TRUMP CONTRE HUAWEI : ENJEUX GÉOPOLITIQUES DE LA 5G

Kavé Salamatian

La Découverte | « Hérodote »

2020/2 N° 177-178 | pages 197 à 213

ISSN 0338-487X
ISBN 9782348060250

Article disponible en ligne à l'adresse :

https://www.cairn.info/revue-herodote-2020-2-page-197.htm

Trump contre Huawei : enjeux géopolitiques de la 5G

Kavé Salamatian[1]

Le 15 mai 2019, le président des États-Unis signait un ordre exécutif sur la « sécurisation des technologies de l'information et la communication et de la chaîne logistique » [Trump, 2019]. Invoquant une urgence nationale à propos des risques relatifs à la création et à l'exploitation des vulnérabilités dans les équipements et les services de communication, le président motive sa mesure en arguant qu'il « trouve que l'utilisation, aux États-Unis, sans restriction d'équipements conçus, développés, construits ou fournis par des [...] adversaires étrangers [...] constitue une menace inhabituelle et extraordinaire à la sécurité nationale [*sic*] ». Le texte souligne par ailleurs que « même si un climat ouvert d'investissement dans les technologies de l'information et de la communication [...] est important pour la croissance et la prospérité générales des États-Unis, une telle ouverture doit être mise en balance avec la nécessité de protéger le pays vis-à-vis des menaces critiques de sécurité nationale ». Bien que l'ordre exécutif du 15 mai soit très général et ne cite aucun pays en particulier, il vise – de l'avis de tous les observateurs – l'entreprise chinoise Huawei. Et de fait, dans le même temps, le département du Commerce ajoutait Huawei à sa « liste des entités » par ordre exécutif, excluant ainsi l'entreprise chinoise du marché américain des télécommunications.

Cette initiative constitue une étape significative dans l'escalade de la guerre commerciale à laquelle se livrent les États-Unis et la Chine depuis janvier 2018, et les premières annonces tarifaires de l'administration Trump contre l'importation des panneaux solaires chinois. Mais, comme le laisse entrevoir le texte même

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

1. Professeur des universités en informatique, LISTIC-Polytech Annecy.

de l'ordre exécutif, d'autres considérations stratégiques entrent en jeu. Durant les années 2018 et 2019, les États-Unis ont appuyé de tout leur poids sur leurs alliés pour qu'à leur tour ils prennent des décisions d'interdiction similaires, particulièrement à l'encontre de l'entreprise Huawei.

L'interdiction de Huawei aux États-Unis doit se comprendre dans le cadre de la transition technologique des réseaux mobiles de la quatrième génération (4G) vers la cinquième (5G) – au cœur de la décision –, dont les enjeux sont à la fois géopolitiques, technologiques et économiques. L'objectif de cet article est d'analyser le cas Huawei par une approche cyberstratégique et, par ce biais, d'étudier les tenants et aboutissants de la question hautement stratégique des infrastructures critiques.

Le marché de l'équipement 5G : la poule aux œufs d'or de 50,6 milliards de dollars

Le marché mondial de l'équipement 5G a été estimé en 2018 à 720 millions de dollars et devrait atteindre 50,6 milliards de dollars en 2026, soit une croissance annuelle de 76 %[2]. Ces équipements couvrent un espace très large de technologies allant de la communication sans fil à des routeurs et des commutateurs de réseaux, des serveurs de calculs hébergés dans des nuages informatiques (ce qu'on appelle le calcul en brouillard, *fog computing*), et des composants logiciels fournissant les différents services. Les constructeurs d'équipements terminaux mobiles intelligents (*smartphones)* sont aussi bien évidemment à prendre en compte. Le marché de l'équipement 5G se partage ainsi entre de nombreux acteurs, à commencer par les gouvernements qui attribuent les fréquences.

Les communications mobiles nécessitent en effet des bandes de fréquences pour transporter les signaux physiques. Chaque communication active requiert un accès exclusif (sans interférence) à un canal de communication dont la largeur est d'autant plus grande que le débit de l'information transmise est important. Les différentes fréquences ont des caractéristiques physiques spécifiques. Plus la valeur de la fréquence augmente, plus les ondes électromagnétiques ont un comportement qui se rapproche de la lumière (*i.e*. l'onde devient directive et sa portée se réduit). Ainsi les fréquences qui permettent une bonne propagation et une largeur de bande élevée sont très demandées. Or elles sont déjà allouées

2. « 5G infrastructure market size, share and industry analysis by component (fibers, cables, antenna, transceiver, wireless backhaul, modem, router), by communication infrastructure (small cell, macro cell, radio access network (RAN), distributed antenna system (DAS)), and regional forecast 2019-2026 », *Fortune Business Insights*, juillet 2019, en ligne.

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

à des utilisations parfois critiques, comme les radars d'aviation ou les applications de positionnement aérien. Le contrôle du spectre de fréquence est ainsi un des domaines régaliens les plus sensibles et l'autorisation d'utilisation des bandes de fréquences est une source importante de revenus pour les États. En France, l'Autorité de régulation des communications électroniques et des Postes (ARCEP) a attribué les bandes de fréquence 4G LTE (*Long term evolution*) aux opérateurs de télécommunications en 2011 et en 2015. Ces enchères ont rapporté à l'État plus de 3,5 milliards d'euros en 2011 et 2,8 milliards d'euros en 2015[3]. Aux États-Unis, les enchères pour la bande de 700 MHz utilisée par la 4G et la 3G ont engendré 19,5 milliards de dollars en 2008[4]. En France, celles pour les fréquences de la 5G sont en cours, toutefois le gouvernement français a déjà annoncé un prix de réserve de 2,17 milliards d'euros[5]. Les réseaux mobiles sont donc une source majeure de financement public et la bande passante une part importante du capital des opérateurs de téléphonie mobile.

