INSTITUT
MONTAIGNE

L'Europe et la 5G : le cas Huawei

NOTE MAI 2019

Think tank indépendant créé en 2000, l'Institut Montaigne est une plateforme de réflexion, de propositions et d'expérimentations consacrée aux politiques publiques en France et en Europe. À travers ses publications et les événements qu'il organise, il souhaite jouer pleinement son rôle d'acteur du débat démocratique avec une approche transpartisane. Ses travaux sont le fruit d'une méthode d'analyse et de recherche rigoureuse et critique, ouverte sur les comparaisons internationales. Association à but non lucratif, l'Institut Montaigne réunit des chefs d'entreprise, des hauts fonctionnaires, des universitaires et des personnalités issues d'horizons divers. Ses financements sont exclusivement privés, aucune contribution n'excédant 1,5 % d'un budget annuel de 4,5 millions d'euros.

INSTITUT
MONTAIGNE

L'Europe et la 5G : le cas Huawei

NOTE - MAI 2019

Il n'est désir plus naturel
que le désir de connaissance

SOMMAIRE

INTRODUCTION

L'offre apparemment incontournable de Huawei dans la 5G, après sa conquête de nombreux marchés 4G et une percée mondiale dans les smartphones, a pris une dimension polémique et servi de révélateur d'enjeux stratégiques que les générations précédentes de réseaux mobiles n'avaient pas mis en évidence. Il y a pour cela des raisons qui tiennent à la nature de la 5G, mais aussi à la spécificité de l'entreprise Huawei.

Commençons par la 5G. On le sait, il ne s'agit pas seulement d'augmenter, en principe d'ici 2025, les débits de la communication entre individus, même si la téléphonie mobile profitera elle aussi d'une vitesse supérieure et d'un temps de latence réduit[1]. La conséquence de la rapidité et du débit de la 5G, ce sont ses multiples usages nouveaux, qu'il est aussi impossible d'anticiper que ne le furent en son temps les applications d'internet. Les usines digitales et notamment la multiplication de la production 3D, le télédiagnostic et la chirurgie à distance, l'ensemble des réseaux intelligents et la généralisation de l'internet des objets (IoT), à commencer par la conduite autonome qui est l'aspect le plus popularisé, la prééminence des *clouds* numériques sur les serveurs localisés, l'intelligence artificielle et la modernisation des services publics sont quelques-unes des conséquences prévisibles. Qui possèdera ou captera en temps réel les données et les algorithmes dominera l'industrie, les services, et aussi nombre d'aspects confidentiels de la vie humaine. La fiabilité et la sécurité des flux de données, les risques de vol, de piratage ou de sabotage seront bien plus importants que dans la dimension antérieure d'internet.

L'infrastructure 5G doit donc être considérée comme critique. Elle transformera l'activité économique, avec des conséquences positives et négatives. Elle va très vite engendrer un saut générationnel pour les entreprises et les services qui adoptent la fabrication numérique, et pénalisera donc les entreprises ou les régions qui restent en dehors du déploiement. Tout comme la 4G a permis l'émergence des géants de l'Internet, la 5G sera à l'origine de l'émergence de nouveaux grands acteurs. A l'inverse, la digitalisation étendue pose des problèmes de protection des données d'une ampleur sans précédent. On peut aussi bien imaginer le risque de sabotage de réseaux de distribution, de services publics, que la prise de contrôle à distance d'automobiles, d'appareils médicaux ou d'usines entières. La 5G est donc une promesse de productivité, mais aussi un risque de décrochage pour la compétitivité de pans entiers des économies européennes, et une question de sécurité nationale.

[1] « L'Europe et la 5G : passons la cinquième ! Partie 1 », Institut Montaigne, mai 2019, https://www.institutmontaigne.org/publications/leurope-et-la-5g-passons-la-cinquieme-partie-1

Le choix des opérateurs, des infrastructures et de leurs fournisseurs ne peut se résumer à une question d'opportunité et de coût économique. La confidentialité des données et la sécurité des flux, y compris par rapport à des interférences extérieures, sont un enjeu majeur. L'Europe a beaucoup de chemin à rattraper sur ce plan. Elle qui avait naguère créé la norme GSM se trouve aujourd'hui fragmentée en marchés nationaux structurés par un nombre limité de trois à quatre opérateurs. L'avantage immédiat de la concurrence ouverte pour les consommateurs est aujourd'hui au prix d'une faible capacité d'investissement des opérateurs et fabricants existants, et, on le verra, d'une maîtrise insuffisante de la norme 5G elle-même.

C'est ici que Huawei entre en scène. Le géant chinois – et désormais mondial – des télécommunications est hors normes à tous points de vue.

