Les différents « continents » et « pays » d'Internet communiquent entre eux grâce à des portails dénommés BGP (Border Gateway Protocol), qui permettent l'interconnectivité des FAI, et IGP (Internet Gateway Protocol) qui permettent aux AS de communiquer entre eux. Les fournisseurs d'accès américains – comme AT&T ou Verizon – sont de véritables géants du net, mais s'ils se heurtent à la concurrence de fournisseurs d'accès nationaux dans d'autres Etats – comme Orange en France - ils disposent en revanche d'un levier d'influence très efficace, puisque les Etats-Unis concentrent encore une bonne partie de ces portails et nœuds de connexion qui permettent aux grands continents du cyberespace de communiquer entre eux. Autrement dit, ils disposent encore des infrastructures physiques qui permettent d'aiguiller les flux de données au niveau mondial et de les contrôler. Pour ce qui est du stockage de données et du « cloud computing », les Etats-Unis sont encore en position de domination. Les entreprises qui contrôlent ce secteur sont aussi en très grande majorité américaines.
Deux exceptions notables sont à souligner avec la Chine et la Russie. La première, en plus de son « Pare-feu national », a fini, si elle n'a pu obtenir de l'ICANN la révolution du DNS qu'elle souhaitait, par obtenir l'attribution de sa propre racine DNS. Tout site, y compris étranger, consulté en Chine, est en réalité une version sinisée, hébergée sur le DNS chinois et dotée d'une extension en .cn. Il faut obligatoirement utiliser un VPN pour accéder aux véritables versions des Google, Facebook et consorts. La Russie, par ailleurs est un Etat qui a profité du développement précoce d'une infrastructure réseau solide, depuis les travaux pionniers du projet Démos et de Telkom, durant la guerre froide, ayant donné naissance à ce que l'on nomme aujourd'hui le « RUNET », l'Internet Russe, qui se trouve régulièrement mis en cause pour son usage de l'arme informatique, notamment lors des cyberattaques contre l'Estonie en 2007 et jusqu'aux soupçons d'ingérence dans les campagnes présidentielles américaine ou française en 2016 ou 2017. Ces exemples peuvent être complétés par celui du projet d'Internet « national » iranien et enfin l'exemple des darknets, réseaux alternatifs protégés par des technologies de chiffrage complexes.

II - Un Internet sécessionniste ?