Aux bénéfices économiques directs de la 5G s'ajoutent ses bénéfices indirects, largement invisibles. Car la valeur indirecte d'une infrastructure critique n'apparaît réellement que lorsqu'une attaque ou une panne en prive les utilisateurs. La 5G promet d'augmenter les débits par rapport à la 4G par un coefficient pouvant aller jusqu'à 100, de réduire drastiquement les délais à des valeurs inférieures à une milliseconde (alors que les délais actuels sur les réseaux 4G sont plutôt de l'ordre de la cinquantaine de millisecondes), et de multiplier par 20 la densité de terminaux mobiles. Elle offre l'avantage de pouvoir être déployée de manière beaucoup plus rapide et beaucoup moins coûteuse que la fibre, particulièrement dans les zones difficiles d'accès. Ceci permettra le développement de nouvelles applications et d'usages gourmands en bande passante et qui ne sont aujourd'hui pas encore concevables. La disponibilité de la 5G deviendra ainsi incontournable pour un vaste spectre de besoins de communications allant des applications classiques actuelles (applications bancaires, réseaux sociaux, Web, etc.) aux domaines de l'Internet des objets et de l'intelligence ambiante[6], ainsi

3. Romain Gueugneau, « Les enchères pour les fréquences 4G sont bel et bien terminées », *Les Échos*, 24 novembre 2015.

4. Federal Communications Commission, « Auction 73 : 700 MHz band », *Fact sheet*, 2008.

5. Sébastien Dumoulin, « Enchères 5G : imbroglio autour du prix de réserve », *Les Échos,* 26 novembre 2019.

6. L'intelligence ambiante désigne un espace de vie « intelligent » offrant l'accès à l'information et à des services numériques, simple et convivial d'utilisation, capable de comprendre et s'adapter aux besoins des utilisateurs et de répondre de façon appropriée à leurs demandes. Cette intelligence repose sur la convergence de technologies associant réseaux de communication, objets intelligents et interfaces multimodales.

qu'aux nouvelles applications émergentes de mondes virtuels immersifs. Ainsi, la 5G promet d'être le support de communication de la société de demain. C'est sur ce réseau que se construiront les villes intelligentes, que se concrétiseront les promesses de l'intelligence artificielle (IA) et que se déploieront les communications entre humains. En 2017, le cabinet IHS Markit prévoyait[7], à l'horizon 2035, un chiffre d'affaires global 5G de 12 trillions de dollars, et de 85 milliards d'euros avec plus de 400 000 emplois à la clé pour la France. Tous ces éléments montrent que la problématique économique de la 5G dépasse largement ce que l'on pourrait imaginer pour un simple artéfact technique.

Le contrôle de la technologie sous-jacente à la 5G devient donc un objectif qui a une dimension économique colossale, mais qui a aussi, comme nous le verrons par la suite, des dimensions stratégiques importantes. Pour comprendre ces enjeux stratégiques, il est nécessaire d'expliciter ce que représente le virage technologique de la 5G, et de l'inscrire dans une perspective historique des conflits qui ont présidé à l'émergence des générations précédentes de communications mobiles.

Qu'est-ce que la technologie 5G ?

La première génération de réseaux sans fil mobiles, construite à la fin des années 1970 et 1980, était analogique. La voix était transmise sur des ondes radio non chiffrées, et n'importe qui pouvait écouter les conversations à l'aide d'outils standard. La deuxième génération, construite dans les années 1990, était numérique, ce qui a permis de chiffrer les appels, d'utiliser plus efficacement le spectre sans fil et de fournir les premiers transferts de données pour développer l'Internet mobile. La seconde génération a été une réussite européenne, car elle a été mise au point par l'ETSI (European telecommunications standards Institute) et a permis l'émergence d'acteurs majeurs comme Nokia ou Ericsson. La troisième génération, construite au début des années 2000, a donné un coup de pouce aux réseaux numériques et inauguré la révolution des smartphones. Le premier iPhone, sorti en 2007, n'était même pas compatible avec la 3G. À l'époque, la société finlandaise Nokia était le plus grand fabricant de combinés au monde, en grande partie grâce au leadership européen dans le déploiement et l'adoption de la 2G. Et le Japon était très en avance sur les États-Unis en ce qui concerne la couverture 3G et d'utilisation d'Internet mobile.

L'émergence de la 3G dans les années 1980 était déjà au cœur de sérieuses rivalités de pouvoir géopolitiques. Le processus de développement de la norme

