diploweb.com La revue géopolitique
ISSN : 2111-4307

La France face à la géopolitique de la 5G : quels enjeux autour de la nouvelle génération de réseau sans fil ?

dimanche 29 novembre 2020,par Arsenio CUENCA

Citer cet article / To cite this version :
Arsenio CUENCA, **La France face à la géopolitique de la 5G : quels enjeux autour de la nouvelle génération de réseau sans fil ?**, *Diploweb.com : la revue géopolitique, 29 novembre 2020.*

Quels sont les enjeux liés au déploiement de la technologie 5G au niveau européen et plus précisément, dans le cas de la France ? Une réponse solidement documentée et finement argumentée. Arsenio Cuenca précise d'abord les enjeux éminemment géopolitiques autour de cette technologie innovante. Puis il présente la réaction européenne face à sa situation de dépendance. Enfin, l'auteur brosse l'évolution des représentations autour du système d'alliances français et les agendas public-privés pour un avenir numérique.
Illustré d'une carte sur le problème de la dépendance technologique en Europe et d'une perspective diachronique des enjeux de la 5G en France.

L'ENTREE de la 5G dans nos vies entraînera des progrès immenses en matière d'interconnectivité, puisqu'il s'agit d'un réseau bien plus dynamique, permettant l'incorporation de nouveaux objets connectés avec un temps de latence extrêmement réduit [1]. Cependant, son déploiement comporte un certain nombre de risques associés à sa nature, à savoir une forte dépendance vis-à-vis des fonctions réseau et une extension de la surface potentiellement réceptrice des cyberattaques, avec des conséquences bien plus graves.

De ce fait, la cinquième génération de téléphonie mobile présente une composante stratégique fondamentale pour les acteurs impliqués. L'antagonisme principal se déroule entre les deux premières puissances technologiques et économiques au niveau global : les États-Unis et la Chine. Mais les effets de cette confrontation se font sentir inéluctablement dans l'UE, qui se trouve dans une situation pour le moins délicate [2]. Les grandes puissances de l'Union européenne (UE) considèrent la Chine comme une menace, mais leur dépendance à l'égard de Huawei les empêche de leur interdire le déploiement de la 5G sur le marché de l'UE. Par conséquent, ils permettent l'entrée de Huawei, tout en renforçant leurs systèmes de cybersécurité et leurs mécanismes de contrôle politique face au géant chinois. Les enjeux de la 5G ont mis en évidence la forte dépendance de l'UE envers les deux puissances, ce qui l'amène à chercher son propre espace d'autonomie stratégique.

En France, Emmanuel Macron a déclaré à de nombreuses reprises que la France n'avait aucun intérêt à interdire l'entreprise chinoise. Cette décision est évoquée aussi dans le dernier rapport rédigé au nom de la commission des affaires économiques sur l'exploitation des réseaux radioélectriques mobiles. Cependant, ces allégations marquent un point de rupture important par rapport aux positions officielles précédentes, qui alertaient du danger que Huawei présentait pour la cybersécurité de la France, allant même jusqu'à suggérer l'interdiction de l'installation de ses équipements.

Quels sont les enjeux liés au déploiement de la technologie 5G au niveau européen et plus précisément, dans le cas de la France ?

Des enjeux éminemment géopolitiques autour de cette technologie innovante

Le terme 5G fait référence à la technologie de connectivité mobile de cinquième génération. Elle s'agit d'un saut qualitatif dans le domaine des télécommunications et sa performance dépassera les prestations de l'actuelle 4G. L'espace de bande passante que la 5G libérera va

permettre la diffusion de l'Internet des objets (*IoT* par son acronyme en anglais). Les faibles temps de latence, ainsi que la vitesse de téléchargement de données – multipliée par 1000 –, mettra en service tout un écosystème de nouvelles avancées et d'objets connectés au réseau, dans des divers domaines sociaux comme la médecine, et notamment, l'industrie et les transports [3]. Cette logique suit le principe M2M (*Machine to Machine*), une amélioration de l'interconnectivité entre un nombre important d'objets et d'applications, qui seront capables de « voir, entendre, penser et effectuer des tâches en se parlant, en partageant des informations » [4].

Au début de l'année 2016, dans son rapport quinquennal "Technologies Clés 2020", le Ministère de l'Économie de l'Industrie et du Numérique a consacré une section à l'IoT, affirmant qu'il serait « une dimension fondamentale de l'Internet de demain » [5]. Ce n'est pas par hasard que la secrétaire d'Etat auprès du ministre de l'Economie et des Finances, Agnes Pannier-Runacher, a souligné à plusieurs reprises [6] que la France doit s'impliquer dans l'innovation d'un des secteurs où les applications de l'IoT sont plus prometteuses : l'Industrie 4.0, qui tire son nom de ce qui devrait être la quatrième révolution industrielle [7]. Dans la nouvelle usine numérique, les machines seront connectées via l'Internet des objets industriels (IIoT). Selon IBM, les améliorations appliquées aux processus industriels pourraient augmenter l'efficacité de la production jusqu'à 25% [8]. Ce réseau entrelacera la numérisation avec les processus d'assemblage, veillant sur l'état du produit aussi bien à l'intérieur de l'usine qu'une fois à l'extérieur.