Si la proposition chinoise de mise en place de DNS « nationaux » avait abouti en 2013, cela aurait sûrement conduit à une réelle fragmentation du réseau mondial. Pour autant, de nos jours, cette « fragmentation » peut être également initiée par les tentations de sécession et de constitution d'Internet nationaux par certains Etats. Si les exemples Chinois et Russes s'avèrent déjà assez connus, il peut être intéressant d'évoquer celui de l'Iran, moins fréquemment mis en lumière. En août 2013, Mahmoud Vaezi, Ministre de la Communication en Iran de 2013 à 2017, dévoila le projet d'Internet – ou plutôt d'Intranet – national iranien, ou SHOMA. La brève description qu'en donna le ministre précisa les éléments suivants : Shoma devait être considéré comme un réseau parallèle à Internet reposant sur des infrastructures nationales : centres de données, câbles, routeurs et serveurs installés sur le territoire iranien. L' « Internet national » déjà évoqué par Mahmoud Ahmedinejad, avant son remplacement par Hassan Rohani en 2013, était censé se diviser en deux composantes : l'une confidentielle et sécurisée à l'usage du gouvernement, l'autre, publique, destinée à proposer à la population l'usage d'un véritable « Internet hallal », comme les médias occidentaux avaient commencé à le surnommer. SHOMA n'était pas censé entrer en compétition avec Internet, auquel les Iraniens devaient toujours avoir accès, du moins de manière filtrée.
Le développement du projet SHOMA a démarré au début de l'année 2006, supervisé par le Département des Technologies de l'Information d'Iran et le Centre de Recherches des Télécommunications Iraniennes. Il devait aboutir à une mise en route entre 2009 et 2010. A l'issue du Ve plan économique iranien (2011-2016), les deux tiers des Iraniens devaient être connectés à SHOMA, estimait le gouvernement iranien, dont les ambitions ne se limitaient pas à cela. SHOMA devait permettre la mise en ligne d'un véritable e-gouvernement iranien, de développer l'e-commerce iranien et surtout créer un véritable « Internet islamique » qui contribue aussi à renforcer l'image et le rôle de la République islamique dans le cyberespace. Le 28 août 2016, trois ans après l'annonce de Mahmoud Vaezi, le gouvernement d'Hassan Rohani annonçait le lancement officiel de Shoma, décrivant celui-ci comme « une composante essentielle de l'indépendance du pays. » Le ministre de la Communication Nasrallah Jahangard annonçait quant à lui que le réseau devait être un élément déterminant pour mieux se protéger contre les cyberattaques et qu'il offrirait à la population une vitesse 60 fois plus élevée que celle dont pouvaient profiter les pays les mieux dotés dans le monde. Mais le pari le plus important pour SHOMA et ses créateurs était de pousser les sites iraniens, ainsi que les entreprises, à relocaliser leurs données dans des centres de données à l'intérieur du territoire de la République. Cela avait bien sûr l'immense avantage d'offrir à la théocratie persane le pouvoir de contrôler à terme beaucoup plus étroitement le réseau internet et de le couper si besoin. En 2016 toutefois, bien peu d'Iraniens savaient ce qu'était SHOMA, utilisé seulement par des organisations gouvernementales et quelques banques iraniennes. L' « Internet Hallal » de l'Iran semble avoir depuis fait long feu. Et pourtant, la capacité de l'Iran à couper complètement l'accès à Internet dans tout le pays, face aux manifestations de novembre 2019, en a surpris plus d'un. SHOMA était-il finalement plus opérationnel qu'on ne le pensait ? En réalité, expliquait à ce moment-là Frédérick Douzet, professeur à l'Institut français de géopolitique (Paris-VIII) et directrice de Geode : « Le réseau iranien est connecté à l'Internet mondial par seulement trois points d'entrée.

Ces trois points d'entrée sont des opérateurs [IPM, ITC, TIC] contrôlés par l'Etat, qui peuvent couper l'accès au réseau mondial. » Et la chercheuse de préciser : « L'Internet est un réseau constitué de multiples réseaux indépendants interconnectés. Ils sont reliés entre eux grâce à une série de connexions physiques et un empilement de protocoles, qui leur permettent d'échanger des paquets de données numériques. » Internet aura beau être filtré ou soumis, comme dans le cas iranien, à des tentatives de contrôle élaborées, on ne peut raisonnablement parler d'Internet fragmenté ou d'Internet sécessionniste. Tout simplement parce qu'Internet est fragmenté par nature.

Comme le souligne Milton Mueller dans Will the Internet fragment ?, « En cela réside l'ironie intrinsèque du débat autour de la Balkanisation. On peut utiliser ce concept de fragmentation pour aboutir simultanément à deux conclusions diamétralement opposées : 1) L'Internet est et a toujours été fragmenté. 2) L'Internet n'est pas et ne sera jamais fragmenté. » [11] Pour la bonne et simple raison, explique Mueller, que tous les réseaux, sous-réseaux et sites d'Internet parlent le même langage : adresses IP, DNS, protocole TCP/IP [12]. Tous ? Non. Car dans les tréfonds d'Internet, quelques réseaux irréductibles résistent encore et toujours.