I

HUAWEI, LE FER DE LANCE DU TECHNO-NATIONALISME CHINOIS

L'entité a été créée en 1987 dans le sud de la Chine avec un capital de 21 000 Yuan par un ingénieur vétéran de l'armée chinoise formé à la cryptographie et aux transmissions électroniques. L'ex-numéro deux du groupe, Sun Yafang, aurait travaillé à la division des communications du ministère de la Sécurité d'état : des antécédents qu'on retrouve ailleurs qu'en Chine, dans de nombreuses entreprises de technologies de l'information, et par exemple en Israël dans les entreprises digitales. De nouveaux travaux soulignent la structure de propriété de Huawei, une entreprise qui communique sur ses salariés comme seuls propriétaires[2]. Quoiqu'aujourd'hui détenteur de seulement 1,14 % du capital de Huawei, Ren Zhengfei semble, avec sa famille, exercer le contrôle complet sur l'entreprise, qui est aux mains d'une entité parfois qualifiée de syndicat des employés, mais plus sûrement gérant des actions virtuelles, renouvelées chaque année, donnant aux employés pour la durée de leurs fonctions dans l'entreprise des droits très limités mais les associant aux bénéfices. Il s'agissait peut-être, dans les années 1990, d'un de ces nombreux cas d'entreprise hybride aux formules diverses, intermédiaires entre les entreprises d'état et les véritables entreprises privées, beaucoup plus petites. La composition même de cet actionnariat virtuel est inconnue, quoique Huawei prétende aujourd'hui le tenir à la disposition de chacun : en pratique, à l'ère numérique, il s'agirait de gros registres sur papier détenus dans une tour en verre ! La structure de propriété (Huawei Trade Union Committee possède 99 % de Huawei Holding qui à son tour possède Huawei Technologies, suggère un contrôle indirect du Parti, puisque tous les syndicats en Chine sont soumis à cette tutelle). Ces ambiguïtés autour de la propriété de Huawei sont réminiscences de la structure de l'économie chinoise à l'époque de sa création. Dans la deuxième moitié des années 1980 et au début des années 1990 existaient en Chine des sociétés du troisième type, en chinois « gérées par le peuple » (民 办), qui combinaient différentes formes de propriété.

A l'opacité de la propriété réelle s'ajoute celle sur les sources de financement mises à sa disposition. Avant 2011, plus de 30 milliards de prêts ont été consentis à des conditions préférentielles à Huawei (et son concurrent ZTE) pour leur développement en Chine, en grande partie par la China Development Bank (CDB), la première

[2] Christopher Balding and Donald C. Clarke, « Who Owns Huawei? » *SSRN Electronic Journal* (2019) http://dx.doi.org/10.2139/ssrn.3372669. Filip Jirouš and Jichang Lulu, « Huawei in CEE: From "strategic partner" to potential threat, » *E-International Relations* (2019), https://sinopsis.cz/en/huawei-in-cee-from-strategic-partner-to-potential-threat/ Bob Seely, Peter Varnish Obe, John Hemmings, « Defending our Data, Huawei, 5G and the Five Eyes », Henry Jackson Society (May 2019). https://henryjacksonsociety.org/wp-content/uploads/2019/05/HJS-Huawei-Report-A1.pdf

« banque politique » de l'état-parti chinois, qui reconnaît sans difficulté une relation privilégiée avec Huawei[3]. Pour les années 2012-2018, le total des financements pour des projets à l'étranger par CDB et Eximbank atteint 9,8 milliards de dollars[4]. Il semble qu'une préférence nationale aurait pu être mise en place en Chine. Huawei domine ainsi l'équipement des réseaux mobiles 4G chinois alors même que les coûts de son équipement sur le marché chinois sont supérieurs de 25 % à ceux d'un concurrent européen comme Ericsson, comme l'a démontré un appel d'offre récent[5]. L'enjeu des subventions en Chine pose une question familière de réciprocité avec l'Europe à l'heure du déploiement de la 5G.

Les liens ultérieurs avec l'armée et le cyber espionnage sont une autre zone d'ombre. A la veille de la chute du régime des talibans afghans, Huawei avait conclu un contrat de fourniture d'un réseau de fibre optique à celui-ci, comme il le fera pour l'Iran – des affaires pour lesquelles le soutien politique de l'armée chinoise semble plausible.

Dans l'ensemble, le lien avec le pouvoir chinois est ineffaçable, du fait de la nature du système politique en Chine. Il est reflété par la pénétration de Huawei par le Parti Communiste – une structure naturelle en Chine. À propos des 300 cellules et des 12 000 membres du Parti au sein des 160 000 salariés de Huawei, le secrétaire du Parti de l'entreprise, Zhou Daiqi, souligne que cet arrangement est en « conformité avec le droit chinois, que la fonction des cellules est de contribuer à l'amélioration de la qualité de vie des salariés, de s'assurer qu'ils respectent les principes de déontologie et de l'entreprise, mais qu'elles n'interfèrent pas dans la gestion et les choix politiques »[6]. En effet, le rapport de force entre le Parti et les entreprises, quelles qu'elles soient, n'a aucune raison de s'exprimer dans le quotidien de la vie de l'entreprise – seuls les moments décisifs sont susceptibles de le révéler.