7. IHS Markit, « The promise and potential of 5G : evolution or revolution ? », en ligne.

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

UMTS (Universal mobile telecommunications system) à la base de la 3G s'est déroulé à l'Union internationale des télécommunications (UIT) à partir de la fin des années 1980, pour aboutir à la fin des années 1990. Le choix de la technologie sous-jacente à la 3G a fait l'objet de très importantes controverses. Dans les années 1990, deux technologies de communication étaient en compétition pour être au centre de la 3G, le CDMA (Code division multiple access) et l'OFDMA (Orthogonal frequency-division multiple access). Le CDMA, une technologie en grande partie développée par l'armée américaine et l'entreprise Qualcomm, était déjà utilisé dans plusieurs réseaux d'opérateurs aux États-Unis. La totalité des brevets de cette technologie était entre les mains de Qualcomm et toute utilisation impliquait de lui verser des droits. L'OFDMA, en revanche, était une technologie plus ouverte qui avait été développée par des entreprises et universités européennes, ainsi qu'américaines. L'OFDMA commençait à être utilisé dans les réseaux sans fil WiFi et montrait déjà, à la fin des années 1980, de meilleures performances de transmission de données que le CDMA. Malgré cela, l'entreprise Qualcomm, grâce à un intense lobbying et une intervention très lourde du gouvernement américain[8], réussit à faire accepter sa technologie dans la norme 3G. Pour atteindre ses fins, Qualcomm racheta tous les brevets OFDMA de tous ses concurrents et poussa ainsi la totalité de l'industrie des télécommunications à utiliser une norme, l'UMTS, dont elle savait dès le début que la durée de vie technologique ne dépasserait pas quelques années. Ainsi, la promesse de la 3G de fournir des débits de l'ordre de deux mégabits par seconde aux utilisateurs ne fut jamais atteinte et les débits de l'UMTS, basés sur le CDMA, plafonnèrent à quelques centaines de kilobits par seconde dans des zones privilégiées – alors que des débits de plusieurs mégabits par seconde auraient été possibles avec l'OFDMA. En conséquence, tous les équipements embarquant de la 3G, les terminaux, les stations de base, ainsi que toutes les activités commerciales autour de la 3G, ont eu – et ont toujours – à payer à Qualcomm des droits de licence très conséquents, qu'on estime à plus de 12 % du marché global. L'adoption de cette norme permit aux États-Unis de reprendre l'avantage stratégique sur le développement des communications mobiles, au détriment des leaders de la 2G.

Il faut noter que la Chine déploya initialement, pour son opérateur le plus important China Mobile, une version spécifique de la 3G, basée sur la TD-SCDMA (Time division synchronous code division multiple access) qui n'était pas compatible avec le WCDMA (Wideband code division multiple acccess), déployé partout

8. David Bach, « International cooperation and the logic of networks : Europe and the global system for mobile communications (GSM) », *BRIE*, E-conomy Project, Working Paper n° 139, 14 juillet 2000.

dans le monde. Ce choix reposait sur des arguments de souveraineté et de sécurité, et l'espérance d'une indépendance technologique vis-à-vis des pays occidentaux. Mais rapidement cette décision devint très coûteuse, car les clients souhaitaient utiliser les smartphones de marques Apple et Samsung, conçus pour le marché international et incompatible avec le système chinois. Le gouvernement chinois octroya finalement la licence WCDMA, compatible avec les réseaux mondiaux et en particulier avec les iPhones à China Unicomm, et une licence de CDMA2000 à China Telecom[9].

Une seconde évolution donna le coup de grâce aux constructeurs de combinés et d'équipements de télécommunication qui avaient été les leaders de la 2G et de 2.5G, Nokia et Ericsson : la mise à disposition de jeux de puces électroniques (*chipsets*) par Broadcom et Intel permettant d'intégrer facilement la connectivité 3G et 4G à n'importe quel équipement informatique. Pour la 2G, le téléphone, la station de base et toute la chaîne des équipements étaient considérés de façon monolithique, c'est-à-dire qu'un seul constructeur contrôlait et construisait la majeure partie des équipements nécessaires au déploiement de la 2G. Mais l'arrivée de *chipsets* pouvant être directement implantés sur les téléphones de toute marque a cassé ce monopole en permettant à de nouveaux acteurs d'entrer sur le marché des équipements de télécommunications et même d'y prendre les meilleures places. Elle a en effet permis aux constructeurs de téléphones mobiles de se concentrer sur les autres composants de ce qui allait devenir la nouvelle rupture de la technologie mobile : le smartphone. L'apparition de l'iPhone en 2007, mais aussi des smartphones de Samsung et des autres constructeurs par la suite illustre très bien ce changement. Avec l'avènement de l'Internet mobile, les réseaux mobiles devenaient partie intégrante du cyberespace. Toute une économie des applications mobiles émergeait, révolutionnant les usages et les modes de communication du monde contemporain. Ainsi les entreprises traditionnelles, qui s'étaient construites principalement autour de la production de toute la chaîne d'équipements de télécommunications comme Nokia, Ericsson ou Alcatel, se sont trouvées prises en tenaille sur les composants de communications entre des producteurs de *chipsets* qui étaient plus efficaces, car ne ciblant qu'une petite partie du marché, et les constructeurs de téléphones qui avaient une plus grande expertise dans les composants informatiques et étaient à même d'offrir des équipements avec des écrans et des interfaces utilisateurs plus attractives.

L'augmentation du trafic de données induit par les smartphones démontra rapidement les faiblesses originelles de la 3G relative au débit et, à partir de 2010, la

9. « China's 3G technology gamble : who has the last laugh ? », Wharton University of Pennsylvania, 6 juillet 2011.

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

4G commença à être déployée avec l'OFDMA comme technologie sous-jacente. La 4G a permis d'atteindre des débits de l'ordre de plusieurs dizaines de mégabits par seconde. Néanmoins, Qualcomm et Broadcom possèdent toujours la plupart des brevets relatifs aux technologies sous-jacentes de la 3G, et même d'une partie de la 4G. Ainsi, le passage à la 4G provoqua une augmentation conséquente des revenus de licences de Qualcomm et de Broadcom. On estime les revenus de ces entreprises à plus de 9 % de la totalité du marché de la 4G[10]. La gestion des licences relatives à la 3G et la 4G a été la source d'une quantité innombrable de conflits entre toutes les entreprises parties prenantes. Qualcomm, en particulier, a acquis une redoutable réputation de prédateur de brevets, et suscite depuis la très grande méfiance de tous les acteurs du domaine, qui dans le cadre de la 5G bénéficie à l'entreprise Huawei. Qualcomm a été condamné deux fois à une amende dépassant 1,2 milliard d'euros pour abus de position dominante par l'Union européenne en 2018[11].