Néanmoins, en raison de sa plus grande complexité et parce qu'elle intégrera l'architecture de nombreux secteurs de la société future – les soi-disant « acteurs verticaux » [9] – cette technologie soulève des questionnements sur la sécurité et l'intégrité des États. Selon le rapport du groupe de coopération NIS du 9 octobre 2019 [10], le réseau 5G présente plusieurs caractéristiques qui le rendent plus complexe et potentiellement plus vulnérable. Une conversion des fonctions *hardware* en *software* créera un réseau plus décentralisé dont la périphérie, potentiellement moins supervisée, deviendra plus importante. De nombreuses fonctions réseau passeront au numérique, ce qui signifiera une plus grande dépendance vis-à-vis des fournisseurs pour les mises à jour périodiques du système. De même, les certificats des logiciels 5G ne constituent pas une mesure suffisante pour garantir la sécurité, car de possibles *spyware* peuvent être téléchargé sur le système lors d'une mise à jour [11]. Les tâches de sécurité seront donc beaucoup plus complexes et il faudra entreprendre des supervisions régulières du système.

Au moment d'identifier les acteurs qui représentent une menace plus grande, parmi les hacktivistes et les cyberterroristes, le rapport pointe vers les États et les entités avec des liens étatiques qui se trouvent en-dehors de l'UE. Ici, l'affrontement dépasse les questionnements technologiques et c'est à ce moment-là que la géopolitique entre en jeu. Le rapport évoque **la vulnérabilité d'un réseau 5G qui s'appuie de plus en plus sur des acteurs privés extra-européens liés à leurs gouvernements**. C'est le cas notamment de Huawei, firme basée dans la « Silicon Valley chinoise », Shenzen, et fournisseur leader dans le domaine de la 5G. Le gouvernement chinois partage des liens politiques et économiques avec ses acteurs nationaux qui opèrent ailleurs dans des secteurs stratégiques. Chez Huawei, les experts attribuent sa création à l'Armée de Libération Chinoise et ils assurent que son PDG, la secrétaire d'Etat auprès du ministre de l'Economie et des Finances Ren Zhengfei, est un de ses ancien cadres [12].

Le rapport entre Huawei et l'Etat chinois répond à une logique stratégique dénommée par les experts « techno-nationaliste » : promouvoir et planifier l'investissement dans le R&D à une échelle nationale pour être indépendante des technologies de ses rivaux ; tout en ayant une plus grande influence sur eux, en exportant le développements conçus au niveau national [13]. En épousant ce principe, Ren s'est entretenu en 1994 avec Jiang Zemin, le président à l'époque, pour avoir son soutien économique et politique en invoquant des motifs d'intérêt national [14]. Huawei et le PCC conjuguent leurs intérêts pour pénétrer les marchés étrangers et pour être en tête du développement technologique au niveau mondial. Ce leadership a finalement réussi dans le domaine de la 5G, ce qui lui permettra d'établir les standards globaux sur lesquels cette technologie sera basée, pour ainsi renforcer l'industrie nationale chinoise et avoir un avantage solide sur sa concurrence [15].

En revanche, bien que les accusations contre la Chine ne soient pas sans fondement, elles ne peuvent pas non plus échapper à une certaine controverse. Le rapport NIS ne mentionne aucun acteur ou État spécifique, et la définition qu'il fournit « d'acteur étatique extérieur à l'UE » englobe aussi les États-Unis. Historiquement, Washington a investi fortement pour financer ses champions de la technologie [16] [17]. De même, en référence au « Cloud Act », un décret en vertu duquel le gouvernement américain peut accéder aux données des entreprises de services de stockage dans le cloud opérant à l'étranger, la législation américaine peut sembler envahissante et intrusive [18]. Leurs antécédents n'aident pas non plus à améliorer leur image, compte tenu des scandales de surveillance de masse découverts par Edward Snowden en 2013 ; ou le fait que, de la même manière que Huawei peut collaborer avec le gouvernement chinois, la firme Microsoft a autorisé la NSA à accéder à Skype ou Outlook pour collecter des vidéos et des messages de ses utilisateurs [19]. Des chercheurs comme Nicolas Arpagian ont également évoqué l'influence de l'agence de renseignement américaine sur Google [20].

Même si Pékin s'est doté depuis 2017 d'une loi similaire [21] au Cloud Act et bien que Huawei soit dans la ligne de mire de pays tels que les États-Unis ou la France depuis des années, cette firme n'avait jamais suscité aucune réaction institutionnelle d'une telle intensité – c'est-à-dire, le veto américain – jusqu'au moment où elle s'est imposée comme acteur principal de la technologie 5G. Alors, deux facteurs hautement imbriqués jouent un rôle fondamental lorsque la Chambre de Commerce américaine inclut Huawei dans sa liste noire : le leadership chinois dans la standardisation de la 5G et la guerre commerciale sino-américaine. **Ces phénomènes dépassent ainsi les enjeux liés à la cybersécurité** : on entre de plain-pied dans les enjeux économiques. Julien Nocetti l'explique : « L'affaire Huawei illustre tout à la fois le repli technologique américain, […] et **la crainte de Washington de perdre sa supériorité technologique face à Pékin**. Depuis deux décennies en effet, Washington a fait du contrôle des données l'axe prioritaire de sa stratégie économique centrée autour de ses géants de la *tech* et de sa stratégie de sécurité » [22].