La Chine déploie donc un arsenal impressionnant pour soutenir Huawei. Il n'est pas surprenant que plusieurs niveaux de l'État chinois soient directement impliqués dans la défense de Huawei contre les attaques que l'entreprise subit. Le ministre

[3] Matthew Dalton, « EU Finds China Gives Aid to Huawei, ZTE », *The Wall Street Journal* (2011), https://www.wsj.com/articles/SB10001424052748703960804576120012288591074

[4] « A Transactional Risk Profile of Huawei », *RWR Advisory Group* (2018), https://www.rwradvisory.com/wp-content/uploads/2019/03/RWR-Huawei-Risk-Report-2-13-18.pdf

[5] Davy Zhu, « Ericsson Is Surprisingly Cheapest Vendor in Huawei's China », *Bloomberg* (2019), https://www.bloomberg.com/news/articles/2019-02-14/in-huawei-s-china-ericsson-is-surprisingly-the-low-cost-vendor

[6] "互联网公司在招聘上不要党员？" (Les compagnies internet insistent-elles dans leurs offres d'emploi sur le rejet des members du Parti?) (2016), http://www.sohu.com/a/100572816_359612

des Affaires étrangères Wang Yia récemment souligné que Huawei ne devait en aucun cas se comporter comme un « agneau silencieux », que la Chine se réservait le droit de répondre par « toutes les mesures nécessaires » aux attaques contre Huawei, qu'il s'agissait de défendre les « intérêts de développement légitimes d'un pays et de ses ressortissants »[7]. Le ministère de la Sécurité d'État a arrêté plusieurs ressortissants canadiens en représailles à la procédure d'extradition aux États-Unis entamée par la justice canadienne envers la directrice financière de Huawei, Meng Wanzhou, feignant d'ignorer qu'il s'agissait d'une obligation pour le Canada liée à son traité d'extradition avec les États-Unis, et non d'une décision politique[8].

Les termes ne sont pas neutres, et les correspondances sont révélatrices. Lorsque Wang Yi qualifie Huawei « d'agneau silencieux », il ne peut ignorer le terme de « culture loup » (狼性文化), popularisé par Ren Zhengfei lui-même pour motiver ses employés[9]. La métaphore du loup a pris au fil des années une dimension identitaire pour Huawei, reflétant une culture interne à l'entreprise favorisant l'ambition, la prise de risque et le *eat what you kill,* inspirant son expansion agressive sur les marchés chinois et internationaux. Dans les années 1990, en plus de la « culture loup », les slogans de motivation du personnel de Huawei se nourrissent d'une imagerie quasi-militaire de la survie et du combat. On compte des phrases telles que « l'oiseau qui brûle sans mourir est un phénix » (烧不死的鸟是凤凰), « levons un verre lorsque nous remportons un succès, défendons-nous au prix de notre vie lorsque nous subissons une défaite » (成则举杯相庆，败则拼死相救), et de multiples références à Lei Feng, le travailleur modèle mythique des années 1960 dont la personne est encore utilisée aujourd'hui dans la propagande chinoise à destination de l'intérieur du pays. La charte interne de l'entreprise, adoptée en 1998, fait entièrement sienne le patriotisme économique : « Au service de la prospérité de notre grande mère-patrie, au service de la réjuvénation du peuple chinois » (为伟大祖国的繁荣昌盛，为中华民族的振兴)[10]. Tout récemment encore, la fille du fondateur, Meng Wanzhou, qualifie l'entreprise de « forteresse » (堡垒) dans un message diffusé aux employés[11].

[7] Ben Blanchard, « No 'silent lambs': China supports Huawei's bid for U.S. legal redress », *Reuters* (2019), https://www.reuters.com/article/us-china-parliament-huawei-tech/top-chinese-diplomat-says-supports-huaweis-bid-for-legal-redress-idUSKCN1QP089

[8] Chris Buckley and Catherine Porter, « China Accuses Two Canadians of Spying, Widening a Political Rift », *The New York Times* (2019), https://www.nytimes.com/2019/03/04/world/asia/china-canada-michael-kovrig-huawei.html

[9] 杨媚, "华为总裁任正非：缔造"狼性文化"," (Le PDG de Huawei Ren Zhengfei sur la construction d'une culture loup)中国企业报 (2011), http://dangjian.people.com.cn/GB/240027/17578570.html

[10] "《华为基本法》是什么？" (Qu'est-ce que la loi fondamentale de Huawei?) (2016), http://www.cghuawei.com/archives/2149. Texte complet : http://blog.sina.com.cn/s/blog_6263274c0102wg41.html

[11] "孟晚舟听证会后致信华为人：心中从未如此丰富而广阔，谢谢你们," (Meng Wanzhou's letter to Huawei staff after her hearing: my heart has never been that rich and wide, thank you) (2019), https://www.guancha.cn/economy/2019_05_13_501337.shtml