L'arrivée des smartphones a non seulement bouleversé les usages, mais aussi les modes de transmission des données. Dans les premières générations de téléphonie mobile, le réseau de l'opérateur de télécommunication était un réseau fermé avec des mécanismes de signalisation spécifiques à la téléphonie. À partir de la 2G, des passerelles vers l'Internet sont ajoutées même s'il n'existe encore aucune connexion directe entre les équipements du réseau et l'Internet. Le trajet des données issues des téléphones mobiles vers l'Internet se passait essentiellement à l'intérieur du réseau de l'opérateur, qui avait ainsi un contrôle complet sur le trafic et pouvait s'assurer qu'aucun service additionnel ne serait déployé sans son accord, et donc sa validation technique et financière.

L'arrivée des smartphones a remis en cause cette approche. En effet, les applications pouvaient être développées au-dessus du réseau mobile, en considérant l'opérateur comme un simple fournisseur de tuyau et non de contenu. Par exemple, le SMS était pendant un temps l'une des principales sources de revenus des opérateurs, mais il a été supplanté par les applications de messagerie sur l'Internet, qui permettent également de téléphoner gratuitement. Ainsi, les réseaux de téléphonie mobile se sont rapprochés des réseaux WiFi et la communication sans fil est progressivement devenue une extension de l'Internet. Ainsi à partir de la 4G les réseaux Internet (IP) se sont de plus en plus intégrés aux réseaux des opérateurs mobiles. D'un point de vue technique, la distance entre les stations de base fournissant la couche radio et celles fournissant la passerelle de connexion à l'Internet

10. Dan Steinbock, « Wireless horizon : strategy and competition in the worldwide mobile marketplace », AMACOM, Div American Mgmt Assn., 2003, p. 305.

11. Foo Yun Chee, « EU fines chipmaker Qualcomm $1.2 billion over exclusivity deal with Apple », Reuters, 23 janvier 2018.

s'est réduite jusqu'à ce que le réseau Internet arrive, dans certains cas, au pied de la station de base de l'opérateur.

La technologie 5G est l'aboutissement de ce processus. Elle vise à ouvrir l'architecture du réseau de l'opérateur à des fournisseurs de services externes et à intégrer complètement les réseaux IP dans le réseau de l'opérateur de télécommunications.

La 5G est une suite de technologies visant plusieurs objectifs. Elle permet des débits de données plus élevés – plusieurs gigabits par seconde pour les utilisateurs –, une réduction drastique des latences pour des applications industrielles comme les réseaux de transport d'électricité intelligents, mais aussi des communications plus fiables et omniprésentes, permettant le développement de l'Internet des objets qui implique une multiplication par 100 du nombre de terminaux (téléphones, objets) connectés simultanément au réseau.

Afin d'atteindre ces objectifs, la 5G institue l'hétérogénéité des composants en principe fondamental. Les générations précédentes définissaient clairement trois composants : le composant radio ayant la responsabilité de mettre en place et de gérer l'interface radio et les ressources s'y rattachant ; le réseau de l'opérateur qui assure les fonctionnalités liées à l'opérateur, comme la gestion de la mobilité (*roaming*), la facturation ou la gestion des droits d'accès, ainsi que la mise en place des circuits de voix ; et finalement la passerelle vers l'Internet. Dans la 4G et la 3G, chacun de ces composants doit suivre des normes bien définies. Pour la 5G, en revanche, c'est l'hétérogénéité qui prime. L'interface radio peut suivre la norme définie pour la 4G, mais aussi celle définie pour le WiFi ou même celle d'une nouvelle génération d'interfaces en ondes millimétriques. Afin de tenir la promesse de faibles délais (de l'ordre de la milliseconde) et de fiabilité, l'opérateur de 5G devra ouvrir son réseau et le partager avec des fournisseurs de services externes. Cette intégration s'appuie sur des mécanismes similaires à ceux déployés dans les nuages (*clouds*) informatiques. La virtualisation, c'est-à-dire le découpage (*slicing)* et le partage des ressources du réseau de l'opérateur, permet de donner l'accès du réseau à des fournisseurs de services multiples tout en garantissant une étanchéité et une séparation entre eux. Ceci aboutit à un changement en profondeur du modèle économique des opérateurs de télécommunications mobiles. Traditionnellement, ces opérateurs avaient une position privilégiée en contrôlant de façon directe des services déployés dans leurs réseaux, dont ils récoltaient les bénéfices économiques. Or la virtualisation peut faire entrer le loup de la concurrence des fournisseurs de services dans la bergerie, jusqu'ici protégée, des réseaux d'opérateurs.

La 5G aboutit à une transformation en profondeur de l'infrastructure de télécommunication, traditionnellement construite sur la base de composants matériels propriétaires, en une infrastructure en grande partie logicielle. On observe donc pour la 5G le même phénomène, fondé sur le concept d'OEM (*Original Equipment*

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

Manufacturer), qui a radicalement changé le marché des ordinateurs personnels dans les années 1990, à savoir la construction de systèmes de communications 5G par l'assemblage de composants génériques conçus par des sous-traitants qui fournissent ces mêmes composants à plusieurs constructeurs. C'est ainsi le logiciel qui permet à tout ce système hétérogène de fonctionner et présente l'avantage d'être beaucoup plus flexible, donc de s'adapter facilement aux besoins. Mais il reste en revanche plus vulnérable vis-à-vis des cyberattaques, alors que les composants matériels, limités en nombre et en diversité, étaient relativement sécurisés. C'est ce point qui est aujourd'hui au centre de la controverse sur la sécurité de la 5G.