La réaction européenne face à sa situation de dépendance

L'UE n'est pas étrangère à cette situation, consciente que les enjeux entourant le réseau 5G et Huawei sont loins d'être simplement liés à la cybersécurité. Le comportement des États-Unis s'expliquerait aussi par la crainte de perdre progressivement leur supériorité technologique et économique et commerciale face à Pékin. Pour cette raison, **l'UE tente de maintenir**

l'équidistance entre les deux puissances sans pointer directement du doigt un pays ou une entreprise, comme l'ont fait les États-Unis. Le groupe NIS concentre son analyse principalement sur la qualité des équipements du réseau 5G, mais nullement sur leur provenance. De plus, le vieux continent ne peut pas rejeter frontalement Huawei comme l'ont fait les États-Unis car il dépend de cette firme pour la mise en place du réseau 5G.

C'est pourquoi la 5G altère de manière substantielle les rapports entre les Etats-Unis et l'UE. Pour ainsi dire, l'habitat naturel de l'Union européenne serait aux côtés des États-Unis, son allié historique. Washington est le partenaire privilégié de Bruxelles, non seulement en raison de l'étroite collaboration qui existe entre les deux à travers des organisations telles que l'OTAN, mais aussi à cause des nombreux échanges commerciaux et d'informations entre les américains et plusieurs pays de l'Union [23]. Néanmoins, elle s'éloigne du veto américain, alors qu'elle cherche de plus en plus à prendre ses distances à l'égard de Washington afin de développer sa propre technologie et son industrie numérique. La dépendance vis-à-vis des GAFAM compromet la souveraineté de l'UE, notamment dans la gestion et l'exploitation des données européennes, un enjeu majeur aujourd'hui auquel Commission von der Leyen s'intéresse depuis le début de son mandat [24].

Il faut aussi remarquer que si l'actuelle Commission européenne semble plus déterminée à renverser les rapports de forces autour de l'alliance transatlantique, autour des initiatives européennes de souveraineté technologique et numérique ont été mises en place auparavant. La stratégie suivie auparavant par la Commission a consisté à renforcer les mécanismes de défense chargés de protéger les données personnelles des citoyens européens [25]. De cette initiative est né le Règlement Général de Protection des Données (RGPD), approuvé en 2018. Conçu comme un mécanisme avec une composante géostratégique importante, le RGPD vise à protéger les données européennes stockées dans les serveurs des GAFAM américains [26].

Du côté chinois, même si les principaux Etats membres s'opposent au veto de Huawei, l'UE durcit aussi les termes de son rapport avec la Chine. Au cours de la dernière décennie, les puissances européennes ont été séduites par l'Empire du Milieu lorsque son poids dans l'économie mondiale a augmenté. Néanmoins, après l'avoir accusé à plusieurs reprises de vol de propriété intellectuelle, d'espionnage industriel et de ne pas respecter les accords des organisations internationales comme l'OMC, l'UE considère aujourd'hui la Chine comme un « rival systémique » : à la fois un partenaire commercial important, mais aussi un rival économique, politique et idéologique [27]. Les critiques de la Commission européenne se concentrent surtout sur son manque répété d'engagement envers les principes de l'OMC, qui exige la réciprocité – l'ouverture du marché chinois aux investissements européens -, et sanctionne le *dumping* chinois [28].

L'absence manifeste de réciprocité se pose lorsque les pays de l'UE rencontrent des obstacles pour investir ailleurs - la Chine étant un des pays où les investissements se font très difficilement. De plus, les investissements étrangers sont parfois réalisés dans des domaines hautement stratégiques de l'industrie européenne. Pour éviter ce problème, la Commission a lancé en 2016 l'*International Procurement Instrument* (IPI) [29], un instrument légal destinée à lutter contre la situation désavantageuse dans laquelle se trouve l'UE, et soutenir les investissements des États membres dans les pays en-dehors de la zone euro. Une date butoir pour la mise en œuvre de cette procédure a été fixée pour fin 2019, mais le rejet de certains pays tel que l'Allemagne ayant de bonnes relations avec le marché chinois l'a jusqu'à présent

freiné [30].

En cela, l'Union européenne vise à réduire sa relation de dépendance économique et technologique vis-à-vis des États-Unis et de la Chine après avoir vu sa base de pouvoir se réduire en raison de sa forte dépendance envers les GAFAM, ainsi que des télécoms chinoises. Elle met en place une série de mécanismes protectionnistes pour remédier à cette situation et récupérer son espace d'autonomie. Lors de la publication du rapport « Une Europe adaptée à l'ère du numérique » [31], le commissaire européen au Marché intérieur, Thierry Breton, utilisait l'expression « guerre des données industrielles ». Cette représentation belliqueuse réaffirme **la nécessité pour l'UE de prendre le contrôle souverain de sa production de Big Data industriel**, qui devrait se multiplier de façon exponentielle avec l'arrivée de la 5G et l'Industrie 4.0. **L'avenir de l'Union européenne passe par la récupération d'une partie de son autonomie dans la sphère numérique**, sachant qu'environ 90% des données de tout l'Occident sont stockées aux États-Unis [32]. « Les règles du jeu ont changé », soulignent les ministres de la France, Bruno Le Maire, et de l'Allemagne, Peter Altmaier ; l'UE doit commencer à renforcer ses liens institutionnels avec les entreprises dans les secteurs les plus stratégiques [33]. Ces mesures viendront remédier au problème de la dépendance technologique européenne, illustré dans la Figure 1.