Alors que la communication de Huawei en Chine se nourrit d'un champ lexical martial et d'une imagerie communiste, elle procède à l'international de ressorts très différents. En Europe, le président du conseil d'administration de Huawei proclame sa « confiance dans l'ouverture et l'innovation », et aux États-Unis, Huawei se qualifie parfois de « graine de sésame »[12]. En Europe, sur les réseaux sociaux et dans la presse, Huawei est un acteur incontournable dont l'effort de relations publiques permet une couverture médiatique inégalée. Sur tout le continent, sillonné par le camion publicitaire 5G Huawei, l'entreprise conduit un programme de recrutement de talents, « graines pour le futur » *(seeds for the future)*[13]. L'entreprise recrute dans les milieux de la sécurité et de la défense, avec des prises de choix telles que Andrew Hopkins, l'ex-directeur adjoint du GCHQ, le service de renseignement de nature électronique du Royaume-Uni[14]. L'employé polonais d'Orange accusé en janvier 2019 d'espionnage en liaison avec un cadre de Huawei était un ancien responsable du contre-espionnage polonais. Huawei ne fournit pas d'information sur son site internet sur la composition de son International Advisory Council, alors que certains articles de presse en mentionnent l'existence. En 2013, aux dires de l'entourage du commissaire européen au commerce Karel de Gucht, Huawei était la multinationale qui dépensait le plus en lobbying à Bruxelles. En 2017, Huawei aurait dépensé selon ses déclarations obligatoires 2,19 millions d'euros en lobbying à Bruxelles[15]. On retrouve son sponsoring dans de nombreux évènements publics dans toute l'Europe selon son site internet[16].

Ces liens congénitaux avec la colonne vertébrale du système politique chinois permettent de mesurer l'importance de l'immense succès de Huawei à l'aune du projet national de Xi Jinping, tel que celui-ci est présenté avec une grande clarté dans une feuille de route présentée au 19e Congrès du Parti Communiste en novembre 2017 : la transformation de la Chine en « leader mondial en matière d'innovation » à l'horizon 2035, puis en « leader mondial en matière de puissance nationale composite et d'influence internationale » à l'horizon 2050[17].

---

[12] Yang Ge, « Huawei Is "Sesame Seed" Under Attack from U.S. "National Machine", Chairman Says », Caixin (2019), https://www.caixinglobal.com/2019-02-18/huawei-is-sesame-seed-under-attack-from-us-national-machine-chairman-says-101380966.html

[13] Huawei, Huawei 5G Truck Bring 5G to Public and Invite Ecosystem to Explore 5G Together (2018), https://www.huawei.com/en/press-events/news/2018/11/Huawei-5G-Truck-Public-Invite-Ecosystem

[14] Tamlin Magee, « Huawei Controversies Timeline », ComputerWorldUK (2019), https://www.computerworlduk.com/security/huawei-controversies-timeline-3692840/

[15] « Huawei Technologies (Huawei) » LobbyFacts (2019), https://lobbyfacts.eu/representative/c6677e9de90e4a2c86e5640c83e3dfbc

[16] «Events », *Huawei* (2019), https://www.huawei.com/en/press-events/events

[17] « Full text of Xi Jinping's report at 19th CPC National Congress », *Xinhua* (2017), http://www.xinhuanet.com/english/special/2017-11/03/c_136725942.htm

II

HUAWEI ET LA SÉCURITÉ DE L'EUROPE, UN DÉBAT EN TROMPE-L'ŒIL

Huawei est au cœur de l'Europe. Sur les 105 milliards de dollars de revenus de la compagnie en 2018, 24,3 % provenaient de la zone Europe/Moyen-Orient/Afrique, et 40,8 % des contrats d'équipement avec les opérateurs téléphoniques[18]. Huawei détient 17,5 % du marché des smartphones en Europe, derrière Samsung et Apple[19].

L'entreprise présente-t-elle un risque pour la sécurité nationale des États européens ? Si Huawei a toujours échoué à démontrer le contraire, ses détracteurs ont parfois apporté des indices de complicité probable de Huawei dans des opérations de cyber espionnage, mais non des preuves décisives. Citons les principales affaires : celle de l'Union Africaine, l'organisation internationale basée à Addis-Adeba, est sans conteste la plus frappante. Huawei y était depuis 2012 le fournisseur presqu'exclusif de solutions informatiques intégrées, du serveur au *cloud*, en passant par le wifi et le stockage local de données. De 2012 à 2017, toutes les nuits entre minuit et deux heures du matin, l'ensemble des données collectées était envoyé à un serveur inconnu à Shanghai… S'il est possible que des failles fortuites dans les solutions Huawei expliquent cette fuite, il n'est pas imaginable que l'entreprise ait pu ne jamais les détecter pendant cinq ans. Une autre affaire concerne les liens de Huawei, en 2015-2016, avec une entreprise chinoise, Boyusec, convaincue de cyber espionnage aux États-Unis, ainsi que les liens de ces deux entreprises avec le groupe de cyberhackeurs chinois APT-3. En 2015 et 2016, des logiciels malveillants ont été détectés dans plusieurs modèles de smartphones vendus par Huawei, Lenovo et Xiaomi, donnant accès à certains de leurs contenus[20].