Analyse cyberstratégique de la 5G

On peut définir la cyberstratégie en paraphrasant la définition classique de la stratégie comme l'art de positionner, diriger et gouverner ses cyber-forces dans le cyberespace afin d'atteindre ses cyber-objectifs. Les éléments précédemment décrits donnent les principaux outils afin de développer une analyse cyberstratégique de la 5G.

Commençons par décrire les objectifs que souhaitent atteindre les gouvernements par le biais de la 5G. Nous avons déjà évoqué la valeur colossale de l'activité économique qui sera directement ou indirectement engendrée par la 5G. Celle-ci peut devenir l'épine dorsale de changements économiques profonds, car elle permettra l'émergence de l'Internet des objets, qui est la technologie sous-jacente des villes intelligentes, des réseaux véhiculaires qui sont les précurseurs des véhicules autonomes, ou encore de l'intelligence artificielle ambiante. Ainsi, la 5G est une infrastructure essentielle pour tous les États. De plus, la 5G rebat les cartes technologiques, et certains gouvernements, la Chine en particulier, souhaitent s'appuyer sur cette nouvelle technologie pour prendre ou reprendre des parts dans le marché lucratif des équipements de la 5G. Ainsi l'un des objectifs est d'obtenir une position centrale dans le développement de cette technologie, ou du moins de ne pas dépendre de compétiteurs stratégiques.

Les réseaux mobiles doivent par ailleurs être considérés comme des Opérateurs d'importance vitale (OIV), et l'État a donc une responsabilité régalienne d'évaluation des risques et de protection de ces infrastructures. La directive NIS clarifie cette responsabilité pour les États de l'Union européenne. Et beaucoup d'autres États dans le monde ont mis en place des mécanismes semblables. Les États sont donc tiraillés entre deux impératifs à propos de la 5G. D'une part, l'obligation de protection des infrastructures critiques des réseaux mobiles nécessite de demander aux opérateurs de mettre en place des mécanismes parfois coûteux, qui risquent de nuire à leur avantage compétitif, par exemple l'utilisation de normes

de communications non standard qui augmenteraient les frais d'exploitation du réseau (norme TD-SCDMA en Chine en 2003) ; le déploiement de coûteux mécanismes de sécurité ; ou encore l'interdiction d'achat de fournisseurs étrangers, qui réduit la compétition sur le marché et augmente les coûts. D'autre part, l'impératif économique des opérateurs, et indirectement de la société tout entière, nécessite de permettre aux opérateurs de développer une activité économique avec un minimum d'entrave compétitive.

La régulation des acteurs est souvent une décision à double tranchant. Un État peut décider d'agir sur le choix des fournisseurs d'équipements de réseaux mobiles des opérateurs et imposer une préférence nationale, exclure certains constructeurs (par exemple Huawei) sur des arguments de sécurité nationale (ce qui est l'un des cas particuliers où l'Organisation mondiale du commerce [OMC] permet de s'affranchir de ses règles), ce qui a des conséquences, notamment en termes de mesures de rétorsion économiques. Mais le problème de fond, comme nous le verrons, est qu'une telle décision ne résout nullement les problèmes de cybersécurité de la 5G.

Le fond de la controverse US-Chine au sujet de Huawei

Nous observons depuis 2018 une campagne organisée par le gouvernement américain et dirigée principalement contre Huawei, le leader chinois de la 5G. Mais les vrais problèmes qui motivent cette offensive américaine ne sont jamais directement énoncés.

La politique américaine à l'égard de Huawei doit être replacée dans le contexte plus général de la détérioration des relations sino-américaines, résultant de l'émergence de la Chine en tant que rival géopolitique des États-Unis, aussi bien dans l'économie mondiale que plus généralement dans les relations internationales. D'une part, la Chine s'est engagée depuis 2013 dans le projet des « Nouvelles routes de la soie ». Ce projet vise à construire un marché intégré combinant les marchés domestiques et internationaux, par le biais d'intégration d'infrastructures. L'accent a été mis initialement sur la construction d'infrastructures de transport. Depuis, les volets énergies et télécommunications du projet prennent une importance croissante. Dans ce cadre, la maîtrise de la 5G – qui sera la technologie sous-jacente de ces infrastructures – prend une importance particulière. L'utilisation par la Chine des infrastructures de communication comme moyen de prise de position stratégique est particulièrement visible aujourd'hui en Afrique. Elle commence aussi à s'étendre fortement en Asie.

La croisade anti-Huawei de l'administration américaine s'inscrit aussi dans une évolution du libéralisme et de la mondialisation, dont le champion a été les

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

USA, vers un nationalisme technologique, qui pourrait être contre-productif au vu du poids de plus de 50 ans de politique plus libérale. Ainsi, le développement des nouvelles technologies, et plus généralement l'évolution scientifique, risque d'être pris en otage par du protectionnisme économique déguisé en arguments de sécurité nationale. Il serait simpliste d'attribuer la totalité du problème au président Trump – même si son comportement est de nature à exacerber la controverse –, et de focaliser la discussion sur des éléments parfois marginaux au détriment des éléments stratégiques plus fondamentaux. Les racines du désaccord ont précédé sa présidence de près d'une décennie et peuvent être trouvées dans l'émergence géopolitique de la Chine en Asie [Samaan, 2012], dans le Pacifique et plus récemment en Asie centrale et au Moyen-Orient avec le projet des Nouvelles routes de la soie. La lutte des valeurs entre les États-Unis et la Chine joue aussi un rôle, certes moins central dans le cadre de l'administration Trump, mais qui a son importance pour le public occidental.