En 1999, Ian Clarke, un étudiant de 22 ans de l'Université d'Édimbourg, né un 16 février 1977 à Navan, petite ville irlandaise du comté de Meath, élabore pour son projet de fin de cycle, un logiciel qui laisse ses professeurs sceptiques. Il s'agit de Freenet, A Distributed, Decentralised Information Storage and retrieval System [13], comme l'intitule Ian Clarke. Nous sommes en juillet 1999. En juin de la même année, de l'autre côté de l'Atlantique, Shawn Fanning vient juste de lâcher Napster, un logiciel de partage gratuit de fichiers mp3, sur le réseau mondial, suscitant une réaction forte des autorités et de l'industrie culturelle. Les amendes pleuvent, et même les emprisonnements. De l'Ecosse où il travaille sur Freenet, Clarke observe l'hystérie montante. Il observe aussi que dans des pays plus autoritaires comme la Chine, les internautes peuvent être arrêtés et mis en prison simplement pour avoir émis une critique vis-à-vis du gouvernement. Interrogé en 2005 par le journaliste indépendant Bruno Fay dans les pages « Cyberculture » du Monde, l'informaticien irlandais confiait : « Il y avait deux motivations. D'abord, j'étais sensible au fait qu'il est extrêmement facile pour des gouvernements de contrôler les informations circulant sur Internet. Cela me semblait contraire à la liberté d'expression. Ensuite, Freenet représentait un challenge technologique intéressant. » [14]

Freenet se présente à la fois comme le doyen des darknets, puisqu'il fêtait l'an dernier ses vingt ans, et peut-être encore le plus sûr d'entre eux en termes d'anonymat et de résistance à la censure, même s'il n'existe aucun système garantissant à 100% l'anonymat à ses utilisateurs. Freenet constitue en effet un réseau totalement décentralisé dont le fonctionnement est garanti par les utilisateurs eux-mêmes qui, en installant le logiciel, allouent un espace de stockage sur leur ordinateur pour héberger les données des sites qu'ils consultent sur ce réseau Internet parallèle. Ce faisant, ils permettent ainsi aux freesites consultés de se voir répliqués de multiples fois à mesure que le nombre de consultations augmente. Pour autant, l'utilisateur de Freenet n'hébergera jamais en tant que telles des données qui pourraient être conservées et consultables sur son disque dur. Les informations qui transitent par son disque dur sont « hachées », disséminées et réparties en petits tronçons illisibles. Elles sont également protégées par une clé de chiffrement. Un utilisateur se connectant à Freenet et désirant consulter un site particulier demandera donc à sa machine et au moteur de recherche de Freenet d'aller chercher la clé qui permet de rassembler tous les morceaux de données « hachées » éparpillés sur les ordinateurs du réseau. Pour Clarke, même dans les États démocratiques, la concentration des moyens, la logique monopolistique ainsi que la volonté de surveillance du réseau manifestée par les États ne pouvaient mener à terme qu'au renforcement de la censure et au recul de la liberté d'expression sur Internet, de manière évidemment plus atténuée que dans les États autoritaires, tels que la Chine, mettant en place un vaste contrôle étatique du réseau sur leur territoire. Le projet développé par Ian Clarke à la fin de son cycle d'études avec Freenet reposait donc sur une idée assez simple : puisque Internet pouvait être menacé par l'accaparement des structures physiques – les serveurs et centres de données – lui permettant de fonctionner et que les États pouvaient être tentés d'exercer une censure plus grande sur le réseau, il suffisait de permettre aux millions d'utilisateurs naviguant sur la Toile d'héberger eux-mêmes sous forme hachée et cryptée les données des sites qu'ils allaient visiter. Si ces données sont éparpillées à

travers une myriade d'ordinateurs personnels dont chacun joue le rôle d'un data center en miniature, il devient alors très difficile d'exercer le moindre contrôle et la moindre censure sur les contenus qui s'y trouvent et les utilisateurs qui les consultent.