Le cinquième rapport annuel du centre de cybersécurité de Huawei au Royaume-Uni, financé par Huawei mais supervisé par les services de sécurité britanniques, dont le GCHQ, donne un autre éclairage[21]. Il conclut que « l'approche de Huawei en matière de développement logiciel pose des risques importants pour les opérateurs du Royaume-

[18] Huawei Investment & Holding Co., Ltd.2018 Annual Report, https://www-file.huawei.com/-/media/corporate/pdf/annual-report/annual_report2018_en_v2.pdf?la=zh

[19] « Mobile Vendor Market Share in Europe - April 2019, » *StatCounter* (2019), http://gs.statcounter.com/vendor-market-share/mobile/europe

[20] Julien Lausson, « Des malwares pré-installés dans des mobiles Huawei, Xiaomi, Lenovo… » *Numerama* (2015), https://www.numerama.com/magazine/34130-malwares-mobiles-chinois.html

[21] « Huawei cyber security evaluation centre oversight board: annual report 2019 », *Gov.UK* (2019), https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2019

Uni (…) et le comité de supervision n'est en mesure d'apporter que des assurances limitées que les risques posés par l'équipement Huawei déployé aujourd'hui au Royaume-Uni peuvent être gérés. Les logiciels déployés par Huawei sont défectueux et comportent de nombreuses failles (« plusieurs centaines de vulnérabilités »), auxquelles Huawei n'a pas apporté de remède. Le contexte, et notamment l'usage apparent d'un OS dépassé acheté auprès d'une entreprise tierce, suggère aussi que la mauvaise qualité des logiciels Huawei n'est pas nécessairement intentionnelle : elle pourrait bien provenir tout simplement d'une indifférence plus grande à la sécurité dans le contexte de l'économie chinoise, et d'une course à l'efficacité immédiate. D'autres affaires – concernant dans un cas le réseau italien de Vodafone, puis des réseaux des Pays-Bas – sèment de nouveaux doutes sur l'existence de failles : en Italie, celles-ci semblent même avoir été réinstallées à plusieurs reprises[22].

Huawei admet cette faiblesse dans son rapport d'activité annuel[23]. Celui-ci met en avant un investissement de 2 milliards de dollars approuvé en 2018 pour l'amélioration des capacités d'ingénierie logiciel de Huawei. Pour l'entreprise, il s'agit d'un saut qualitatif nécessaire à l'heure du passage à la 5G, puisque le fonctionnement des réseaux sera défini en grande partie par son infrastructure logicielle. Cette offre est dédaignée par le rapport britannique car Huawei n'a apporté aucun détail sur son emploi. De la confusion a été créée puisque Huawei a communiqué sur un même investissement de 2 milliards de dollars (soit 23 % de son bénéfice net mondial en 2018) pour la seule sécurisation de ses équipements au Royaume-Uni, alors qu'il semble s'agir d'après son rapport annuel d'un investissement R&D pour sa croissance globale[24].

Le travail effectué par les services de cybersécurité britanniques est particulièrement important, car il s'agit du pays européen qui s'est le plus engagé dans le passé avec Huawei – 70 % de l'infrastructure 4G du pays a été construite par l'équipementier chinois. Le Royaume-Uni en tire les conséquences, puisque British Telecom a annoncé le retrait des équipements Huawei déjà installés dans les cœurs de réseau 4G[25]. Le débat fait aujourd'hui rage au Royaume-Uni sur le périmètre à laisser à Huawei

[22] Daniele Lepido, « Vodafone Found Hidden Backdoors in Huawei Equipment », *Bloomberg* (2019), https://www.bloomberg.com/news/articles/2019-04-30/vodafone-found-hidden-backdoors-in-huawei-equipment. Huib Modderkolk, « Huawei mogelijk betrokken bij Chinese spionage in Nederland », *deVolkskrant* (2019), https://www.volkskrant.nl/nieuws-achtergrond/huawei-mogelijk-betrokken-bij-chinese-spionage-in-nederland~b4fadc1c/?referer=https%3A%2F%2Fwww.forbes.com%2F

[23] « Huawei Investment & Holding Co., Ltd. 2018 Annual Report », *Huawei* (2018), https://www-file.huawei.com/-/media/corporate/pdf/annual-report/annual_report2018_en_v2.pdf?la=zh

[24] Jack Stubbs, « Huawei $2 billion security pledge followed walkout by British official - sources », *Reuters* (2018), https://uk.reuters.com/article/uk-huawei-europe-britain/huawei-2-billion-security-pledge-followed-walkout-by-british-official-sources-idUKKBN1OC23Q

[25] Alex Hern, « BT removing Huawei equipment from parts of 4G network », *The Guardian* (2018), https://www.theguardian.com/technology/2018/dec/05/bt-removing-huawei-equipment-from-parts-of-4g-network

dans la construction de l'infrastructure 5G. Tous les réseaux de télécommunications sont vulnérables à l'espionnage, au sabotage et au chantage en cas de confrontation avec un État capable de les paralyser. Les failles de Huawei, comme celles de tout autre fournisseur d'équipement réseau, peuvent être exploitées par tout service de renseignement disposant des capacités techniques suffisantes. D'un côté, les autorités britanniques appliquent un principe de précaution rétrospectif aux cœurs de réseaux 4G, de l'autre le débat n'est pas clos sur la 5G.