Les quatre arguments principaux de l'administration américaine vis-à-vis de Huawei sont les suivants : l'équipement Huawei 5G pose de graves menaces de cybersécurité ; Huawei vole la propriété intellectuelle ; Huawei obtient des subventions gouvernementales ; Huawei est indissociable du gouvernement chinois et en est l'outil.

Ces arguments semblent forts, définitifs et convaincants. Mais une analyse plus critique et empirique montre leurs faiblesses.

Huawei et la cybersécurité

Les services de renseignement américains affirment que la présence d'équipements ou de logiciels Huawei dans un réseau 5G est à même de compromettre la sécurité de l'ensemble des systèmes 5G. L'argumentaire des services de renseignement projette ainsi l'opposition politique et stratégique avec la Chine sur la sécurité des équipements et des systèmes informatiques, une problématique très technique. En effet, il n'y a pas besoin de faits pour répandre la peur et développer une paranoïa nationaliste voire un maccarthysme technologique. Ceci aboutit à des arguments qui ne peuvent sembler discutables que pour les personnes ayant des connaissances techniques.

Il n'y a aujourd'hui aucun cas documenté rendu public de mise en place de porte dérobée dans les équipements Huawei. Il y a certes des vulnérabilités, des erreurs, des processus de développement sécurisés de logiciels déficients, ainsi que l'a rapporté le seul processus sérieux d'évaluation de sécurité des équipements Huawei par le laboratoire commun entre Huawei et le service national de cybersécurité (NSCS), le « Huawei Cyber Security Evaluation Center » (HCSEC) au

Royaume-Uni. Ce centre rapporte « des défauts graves et systématiques dans les processus de Huawei en matière de génie logiciel et de cybersécurité[12] ». Une autre conclusion clé du rapport du HCSEC est que le NCSC du Royaume-Uni « ne croit pas que les défauts identifiés sont le résultat de l'ingérence de l'État chinois ». Le rapport continue avec cette assertion : « Les contrôles architecturaux en place dans la plupart des opérateurs britanniques limitent la capacité des attaquants à mettre en place la communication avec des éléments de réseau qui ne sont pas exposés au public, ce qui, avec d'autres mesures en place, rend l'exploitation des vulnérabilités plus difficile. »

Mais ces défauts ne sont nullement plus importants que ceux des autres constructeurs d'équipements de communications, notamment américains, comme Cisco[13], Juniper[14], ou Qualcomm[15] – avec la différence que certains d'entre eux ont un passé documenté de mise en place de portes dérobées. Le seul cas connu, aujourd'hui, de mise en place de *backdoor* dans des équipements de télécommunications chinois est celui du siège de l'Union africaine à Addis-Abeba en 2018[16]. Les détails de cette affaire montrent que l'introduction de portes dérobées s'est faite durant le transport[17]. Ce qui met en exergue le problème autrement plus important de la sécurité des chaînes logistiques.

Ceci ne signifie aucunement que la Chine n'a pas fait preuve d'un cyber-hackitivisme véhément et n'a pas attaqué des équipements de télécommunications. Le cyberespionnage chinois est un problème pour tous les pays, en particulier les pays occidentaux. Mais il n'y a pas de preuve publique que la Chine a mené ses opérations d'espionnage en utilisant des *backdoors* implantées par les entreprises chinoises dans leurs équipements.

Un autre argument utilisé est le risque de *black-out*. Autrement dit, les équipements Huawei dans le monde pourraient fonctionner normalement de nombreuses années jusqu'à une crise, durant laquelle le gouvernement chinois mettrait hors circuit tous les équipements Huawei, avec un impact mondial potentiellement

12. « Huawei cyber security evaluation centre (hcsec) oversight board. A report to the National Security Adviser of the United Kingdom », rapport annuel 2019, accessible en ligne.

13. Cisco, « Cisco Nexus 9000 series fabric switches application centric infrastructure mode default SSH key vulnerability », 9 mai 2019, accessible en ligne.

14. Kim Zetter, « New discovery around Juniper backdoor raises more questions about the company », *Wired*, 8 janvier 2016.

15. « What's behind the Broadcom, Qualcomm and Intel acquisition (backdoor inside) », Steemit, 10 mars 2018.

16. Reuters, « China rejects claim it bugged headquarters it built for African Union », *The Guardian*, 30 janvier 2018.

17. La Chine n'a nullement inventé ce genre d'attaque. Les révélations Snowden ont montré l'utilisation de ce genre d'approche par la NSA.

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

catastrophique. Cet argument est d'autant plus pertinent que les États-Unis et même la France ont utilisé des approches semblables dans le passé[18].

Un problème plus profond est que la campagne américaine contre Huawei transforme des risques inhérents à tous les systèmes informatiques complexes en un problème que seuls les entreprises et les équipements chinois causeraient. Ce faisant, les États-Unis font miroiter l'illusion dangereuse que les matériels américains ou européens seraient plus sûrs par définition. De fait, en étant largement plus dépendante du logiciel que les générations précédentes, la 5G est confrontée à un nouvel ensemble de risques. Ce sont en fait la flexibilité et l'augmentation des débits apportés par la virtualisation sur laquelle s'appuie la 5G qui sont la principale source de risque. Ces risques ne sont pas réductibles à l'origine nationale du fabricant ou du développeur.