Freenet est l'exemple type de ce phénomène popularisé depuis quelques années sous le nom de « Darknet », encore souvent confondu avec l'expression « Deep web ». L'expression « Deep web » désigne non pas un internet caché mais un internet pas ou mal référencé : l'ensemble des données produites et stockées en ligne depuis la création d'internet, immense continent numérique constitué par la création de bases de données publiques, privées et particulières, encore extrêmement mal cartographié puisque les moteurs de recherche traditionnels n'en indexent que 10 à 20 % selon les estimations. Un document stocké sur Google Drive appartient ainsi au « web profond », au même titre que les archives d'un forum de discussion ou qu'un réseau privé et sécurisé. Un darknet est un réseau superposé qui utilise des protocoles spécifiques intégrant des fonctions d'anonymisation. Certains darknets se limitent à l'échange de fichiers, d'autres permettent la construction d'un écosystème anonyme complet comme Freenet. Les darknets sont distincts des autres réseaux pair à pair distribués car le partage y est anonyme (c'est-à-dire que les adresses IP ne sont pas dévoilées publiquement) et que les utilisateurs peuvent donc communiquer sans grande crainte d'immixtion de la part de gouvernements ou d'entreprises. Pour ces raisons, les darknets sont souvent associés aux dissidences politiques et aux activités illégales. Plus généralement, le terme « Darknet » peut être utilisé pour décrire toutes les technologies et communications web « underground », plus communément associées aux activités illégales ou dissidentes.

Le Darknet peut être comparé au Quartier Rouge caché dans une ville, dont l'accès est limité par ceux qui y exercent une activité qu'ils ne souhaitent pas rendre publique », explique David Omand, ancien directeur du GCHQ, la NSA britannique, dans un article. Si le « Web Profond » est donc constitué des pages, archives et données non indexées par les moteurs de recherche classique, le Darknet se définirait plus quant à lui comme une sorte de web caché constitué de réseaux privés ou de navigation cryptée auxquels on n'accède que grâce à des outils bien spécifiques, le plus connu aujourd'hui étant TOR, moteur de recherche dont l'acronyme signifie « The Onion Routeur ». En réalité, il existe donc autant de « Darknets » qu'il existe de réseaux anonymes ou privés : Freenet, TOR, sans oublier les réseaux développés grâce aux logiciels GNUnet, I2P, Waste ou Retroshare. Ces réseaux ont une histoire ancienne. Les plus populaires, TOR, Freenet et I2P sont de véritables réseaux parallèles qui utilisent des protocoles informatiques et cryptographiques développés depuis longtemps.

Freenet existe toujours mais reste un réseau extrêmement confidentiel. En 2005, Ian Clarke lui-même le reconnaissait auprès de Bruno Fay du Monde : « Freenet n'est pas aussi facile à utiliser que je l'espérais. Je crois que la principale raison est que Freenet est à la fois un projet de recherche et un projet de logiciel grand public. » Freenet souffrait à sa naissance de deux défauts majeurs : le premier était la lenteur extrême de ce réseau collaboratif sur lequel il

fallait parfois attendre vingt minutes qu'une page se charge, autant dire une insupportable éternité à l'heure de l'ADSL, et le second était l'extrême complexité technique du principe de fonctionnement de Freenet. De nos jours, le premier des deux défauts a été largement amendé et Freenet fonctionne bien plus rapidement qu'il y a dix ans. Cela est dû sans aucun doute à l'augmentation de la fréquentation du réseau et aux perfectionnements techniques apportés par l'équipe de développement. En 2011, Ian Clarke reconnaissait modestement accueillir un peu moins de 30 000 utilisateurs journaliers. Si l'on en croit les statistiques communiquées aujourd'hui par Freenet, ce chiffre a doublé, ce qui reste une goutte d'eau dans l'océan du web.
Un autre darknet rencontre cependant de nos jours un succès bien plus important que celui de Freenet, il s'agit de Tor, acronyme de The Onion Router, le « routeur en oignon ». TOR est sorti des laboratoires de la Navy américaine, ce qui peut sembler surprenant puisque ce réseau crypté qui rassemblerait quelque 80 000 sites différents est devenu la bête noire des services américains et est aujourd'hui géré par une ONG qui milite pour le respect des libertés sur internet, l'Electronic Frontier Foundation. En réalité ce n'est pas si surprenant, quand on prête attention à ce que Paul Syverson, mathématicien et informaticien et l'un des premiers développeurs de Tor, a confié en 1996 à l'un de ses supérieurs : « Bien sûr, nous savions que ces usages détournés seraient inévitables mais cela était sans réelle importance par rapport au problème que nous avions à résoudre, et si ces usages nous procuraient une meilleure couverture de trafic nous permettant de dissimuler l'utilisation que nous voulions faire du réseau, c'était d'autant mieux... Comme je l'ai dit un jour à un officier supérieur, pour son plus grand désarroi. » [15]
Internet, réseau des réseaux, assure l'interopérabilité des protocoles mais dépend aussi de la volonté des individus de partager ou non, et de celle des gouvernements qui peuvent limiter le trafic. Il importe de considérer les conséquences d'une volonté de limiter localement la connectivité. Plus largement, l'idée même d'un espace unifié peut être aussi inquiétante pour les gouvernements (installations sensibles, militaires, industrielles) comme pour les individus (vie privée) qui peuvent vouloir limiter cette universalité de l'interopérabilité. A l'âge de l'Internet des objets, l'interopérabilité peut être vue comme bénéfique mais avant tout comme virale. Le développement des darknets s'inscrit lui aussi dans le débat sur la gouvernance d'Internet parce que ce phénomène, qui participe d'une évolution importante des technologies du numérique, est attaché à des problématiques majeures, également au cœur des préoccupations des différents gouvernements de la planète vis-à-vis d'Internet : sécurité et cybersécurité, alignement d'Internet avec les juridictions nationales et, à l'inverse, possibilité d'échapper partiellement aux contraintes législatives et juridiques et maintien d'un protocole commun garantissant toujours l'interopérabilité universelle des systèmes.