Deuxième nuance importante, les cas d'espionnage industriel chinois documentés en source ouverte se sont en général appuyés sur des vecteurs autres que la maîtrise de l'équipement réseau : l'hameçonnage, les failles humaines et les vulnérabilités logiciel[26]. Dans le domaine public, il existe un seul cas émanant des services de renseignement australien d'opération d'espionnage chinoise au moyen de codes fournis par Huawei permettant l'intrusion dans un réseau produit par l'équipementier[27]. Ce cas est peu documenté. Tout indique que les équipements Huawei sont très vulnérables, et que dans certains cas l'entreprise a fermé les yeux, mais les preuves manquent pour démontrer que Huawei installe des portes dérobées dans son architecture réseau pour le compte des services de renseignement chinois. En revanche, l'histoire de l'entreprise est émaillée de cas d'espionnage et de vol de propriété intellectuelle ayant impliqué certains employés aux États-Unis. S'il a lieu, le procès de la directrice financière Meng Wanzhou après son extradition aux États-Unis permettra de déterminer jusqu'à quel point Huawei a mis en place un système de fraudes pour violer les sanctions des Nations Unies à l'égard de l'Iran[28].

Or, dans un écosystème 5G, de nombreuses failles potentielles sont exploitables par des groupes malintentionnés, d'autant que l'équilibre entre le niveau des attaquants et les mises à jour des systèmes défensifs sera en perpétuelle évolution. L'approche parole contre parole centrée sur le risque de cheval de Troie occulte le fait que l'origine de l'équipement ne sera pas le point d'entrée unique à défendre pour gérer la cybersécurité dans une architecture 5G. L'écosystème 5G multiplie les vulnérabilités exploitables à différents points d'entrée du réseau, créant de nouveaux défis pour la sécurisation des flux de données qui ne sont pas liés uniquement à l'architecture

[26] Jan-Peter Kleinhans, « 5G vs. National Security - A European Perspective », *Think Tank für die Gesellschaft im technologischen Wandel* (2019), https://www.stiftung-nv.de/sites/default/files/5g_vs._national_security.pdf

[27] « China Used Huawei To Hack Network Says Secret Report », *The Australian*, (2018) https://www.theaustralian.com.au/nation/china-used-huawei-to-hack-network-says-secret-report/news-story/510d3b17c2791cbcac18f047c64ab9d8

[28] « Chinese Telecommunications Conglomerate Huawei and Huawei CFO Wanzhou Meng Charged With Financial Fraud », *The United States Department of Justice* (2019), https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-huawei-cfo-wanzhou-meng-charged-financial

des cœurs de réseau et de l'équipement radio. L'architecture logiciel opérant sur le réseau, le stockage des données dans le *cloud* et les objets connectés sont les points de vulnérabilité les plus évidents, qui demanderont de nouvelles mesures de défense mises en œuvre par les opérateurs et les États.

En revanche, la question de confiance soulevée par Huawei ne souffre pas de nuance. L'entreprise a mal géré la controverse sur ses obligations envers le droit chinois. L'article 7 de la loi nationale sur le renseignement de 2017 dispose que toutes les entreprises, « ainsi que les citoyens, doivent soutenir, coopérer et collaborer au travail national de renseignement, et préserver le secret sur le travail national de renseignement dont ils ont connaissance »[29]. Cet article a entamé la crédibilité de Huawei car l'entreprise ne peut pas réécrire le fonctionnement du système chinois, où la branche juridique est soumise au pouvoir exécutif, et celui-ci au Parti. L'absence de séparation des pouvoirs est une caractéristique des régimes léninistes, qui l'ont même théorisée comme un élément de supériorité sur les systèmes démocratiques.

Dans ce contexte, le déni en bloc, y compris de la part de Ren Zhengfei qui est sorti de son silence à cette occasion pour proclamer que si Xi Jinping lui-même lui ordonnait d'utiliser ses équipements pour espionner, il ne lui obéirait pas « en vertu de la Constitution », peine à convaincre[30]. Entre la branche exécutive du pouvoir chinois et le monde des entreprises, qu'il soit public et privé, le rapport de force est tel qu'aucun acteur économique ne peut espérer opposer une fin de non-retour à une demande du parti-Etat sans coût important. Les disparitions soudaines de chefs d'entreprise ces dernières années, de Fosun à Anbang, CEFC et HNA en sont une démonstration éclatante[31]. Dans son argumentation légale, Huawei met en avant la protection juridique accordée aux entreprises dans le droit chinois, ou la primauté du principe de protection de la vie privée dans la Constitution de la RPC (article 40, qui limite cette protection dans les cas liés à la sécurité nationale)[32]. Ces arguments ne résistent pas à l'observation de l'arbitraire dans l'exercice du pouvoir en Chine.