Il est dès lors nécessaire d'évaluer l'équilibre entre les bénéfices escomptés et les risques induits par la 5G. Cette démarche semble nécessaire plus généralement pour toutes les infrastructures informatiques sensibles, telles que les centres de données et l'informatique en nuages (*cloud computing*). Il est de la responsabilité des États de faire cette analyse de risque et de définir leurs priorités stratégiques. L'erreur serait de considérer que ces décisions ne sont que du ressort des industriels du domaine et que l'État n'a pas à s'y immiscer. Or c'est pourtant ce qu'ont fait la plupart des États pour les technologies précédentes. La controverse actuelle sur la 5G a eu cette qualité pédagogique de leur rappeler leurs responsabilités et de les amener à se questionner sur les choix technologiques. On se demande d'ailleurs quand cet examen minutieux sera appliqué à d'autres objets informatiques qui ont, dans la société contemporaine, une position stratégique plus importante que la 5G, comme les systèmes d'exploitation Microsoft ou Android, dont les vulnérabilités sont endémiques.

Néanmoins, le cas Huawei met en relief un problème de cybersécurité plus fondamental. Les chaînes d'approvisionnement sont aujourd'hui mondialisées. Un équipement 5G embarque des composants venant de plus 20 pays ! Les principaux producteurs de puces électroniques mondiaux sont basés à Taiwan. Les téléphones Samsung et Apple sont construits en Chine. Une voiture vendue en France peut être construite au Mexique avec des composants électroniques conçus au Japon, construits à Taiwan et assemblés en Chine. L'interdépendance actuelle est tellement forte qu'il est extrêmement difficile de nationaliser n'importe quel équipement informatique. La cybersécurité des circuits d'approvisionnement est donc la principale source de risque cyber, et il est impossible de réduire ce

18. Anatoly Malyuk, « Hidden threats from foreign software », Russian International Affairs Council, 9 octobre 2012, en ligne.

problème à l'origine nationale d'une seule entreprise qui assemble ou conçoit un équipement.

La posture de cybersécurité de l'administration américaine dans le cas Huawei remet ainsi profondément en cause le système de libre-échange dans les technologies et les services informatiques, or ce sont les entreprises américaines, en particulier les Gafa[19], qui bénéficient le plus de ce système. C'est donc une source de risque important pour ces acteurs, et donc plus largement pour tous les acteurs internationaux.

Les problèmes de vol de propriété intellectuelle

Le second argument de la campagne américaine contre Huawei est lié au vol de propriété intellectuelle : Huawei n'aurait développé sa technologie, et ses équipements ne seraient compétitifs, que parce qu'elle les a copiés des Occidentaux. Comment une entreprise créée en 1987 à Shenzhen serait-elle capable aujourd'hui de devancer les leaders d'industries américains, alors que dans le même temps les entreprises européennes du secteur ont toutes plongé ? Outre le caractère quelque peu raciste de cet argument, il met de côté des éléments objectifs. L'investissement de Huawei en recherche et développement (R&D) a dépassé en 2018 celui de Microsoft, Apple ou Intel. L'entreprise se classe 4e parmi les entreprises technologiques mondiales ayant le plus investi en R&D. L'entreprise Huawei est leader mondial dans le nombre de brevets 5G. Cette forte activité de Huawei s'appuie sur une forte croissance marquée de la Chine dans tous les indicateurs scientifiques, en particulier dans les domaines informatiques, et plus particulièrement des réseaux et de l'intelligence artificielle [Xie et Freeman, 2019]. Ce dynamisme prononcé est le fruit de la stratégie nationale chinoise d'investissements massifs dans l'éducation universitaire et la recherche[20]. La forte croissance chinoise dans la recherche académique et technologique est un sujet d'inquiétude majeur stratégique pour les États-Unis. Mais ce serait une erreur stratégique considérable de sous-estimer ces adversaires en niant leurs capacités [Douzet, 2018].

Il est vrai que Huawei a été au centre de plusieurs cas d'espionnage industriel. Les premières versions des routeurs Huawei utilisaient un langage de commande similaire au langage du système iOS de Cisco. En 2003, Cisco a poursuivi Huawei pour violation de ses brevets et copie du code source utilisé dans les routeurs et les

19. Google, Amazon, Facebook, Apple.

20. La Chine était en 2017 le second pays au monde en termes d'investissement en R&D. Voir China Power Team, « Is China a global leader in research and development ? », *China Power*, 31 janvier 2018.

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

commutateurs. Le jugement a demandé que Huawei supprime le code, les manuels et les interfaces de ligne de commandes contestés et l'affaire a été réglée[21]. En 2010, Motorola et Huawei ont réglé à l'amiable une plainte concernant un vol de secrets commerciaux par d'anciens employés. L'administration américaine cite comme preuve de vol de propriété intellectuelle le robot « Tappy » de T-Mobile. Tappy était un robot tactile permettant de tester les combinés dans des conditions réelles. En tant que tel, ce robot n'est pas une technologie stratégique et n'a aucune incidence sur les principaux marchés d'équipements et de logiciels 5G que Huawei tente de conquérir. Une plainte civile de T-Mobile contre Huawei a déjà été réglée avec des dommages-intérêts mineurs et le rejet des autres accusations. L'utilisation de ce seul argument comme preuve pour l'exclusion de Huawei des marchés américains, et même des marchés mondiaux, est assez limitée.

Ces arguments s'inscrivent dans le contexte des conflits de propriété intellectuelle dans le domaine des technologies de l'information. Il y a des batailles de brevets titanesques entre Apple, Samsung et Qualcomm qui font le bonheur des avocats spécialisés. Cisco et Juniper sont les sujets de nombreuses poursuites croisées en matière de brevet. Cisco et Arista ont récemment réglé un litige contre un paiement de 400 millions de dollars[22]. Dans un contexte globalisé, les conflits aux frontières de leurs brevets respectifs d'entreprises innovantes sont incontournables. Les tribunaux en traitent fréquemment et il n'y a rien de bien particulier à Huawei. Dans les années 1980, le Japon était présenté comme la plus grande menace économique pour les États-Unis et les allégations de vol de propriété intellectuelle faisaient foison contre ce pays. Aujourd'hui, c'est la Chine qui joue le rôle du vilain.