Cependant, tandis que les acteurs sont de plus en plus éloignés les uns des autres, l'écosystème des avancées technologiques qui accompagne le réseau 5G nécessite une intégration beaucoup plus grande entre Etats, acteurs publics et privés. Par exemple, l'industrie automobile du futur présentera un degré élevé d'interdépendance, car la chaîne de valeur deviendra plus internationale et incorporera un plus grand nombre de composants stratégiques. La Chine cherche à être le principal fournisseur des batteries au lithium qui alimenteront les futures voitures électriques [34], dont beaucoup seront autonomes et utiliseront le réseau 5G pour se déplacer. Des champions européens, tels qu'Audi ou Daimler collaborent avec Huawei depuis des années dans les véhicules autonomes. Un exemple paradigmatique de la hausse de l'interdépendance de l'industrie automobile c'est notamment le cas des *5G corridors*, que l'auteur présente plus en profondeur dans le dernier numéro de l'ECJ [35].
Comment gérer cette situation ? Dans un monde interconnecté où, surtout dans le domaine cyber, les systèmes d'interdépendances sont si forts, l'UE fait appel à l'autonomie stratégique [36] [37]. Alors que la souveraineté est le cadre juridique selon lequel un acteur étatique peut légiférer et gouverner dans ses frontières, l'autonomie stratégique est la capacité *de facto* de cet État à réaliser cet objectif. Ce concept permet de traiter la notion de souveraineté dans un monde fortement interconnecté : lorsque les nations sont dépendantes les unes des autres, leur autonomie devient stratégique. Selon des auteurs comme Paul Timmers qui ont traité ce sujet, trois voies mènent à l'autonomie stratégique : la gestion des risques, les alliances stratégiques et la promotion du bien commun. La gestion des risques agit comme un système de défense qui envisage tout incident possible en réagissant de manière organisée, grâce à une étroite collaboration entre les secteurs public et privé. Les alliances stratégiques viennent renforcer la

souveraineté par le biais d'accords internationaux et de coalitions. Que ce soit avec des pays qui partagent les même valeurs (*like-minded*) ou pas, l'important est de promouvoir des scènarios où tout le monde gagne (*win-win)*. Enfin, le but ultime est de promouvoir le bien commun global à travers des initiatives telles qu'un Internet décentralisé qui utilise des mécanismes comme la chaîne de blocs (*blockchain)*.

> A lire sur Diploweb.com François Géré : Communication et désinformation à l'heure d'Internet, des réseaux sociaux et des théories du complot

Evolution des représentations autour du système d'alliances français

La France est dans une situation très similaire à ses homologues européens et, comme dans d'autres Etats membres, le déploiement du réseau 5G ne peut être compris sans regarder son histoire récente. À ce jour, aucune force politique française ne s'oppose frontalement à travailler avec Huawei, au contraire que l'administration Trump. Cependant, les rapports du Sénat français datant d'il y a environ huit ans montrent que le rejet de Huawei serait partagé par certaines composantes politiques et que l'alliance avec les États-Unis recevait alors plus de soutien qu'aujourd'hui. Ainsi, il est nécessaire de se reporter à une série d'événements qui ont eu lieu en France ces dernières années pour comprendre ce basculement dans le système d'alliance français.

En 2012, un nouveau rapport sur la cybersécurité du sénateur Jean-Marie Bockel souligne les rivalités de pouvoir avec la Chine, ennemi de la France dans le domaine du cyberespace. Les représentations mises en jeu dans ce rapport sur l'alliance transatlantique avec les États-Unis évoquent un partenariat solide. Tout au long du texte, Bockel prête attention non seulement aux cyber-attaques chinoises, mais aussi à la menace potentielle pour la souveraineté nationale que présentent les équipements chinois des géants de télécoms Huawei et ZTE. Ainsi, le positionnement du sénateur Bockel arrive même à se pencher sur le rejet direct de l'installation d'infrastructures et d'autres équipements provenant de ces entreprises. Entre-temps, les opérateurs français ont déjà commencé à travailler avec Huawei. Bouygues Télécom signe un accord de collaboration avec Huawei dès 2009 qui est renforcé en 2011 [38]. La collaboration entre SFR et Huawei commence encore plus tôt [39].
L'entrée de Huawei dans le marché français n'a pas seulement été privilégiée par le soutien des banques publiques chinoises. Pékin a été accusé à plusieurs reprises par la concurrence de mener des opérations de plagiat pour compenser leur retard en matière de R&D. Ainsi, la Chine a eu recours à de nombreux échanges entre institutions académiques et alliances commerciales pour collecter des informations sur le savoir-faire de ses rivaux, allant jusqu'à voler la propriété intellectuelle de la concurrence. **Ces pratiques, conjuguées au manque de réactivité du gouvernement français, pourraient avoir précipité la chute du champion des télécommunications français Alcatel**. L'un des premiers échecs du fleuron français a été la délocalisation d'une partie de ses usines en Chine, ce qui a entraîné le transfert (volontaire) et l'appropriation (involontaire) des connaissances sur les produits de la firme. Plus tard, Alcatel a vérifié en 2006 que le code utilisé par Huawei dans l'équipement installé par l'opérateur British Telecom était identique au sien [40].