[29] « National Intelligence Law of the People's Republic of China (2018 Amendment) [Effective] », *Standing Committee of the National People's Congress* (2018), http://en.pkulaw.cn/display.aspx?cgid=313975&lib=law

[30] « Huawei founder says he would defy Chinese law on intelligence gathering," *CBS News* (2019), https://www.cbsnews.com/news/huawei-president-ren-zhengfei-says-he-would-defy-chinese-law-on-intelligence-gathering/

[31] Ann M. Simmons, "Some of China's richest and most powerful men have mysteriously vanished," *Los Angeles Times* (2017), https://www.latimes.com/la-fg-china-billionaires-vanish-20170614-story.html

[32] « Is Huawei compelled by Chinese law to help with espionage? » *Financial Times,* (2019) https://www.ft.com/content/282f8ca0-3be6-11e9-b72b-2c7f526ca5d0. Voir aussi: « Chapter II The Fundamental Rights and Duties of Citizens » *Constitution of the People's Republic of China* (2004), http://www.npc.gov.cn/englishnpc/Constitution/2007-11/15/content_1372964.htm

Il y a une certaine ironie à ce que la loi sur le renseignement, issue d'une démarche administrative visant à clarifier les obligations de chaque acteur en Chine, offre un argument contre Huawei à des officiels en Europe ou aux États-Unis qui projettent sur le système chinois le fonctionnement de leur propre État de droit. Les obligations du secteur privé envers le pouvoir exécutif sont d'ordre politique, au-delà des précisions réglementaires. Mais la singularité de l'ère Xi Jinping, c'est d'avoir voulu codifier dans la loi la domination du Parti sur l'état, et celle du Parti-état sur le pays – le Parti dirige tout (党是领导一切), une expression rajoutée à la Charte du PCC à la suite de son 19e Congrès[33].

Le débat sur les manquements effectifs de Huawei à la sécurisation des données est bien réel, même si les preuves d'une complicité effective dans un acte de cyberespionnage manquent : seul l'affaire de l'Union Africaine s'en approche. Les contre-mesures existent, mais elles sont limitées en efficacité par rapport à cette réalité : Huawei et ses dirigeants ne pourraient en aucun cas s'opposer à une action de pénétration ou de sabotage par les services de leur pays, si même ils en avaient connaissance. C'est donc à chacun d'évaluer la portée du principe de précaution nécessaire, y compris par rapport à des fournisseurs d'autres nationalités, ainsi que le risque particulier que peuvent résulter des actions de ces services ou leurs affidés – hackeurs organisés et régimes proches, tels que la Corée du Nord. Ce risque sera sans cesse changeant, et il est évident que certains pays européens, sans parler des opérateurs eux-mêmes, si même ils connaissent ces risques, n'ont pas les moyens techniques et humains d'y parer.

[33] 薛万博, "怎样认识"党是领导一切的"写入党章？" (How to understand the inclusion in the Party Charter of the Party leads everything?" CPC News (2018), http://cpc.people.com.cn/n1/2018/0125/c123889-29787340.html

III

L'EUROPE EN ORDRE DISPERSÉ

Alors que le déploiement commercial de la 5G a commencé aux États-Unis et en Corée du Sud, l'Europe avance en ordre dispersé. La fragmentation de l'Europe est double : elle concerne le marché des enchères et les normes de sécurité. Chaque espace de déploiement est ainsi national, avec une multitude d'opérateurs qui acquittent des frais élevés d'accès aux fréquences, résultant dans un marché soumis à une intense concurrence sur les prix. Les efforts louables de l'Union européenne ont surtout visé les aspects perceptibles des consommateurs – en particulier la baisse du coût des appels voix et des flux de données à l'intérieur de l'UE. Louable en soi, cette politique réduit aussi l'ARPU – revenu moyen par abonné, et par conséquent les marges d'investissement des opérateurs européens dans les réseaux du futur. Avec un marché à une échelle immense, un tout petit nombre d'opérateurs, des subventions massives à la création de nouveaux standards, la Chine a des revenus par abonné très voisins. Aux États-Unis, la concentration des opérateurs, critiquée en termes de concurrence insuffisante, laisse des revenus beaucoup plus confortables.

Cette structuration du marché explique pourquoi les pays européens en sont aujourd'hui à différents stades de construction de leur infrastructure 5G. En l'absence d'un marché unique des télécoms au sein de l'UE, chaque pays est responsable de la mise en place d'enchères pour l'attribution des fréquences de déploiement de la 5G. Il s'agit d'une étape politique – les règles d'enchères fixent les exigences en matière de couverture du territoire et de qualité du service, déterminent le calendrier de déploiement et arrêtent le nombre d'opérateurs réseau. Cette fragmentation a contribué à ce que l'Europe, qui fut naguère à l'origine de la norme GSM, perde le leadership dans la constitution de la norme 5G. Huawei est aujourd'hui en tête en nombre de brevets 5G, devant Nokia, LG et Ericsson[34]. Du point de vue de Huawei, l'avènement de la 5G représente un saut qualitatif puisque l'entreprise est parmi les leaders de la définition des normes et des standards, en particulier au sein du 3GPP, un regroupement d'organisations de production des standards de télécommunication qui œuvre à leur harmonisation[35]. Du point de vue des intérêts de l'Europe, cette évolution souligne l'amorce d'un décrochage technologique.