Les subventions

Le troisième argument de l'administration Trump consiste à pointer les subventions que recevrait Huawei de l'État chinois : Huawei ne serait compétitif que parce qu'il reçoit de l'argent de l'État chinois. À l'appui de ceci, on cite les informations des renseignements américains montrant que Huawei a été payé par l'Armée populaire de libération et par la Commission de la sécurité nationale de Chine, ainsi que par d'autres composantes du renseignement d'État chinois. Cela signifie simplement que Huawei a des contrats avec le gouvernement chinois et que la Chine a une approche protectionniste de ses marchés publics. N'est-ce pas ce que

21. Jan Wolfe, « Arista to pay $400 million to Cisco to resolve court fight », Reuters, 6 août 2018.

22. *Ibid*.

font aussi les États-Unis ? Serait-il concevable que l'État chinois, qui a poussé au développement de Huawei précisément pour avoir un champion national sur lequel il pourrait compter, ne s'adresse pas à son entreprise nationale dans le seul but de satisfaire les États-Unis ? Ce sont bien des entreprises américaines comme Cisco ou Amazon qui ont des contrats et fournissent des services au département de la Défense, à la CIA, à la NSA et même au DHS. Les révélations Snowden ont montré clairement l'hypocrisie en vigueur dans ce domaine – l'entreprise de cryptographie RSA aurait bien été payée 10 millions de dollars par la NSA pour installer une *backdoor* dans ses équipements de chiffrement[23]. En quoi ce paiement serait-il moins problématique que le paiement de l'État chinois à Huawei ?

Huawei : la cinquième colonne de l'État chinois

La croisade anti-Huawei de l'administration américaine n'a de sens que si l'on considère que l'État chinois est la cible de cette attaque. Le déploiement de la 5G en Amérique, et plus généralement dans le monde, est otage d'un conflit géopolitique sino-américain. La technologie est ainsi transformée en arme dans des manœuvres dont la guerre commerciale en cours n'est qu'une bataille. Le secrétaire d'État Mike Pompeo dit fréquemment que « Huawei est un instrument du gouvernement chinois » et qu'il suffirait d'une simple demande de ce gouvernement pour que tous les opérateurs qui ont acheté des équipements Huawei deviennent des pions impuissants. Cette affirmation est techniquement fausse. Les opérateurs de télécommunications qui déploient et gèrent les équipements mettent en place des mécanismes de segmentation, diversifient leurs sources d'approvisionnement, et s'assurent d'un niveau élevé de contrôle de leurs réseaux. L'idée qu'un constructeur, même Huawei, serait à même de mettre à bas toutes les protections mises en place au sein d'un réseau d'opérateurs est de l'ordre des théories conspirationnistes les plus farfelues. Il est évident qu'au vu des discussions en cours les États et les opérateurs qui déploieraient des équipements Huawei le feront dans le contexte d'une grande défiance qui rendrait de fait ces réseaux plus sûrs et plus fiables que tout autre équipement, du fait d'une surveillance accrue. En effet, ainsi que nous l'avons décrit précédemment, il ne suffit pas de s'assurer au moment de l'achat de la sécurité d'un équipement. Les risques informatiques étant endémiques, il faut déployer ce que l'on a coutume d'appeler une sécurité en profondeur, autrement dit surveiller les équipements et mettre en place des procédures de réactions rapides en cas d'événements anormaux. Il existe bien

23. Russell Brandom, « NSA paid $10 million to put its backdoor in RSA encryption, according to Reuters report », *The Verge*, 20 décembre 2013.

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

évidemment un risque que des vulnérabilités subsistent dans ces équipements. Mais il serait suicidaire pour les services chinois de les utiliser, car tous les indices pointeraient vers eux, et les conséquences des représailles seraient terribles en termes politiques, économiques, diplomatiques, voire militaires.

Conclusion

Tout montre que nous sommes confrontés à une lutte de pouvoir dans un contexte de compétition stratégique exacerbée entre grandes puissances et que la croisade anti-Huawei doit être interprétée dans ce sens. Certaines personnes dans l'administration Trump et dans les cercles de réflexion néoconservateurs considèrent que la montée en puissance chinoise et le déclin américain pourraient être enrayés en sapant certaines industries stratégiques en Chine par des moyens de pression digne de technique d'extorsion mafieuse[24], plutôt qu'en surpassant leurs rivaux sur les plans économique et technologique, comme cela a été le cas depuis la révolution industrielle et en faisant fonctionner à plein régime le « rêve américain », fondé sur une société ouverte où le mérite et la connaissance scientifique sont reconnus comme des valeurs cardinales.

Bibliographie

DOUZET F. (2018), « L'expansion de la puissance chinoise dans le cyberespace », *Revue de défense nationale*, n° 812, p. 89-95.

SAMAAN J.-L. (2012), *La Menace chinoise. Une invention du Pentagone ?*, Paris, Vendémiaire.

TRUMP D. J. (2019), « Executive order on securing the information and communications technology and services supply chain », The White House, 15 mai.

XIE Q. et FREEMAN R. B. (2019), « Bigger than you thought : China's contribution to scientific publications and its impact on the global economy », *China & World Economy*, vol. 27, n° 1, p. 1-27.

24. Katrin Bennhold et Jack Ewing, « In Huawei battle, China threatens Germany "where it hurts" : automakers », *The New York Times*, 16 janvier 2020.