Alcatel ayant pris conscience de ces événements, ses dirigeants ont rapidement alerté Matignon pour savoir s'ils pouvaient compter sur le soutien du gouvernement. Quelques jours plus tard, le gouvernement français les a informés qu'il n'y aurait pas de réaction de sa part, en raison des dimensions que le conflit pourrait prendre. Le directeur de l'entreprise de l'époque, Serge Tchuruk, a tenté de mener la bataille de son côté, mais en raison de ses liens étroits avec la Chine (dix-sept co-entreprises dans le pays), ses mains étaient liées. Finalement, Huawei a versé une indemnité symbolique à Alcatel, une compensation malhonnête compte tenu de ce qu'Alcaltel avait perdu. Un ancien cadre d'Alcatel soutient que **cette manœuvre à fait gagner à Huawei dix années de R&D** suffisant pour donner le coup de grâce à la firme française, qui finit par être achetée en 2016 par le finlandais Nokia [41].

Les opérations de Huawei en France se sont aussi diversifiées au fil des années. En 2017, le groupe automobile PSA, dont font partie les marques emblématiques de la voiture française Citroën et Peugeot, annonce un partenariat avec Huawei pour améliorer les prestations de connectivité des voitures et développer des véhicules à conduite autonome. Dans le milieu académique, Huawei forme un partenariat avec l'Institut Mines-Télécom Atlantique pour faire des recherches sur les liaisons optiques à 100 Gbit/s avec un financement de 80 000 euros. Également, des professeurs de ParisTech ont était salariés de Huawei [42]. La Figure 2 souligne visuellement le contexte historique.

En parallèle, les relations entre Paris et Washington se sont dégradées peu à peu, notamment à la suite de l'entrée de D. Trump à la Maison Blanche (janvier 2017). Après l'affaire Snowden et l'adoption du Cloud Act, la France a approuvée en janvier 2019 une loi fiscale visant les géants numériques mondiaux et qui affecte surtout les GAFAM américaines. La réponse du président Trump à cette mesure est la menace d'augmenter les tarifs douaniers imposés à certains produits français. De ce fait, aussi en 2019 et pendant le basculement du système d'alliances français, la sénatrice Catherine Procaccia publie un nouveau rapport sur la sécurité nationale et l'exploitation des réseaux radioélectriques mobiles [43]. Procaccia décrit ici le comportement des États-Unis vis-à-vis de Huawei plutôt dans le cadre d'une guerre commerciale, s'éloignant ainsi des représentations des cyber-menaces à la sécurité que Washington mettait en jeu. La sénatrice n'est pas sans arguments, mais il est important de souligner un point fondamental : l'intention de la sénatrice est de critiquer le comportement des États-Unis en passant sous silence la dépendance que la France a développée à l'égard de Huawei ces dernières années. La logique ? Si les Etats-Unis agissent dans leur intérêt économique, il est légitime pour la France de s'écarter du veto. Ce virage discursif est connu comme un *disclaimer* [44], une stratégie à travers laquelle l'orateur présente positivement son groupe d'appartenance, la France, et met l'emphase sur les attributs négatifs des *outgropus*, les États-Unis. De cette manière, Procaccia essaie de garder une bonne apparence devant l'opinion publique, tout en cachant le problème de dépendance à l'égard de la Chine.

De même, Procaccia évoque les représentations liées à la « course à la 5G ». Les notions de «

retard » et d'« efficacité » pèsent lourdement dans la représentation des enjeux liées à la 5G. **Huawei est déjà le fournisseur d'environ 50% des équipements de réseau 4G de deux des plus grands opérateurs de téléphonie mobile en France : Bouygues Telecom et SFR**. Selon le rapport, « il semble que plus un équipementier est présent dans une génération précédente, plus il a de chances d'être également retenu pour la génération ultérieure ». Procaccia parle de la transition des équipements 4G à ceux du réseau 5G comme s'ils étaient conditionnés par une sorte d'évolution naturelle. Loin d'être le cas, cette transition doit se faire sur une logique économique « efficace », car le surcoût et le retard qui résulteraient de l'absence de Huawei seraient difficilement supportables par des opérateurs comme SFR ou Bouygues. Encore une autre fois, des enjeux cybersécuritaires sont dépassés par les enjeux économiques.