Le phénomène est en tout cas loin de se réduire à la cybercriminalité mais laisse entrevoir le visage de l'Internet tel qu'il pourrait se dessiner dans les années à venir : un Internet plus fragmenté par les volontés politiques, plus cloisonné par l'usage de la cryptographie ou offrant au contraire de nouveaux territoires numériques à explorer.

Notes

[1] Un serveur « proxy » est un serveur intermédiaire par lequel transitent les flux de données entre des ordinateurs distants. A titre individuel, on peut se servir d'un serveur proxy pour sécuriser son accès à Internet et modifier son IP. En Chine, c'est un véritable système de filtrage à,l'échelle de 800 millions d'internautes, plus que toute la population du continent européen.

[2] Virtual Private Network : logiciel ou application permettant de se connecter à Internet en masquant son adresse IP, en passant par des serveurs hébergés hors de Chine, afin de ne pas être identifié comme un internaute basé en Chine et d'être soumis au filtrage du « Bouclier doré ».

[3] https://www.lepoint.fr/phebe/phebe-les-failles-de-la-grande-muraille-de-la-censure-21-11-2019-2348739_3590.php

[4] https://press.princeton.edu/books/hardcover/9780691178868/censored

[5] Publié chez Profile Books en 2019

[6] Source : Statcounter. https://www.webrankinfo.com/dossiers/etudes/parts-marche-moteurs

[7] Laurent Gayard. « Union européenne vs GAFAM. Le contrôle du Big Data. » Conflits n°17, avril-mai-juin 2018

[8] Hari Balakrishnan. « Wide-Area Internet Routing. » Massachussetts Institute of Technology Department of Electrical Engineering and Computer Science. January 2009.

[9] Pour approfondir la question voir : Laurent Bloch. « Contrôle politique et technique de l'Internet. » Diploweb. 13 septembre 2017

[10] C'est-à dire la capacité d'utiliser un sous-réseau Internet pour stocker et exploiter des données en ligne. Ces données nécessitent cependant d'importantes infrastructures physiques pour être stockées en ligne. Le terme de « cloud », « nuage », est donc tout à fait trompeur.

[11] Op. Cit. p. 22

[12] Transmission and Communication Protocol (TCP), le principe de transmission par paquets de données et Identification Protocol, le principe des

adresses IP expliqué précédemment.

[13] https://www.cs.cornell.edu/people/egs/615/freenet.pdf

[14] Cité dans : Laurent Gayard. Darknet, GAFA, Bitcoin. L’anonymat est un choix. Slatkine&Cie. Juin 2018. 320 p.

[15] Cité dans : Laurent Gayard. Géopolitique du Darknet : nouvelles frontières et nouveaux espaces du numérique. Editions ISTE. Janvier 2018. 184 p.