Ce rapport agira comme le cadre théorique de la loi n° 2019-810 du 1er août 2019, selon laquelle le Premier ministre peut refuser l'installation d'appareils et d'équipements permettant la connectivité au réseau 5G, avec l'ARCEP comme l'organisme conseiller [45]. Cette loi, surnommée « loi Huawei », a été objet de controverses au sein du Parlement et du Sénat français lors de sa ratification. Si Agnes Pannier-Runacher argumente que « La 5G, c'est moins un enjeu « B2C », sauf dans les agglomérations extrêmement denses, qu'un enjeu « B2B » » [46] [47] cette représentation omet les améliorations que les administrations et services publics peuvent réaliser avec les nouvelles applications dérivées de la 5G, comme la télémédecine (si importante dans une crise sanitaire comme celle de la COVID-19), ou l'utilisation de la 5G pour un traitement plus efficace et écologique de l'énergie électrique.

Mais les principaux débats se concentrent autour de l'axe souveraineté technologique *versus* libre marché. Puisque le libre marché peine à encadrer la planification étatique et sa grande présence réglementaire, les forces de droite n'arrivent pas à trouver leur place dans le récit, lorsque des partis comme le PCF ou LFI embrassent l'interventionnisme accru et la récupération de l'engagement de l'Etat dans d'autres secteurs stratégiques [48]. De plus, des forces comme LFI blâment E. Macron de ne pas être intervenu en tant que ministre de l'Économie lors de la législature François Hollande, au moment de défendre Alcatel [49]. Les critiques du front souverain misent aussi sur une expansion de la base de pouvoir de l'État français par l'investissement et la planification dans d'autres secteurs stratégiques. Les mêmes qui accusent le laissez-faire de porter atteinte à la souveraineté technologique française soulignent également cette idée : approuver la « loi Huawei » et ne pas aller dans le sens d'un investissement public majeur dans les secteurs stratégiques de la production est une contradiction.

Des agendas public-privés pour un avenir numérique

Après les premières ventes aux enchères de fréquences pour la 5G, il semble que les tendances d'intégration entre la sphère publique et privée en France se consolident. Ces enchères partent d'un prix fixé par le gouvernement et à partir de là, les opérateurs enchérissent. Les enchères en France ont été différentes de celles de ses voisins. En Italie ou en Allemagne, les opérateurs ont payé environ 66 millions d'euros, alors qu'en France l'Etat n'en a collecté que 27 millions. Alors que ces enchères durent des semaines, l'affaire a été réglée ici en 2 jours. Pourquoi ces différences ? Parce que la France a reporté jusqu'à deux fois les enchères et le retard a donc été compensé en dispensant les opérateurs de débourser comme leurs voisins

[50], l'Etat assumant l'essentiel des coûts. L'État et les acteurs de la 5G doivent faire converger leurs intérêts, en tenant compte du fait que l'Elysée orchestre la concession de 100 000 millions d'euros aux secteurs stratégiques dont une partie sera destinée au lancement de l'Industrie 4.0. La France doit miser sur quatrième révolution industrielle, la robotisation permettant diminuer le coût de la main-d'œuvre de l'équation et favorisant ainsi le rapatriement industriel.
Bien que les politiques commerciales soient maintenues, les Etats envisagent s'écarter les uns des autres pour protéger leur intégrité et systèmes de sécurité, mais surtout pour défendre leurs intérêts économiques. Dans le cas de la France, il est important que le gouvernement oriente le plan de relance avec le système de contreparties, pour que les entreprises misent vraiment sur l'Industrie 4.0 et le rapatriement industriel. Ne pas changer la dynamique de fermeture des usines françaises et de délocalisation peut supposer le gaspillage de cet énorme budget pour finalement être dans une position encore pire dans le long terme.

Les tensions de la géopolitique de la 5G font partie d'un enjeu plus vaste auquel sont aujourd'hui confrontées les principales puissances mondiales : celui de la dépendance technologique. Les Etats qui ne disposent pas d'un muscle technologique et numérique propre, notamment au sein de l'UE, aurons recours à l'autonomie stratégique pour combler leurs dépendances en matière technologique. Mais cette situation est provisoire, puisqu'aucun acteur ne veut dépendre à long terme des puissances étrangères pour la fourniture de biens et services stratégiques, encore moins dans le cadre d'une guerre commerciale. Le maintien de cette dynamique nuirait à leurs systèmes de cybersécurité, ainsi qu'à leurs intérêts financiers à long terme. En cela, dans le cas de la France, l'agenda post-coronavirus COVID-19 doit être marqué par une plus grande synergie entre l'État et les entreprises, qui favorise la mise en œuvre de l'Industrie 4.0, ainsi que le rapatriement industriel. Si l'État ne change pas d'attitude et continue de fournir des lignes de crédit aux entreprises sans demander des contreparties, alors qu'elles délocalisent leur production et n'investissent pas dans la R&D, le tissu industriel français sera gravement endommagé à l'avenir, car il en aura peu à offrir contre la concurrence.

Bonus. Masterclass géopolitique. Quels sont les fondamentaux de la puissance ?

Le monde change, tous les jours, peut-être plus vite que jamais, mais la puissance reste. La puissance reste, mais elle change elle aussi, tous les jours, dans ses modalités. Pourtant, il y a des fondamentaux. Lesquels ? C'est ce que vous allez découvrir et comprendre. Ainsi, vous marquerez des points. Des points décisifs à un moment clé.

P.-S.

Étudiant en Master 2 Cyberstratégie et terrain numérique à l'Institut Français de Géopolitique (Université Paris 8), Arsenio Cuenca s'intéresse aux enjeux liés aux technologies stratégiques auxquels la société internationale fait face aujourd'hui. Il est actuellement apprenti au sein du Pôle national de luttes contre les cybermenaces de la Direction Générale de la Gendarmerie Nationale (DGGN).

Notes

[1] Ramadhan, A. J. (2019). « 5G Network Goals : A Comparative Investigation of the Spectral Efficiencies and Other Performance Parameters of 4G OFDM and 5G OFDM Signals ». J. Eng. Appl. Sci. Accepted

[2] Triolo, P., Allison, K. & Brown, C. (2018) « The Geopolitics of 5G ». Eurasia Group. Date de consultation : 15/05/2020. Source : https://www.eurasiagroup.net/siteFiles/Media/files/1811-14%205G%20special%20report%20public(1).pdf

[3] Andrews, J. G., Buzzi, S., Choi, W., Hanly, S. V., Lozano, A., Soong, A. C., & Zhang, J. C. (2014). « What will 5G be ? ». IEEE Journal on selected areas in communications, 32(6), 1065-1082

[4] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). « Internet of things : A survey on enabling technologies, protocols, and applications ». IEEE communications surveys & tutorials, 17(4), 2347-2376

[5] Ministère de l'Économie de l'Industrie et du Numérique (2016) « TECHNOLOGIES CLÉS. Préparer l'industrie du futur. 2020 ». Date de consultation : 15/05/2020. Source : https://www.entreprises.gouv.fr/files/files/directions_services/politique-et-enjeux/innovation/technologies-cles-2020/technologies-cles-2020.pdf

[6] L'industrie 4.0 n'est pas une option pour notre économie. Source : https://www.lesechos.fr/idees-debats/cercle/lindustrie-40-nest-pas-une-option-pour-notre-economie-1160455

[7] Sadeghi, A. R., Wachsmann, C., & Waidner, M. (2015). « Security and privacy challenges in industrial internet of things ». In 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC) (pp. 1-6). IEEE

[8] How It Works : Internet of Things. Source : https://www.ibm.com/blogs/nordic-msp/how-it-works-internet-of-things/

[9] Santé, énergie et transports, entre autres.

[10] NIS Cooperation Group (2019) « EU coordinated risk assessment of the cybersecurity of 5G networks ». Date de consultation : 20/05/2020. Disponible en : https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049

[11] Popławski, P. (2019) « Germany is open to Huawei's participation in 5G ». OSW, Octobre, 23. Date de la consultation : 03/11/2019. Disponible en : https://www.osw.waw.pl/en/publikacje/analyses/2019-10-23/germany-open-to-huaweis-participation-5g

[12] Bellanger, M. P. (2014). *La Souveraineté numérique*. Éditions Stock, Paris.

[13] Ahmed, S., & Weber, S. (2018). « China's long game in techno-nationalism ». First Monday.

[14] Bataille géopolitique autour de la 5G. Source : https://www.monde-diplomatique.fr/2020/10/MOROZOV/62292

[15] Kim, M. J., Lee, H., & Kwak, J. (2020). "The changing patterns of China's international standardization in ICT under techno-nationalism : A reflection through 5G standardization". International Journal of Information Management, 54, 102145.

[16] Sadin, E. (2016) *La siliconisation du monde*. L'échappée, Paris.

[17] Mazzucato, M. (2013) *The Entrepreneurial State. Debunking Public vs. Private Sector Myths*. Penguin Group, Londres.

[18] Daskal, J. (2018) « Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0. ». Stan. L. Rev. Online, 71, 9.

[19] Microsoft handed the NSA access to encrypted messages. Source : https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data

[20] Arpagian, N. (2012) « Les entreprises, complices et victimes de la « cyberguerre » ? Revue internationale et stratégique. Armand Colin, n° 87 | pages 65 à 72

[21] Cyber sécurité : la main de fer chinoise. Source : https://portail-ie.fr/analysis/2234/cyber-securite-lamain-de-fer-chinoise

[22] Donald Trump et l'affaire Huawei : un pari hasardeux ? Source : https://www.liberation.fr/debats/2019/05/24/donald-trump-et-l-affaire-huawei-un-parihasardeux_1729269

[23] Esteban, M. Otero-Iglesias, M. Berzina-Cerenkova, U. A. Ekman, A. Jerdén, B. Poggeti, L. Seaman, J. Summers, T. Szczudlik, J. (2020) « Europe in the Face of USChina Rivalry ». European Think-tank Network on China (ETNC). Date de consultation : 23/03/2020. Disponible en : http://www.realinstitutoelcano.org/wps/portal/rielcano_en/publication?WCM_GLOBAL_CONTEXT=/elcano/elcano_in/publications/etnc-europe-in-the-face-of-us-chinarivalry

[24] A Union that strives for more. My agenda for Europe. Source : https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf

[25] Gomart, T., Nocetti, J. & Tonon, C. (2018) « L'Europe : sujet ou objet de la géopolitique des données ? ». Études de l'IFRI. Date de consultation : 20/05/2020. Disponible en : https://www.ifri.org/sites/default/files/atoms/files/gomart_nocetti_tonon_europe_geopolitique_des_donnees_2018.pdf

[26] Ibid.

[27] European Commission and HR/VP contribution to the European Council (2019) "EU-China – A strategic outlook". Source : https://ec.europa.eu/commission/sites/beta-political/files/communication-euchina-a-strategic-outlook.pdf

[28] Selon la politique européenne, une entreprise fait du *dumping* si elle exporte un produit vers l'UE à un prix inférieur à la valeur normale du produit. L'Etat chinois met en jeu cette pratique au moment ou il subventionne les entreprises chinoises avec des fonds publics, pour qu'elles puissent vendre ses produits à faibles coûts dans les marchés européennes. Source : https://ec.europa.eu/trade/policy/accessing-markets/trade-defence/actions-against-imports-into-the-eu/anti-dumping/

[29] REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. Source : http://trade.ec.europa.eu/doclib/docs/2016/january/tradoc_154187.pdf

[30] Brattberg, E., & Le Corre, P. (2020). « The EU and China in 2020 : More Competition Ahead ». Carnegie Endowment for International Peace. Date de consultation : 21/02/2020. Disponible en : https://carnegieendowment.org/2020/02/19/eu-and-chinain-2020-more-competition-ahead-pub-81096

[31] Une Europe adaptée à l'ère du numérique. Source : https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_fr

[32] L. Laurent (2019), 'Macron and Merkel are caught in a New Cold War', Bloomberg, 14/XI/2019, https://www.bloomberg.com/opinion/articles/2019-11-14/technological-sovereignty-france-and-germany-join-a-new-cold-war.

[33] Berlín y París exigen protección frente a las empresas chinas. Source : https://www.lavanguardia.com/economia/20200207/473315061502/ue-europa-proteccion-empresaschinas-norteamericanas-gigantes-digitales.html

[34] Lebedeva, N. Di Persio, F. & Boon-Brett, L. (2016). « Lithium ion battery value chain and related opportunities for Europe ». European Commission, Petten. Date de Consultation : 17/04/2020. Disponible en : https://ec.europa.eu/jrc/sites/jrcsh/files/jrc105010_161214_liion_battery_value_chain_jrc105010.pdf

[35] Cuenca-Navarrete, A. (2020) « 5G Corridors, a Promising Investment in Europe's Technological Sovereignty ». *European Cybersecurity Journal*. Vol 6 Issue 2 pp. 61-67. Disponible en : https://cybersecforum.eu/wp-content/uploads/2020/09/ECJ_vol6_issue2_online_v1.pdf

[36] Timmers, P. (2019) « Strategic Autonomy and Cybersecurity ». Policy in focus, EU Cyber Direct.

[37] Timmers, P. (2020). « There will be no global 6G unless we resolve sovereignty concerns in 5G governance ». Nature Electronics, 3(1), 10-12.

[38] Huawei Device renforce son partenariat avec Bouygues Telecom. Source : https://www.channelbp.com/content/huawei-device-renforce-son-partenariat-avec-bouygues-telecom

[39] Le magazine Communicate est une publication gérée par la même société Huawei. L'interview mentionnée ici, intitulée "SFR : 1 + 1> 2" fait partie du numéro 50. Source : https://www.huawei.com/ilink/en/download/HW_079232

[40] Izambard, A. (2019*) France-Chine. Les liaisons dangereuses*. Stock, Paris.

[41] Ibid.

[42] Ibid.

[43] Procaccia, C. (2019) « Rapport fait au nom de la commission des affaires économiques (1) sur la proposition de loi, ADOPTÉE PAR L'ASSEMBLÉE NATIONALE APRÈS ENGAGEMENT DE LA PROCÉDURE ACCÉLÉRÉE, visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles ». Gouvernement Français, Sénat de France. Session ordinaire de 2018-19

[44] Van Dijk, T. (1996). « Análisis del discurso ideológico ». *Versión*, 6. 15-43.

[45] LOI n° 2019-810 du 1er août 2019 visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles (1). Cf Annexe 5. Page 74. Source : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000038864094&categorieLien=id

[46] RAPPORT FAIT AU NOM DE LA COMMISSION DES AFFAIRES ÉCONOMIQUES SUR LA PROPOSITION DE LOI visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles (n° 1722). PAR M. ÉRIC BOTHOREL. Source : http://www.assemblee-nationale.fr/dyn/15/rapports/cion-eco/l15b1832_rapportfond

[47] Ibid.

[48] AVIS FAIT AU NOM DE LA COMMISSION DE LA DÉFENSE NATIONALE ET DES FORCES ARMÉES SUR LA PROPOSITION DE LOI (n° 1722), visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles, PAR M. THOMAS GASSILLOUD. Source : http://www.assemblee-nationale.fr/dyn/15/rapports/cion_def/l15b1830_rapport-avis

[49] Ibid.

[50] Huvé, J. & Krykwinski, C. (2019) « Adjugé vendu : l'acquisition des fréquences 5G, et la suite ». Institut Montaigne. Date de Consultation : 11/06/2020. Disponible en : https://www.institutmontaigne.org/blog/adjuge-vendu-lacquisition-des-frequences-5get-la-suite