La conséquence à long terme est claire. La Chine a un plan d'investissement dans les trois années à venir, évalué entre 180 et 220 milliards de dollars – un montant

[34] Shuli Ren, « China's 5G Riches Are a Blocked Number for Investors », *Bloomberg Opinion* (2019), https://www.bloomberg.com/opinion/articles/2019-02-11/china-s-5g-winners-are-out-of-reach-for-stock-investors

[35] « About 3GPP Home », 3GPP, https://www.3gpp.org/about-3gpp/about-3gpp

qui n'est même pas si élevé, une fois qu'on le rapporte aux 800 millions de mobiles et aux milliards d'objets connectés à venir. L'Europe est en panne d'investissements et de planification collective des infrastructures 5G : à notre connaissance, seuls cinq pays nordiques (Finlande, Suède, Danemark, Norvège et Islande) ont un projet de réseau collectif[36]. À ce stade, de nombreuses sources soulignent que comme pour la 4G, Huawei est bien le fournisseur au coût le plus bas et à la compatibilité rétroactive des équipements la plus poussée (avec Nokia sur ce dernier point). L'entreprise a eu de plus l'habileté de promettre nombre de centres de recherche et de coopérations universitaires dans l'ensemble de l'Europe, un saupoudrage politique qui est aussi un outil de recrutement de main d'œuvre qualifiée. Le principe de précaution, qu'il porte sur la sécurité à terme ou sur l'indépendance industrielle, a été une considération secondaire ou inexistante pour la plupart des États et des opérateurs.

Notre carte interactive du déploiement de la 5G et de la pénétration de Huawei en Europe révèle cette fragmentation[37]. La carte permet l'accès à des fiches détaillées pour trente pays européens (les 28 membres de l'Union européenne, la Norvège et la Suisse), qui chacune contient des données sur l'état du déploiement de la 5G et sur la présence de Huawei dans l'infrastructure télécom du pays, à partir de critères listés dans une fiche méthodologique. Huawei a déjà signé des partenariats avec 14 opérateurs européens pour la construction de l'infrastructure 5G. L'entreprise a annoncé 23 contrats commerciaux en Europe, qui incluent ces partenariats avec des opérateurs, même si tous les contrats ne sont pas encore effectifs[38]. Or, dans de nombreux pays, les enchères d'attribution des fréquences de la 5G ne sont pas encore lancées au printemps 2019. Huawei est d'ores et déjà très présent dans des projets pilotes 5G dans toute l'Europe, le plus souvent à l'échelle de villes, et parfois dans des quartiers centraux comme Mitte à Berlin et Westminster à Londres. Dans plusieurs pays, on note une forte présence de Huawei dans les réseaux radio 4G, comme accompagnateur des opérateurs dans la construction d'une infrastructure *cloud*, dans la fibre. La présence de Huawei se caractérise aussi par des investissements dans des centres de sécurité au Royaume-Uni, en Allemagne et à Bruxelles, et par de nombreux partenariats dans l'éducation, la formation et la recherche, *via* des coopérations universitaires ou des programmes spécifiques.

[36] « 5 Nordic Countries aim to be 1st interconnected 5G region in the world », *IEEE Communications Society Technology Blog* (2018), https://techblog.comsoc.org/2018/06/06/5-nordic-countries-agree-to-accelerate-5g/

[37] Lien vers la carte interactive, https://www.institutmontaigne.org/publications/leurope-et-la-5g-le-cas-huawei-partie-2#section4662

[38] « Huawei reveals it has no 5G contracts from mainland China », *Financial Times,* (2019) https://www.ft.com/content/c6f8da24-6023-11e9-a27a-fdd51850994c?shareType=nongift

Il existe aussi une dimension plus difficile à quantifier de la présence Huawei en Europe : la nature du débat public sur la présence de l'entreprise. Dans certains pays, la classe politique s'est saisie de la question des risques sécuritaires alors que dans d'autres, les activités de Huawei ne sont pas du tout politisées. Ainsi, alors que Malte, Monaco et Duisbourg se sont engagées dans la construction de villes intelligentes avec Huawei et qu'une partie importante de la classe politique italienne apporte un soutien appuyé à l'équipementier chinois, la discussion a dans d'autres pays pris une orientation plus sécuritaire. Dans ces débats, l'entreprise Huawei est tout sauf passive, même si sa campagne de relations publiques diffère de pays à pays de par son intensité.

Ces critères permettent une vision macro de la présence diversifiée de Huawei en Europe, à l'heure des choix pour la 5G. Tous facteurs pris en compte, l'Italie, la Pologne, l'Espagne, la Lettonie, les Pays-Bas, le Portugal et Malte se distinguent par une forte présence de l'équipementier chinois. À l'autre extrême du spectre, la Slovénie, l'Estonie, le Danemark et la Norvège sont des terrains plus difficiles pour Huawei, alors que la Croatie et Chypre accusent un retard général dans la construction de leurs réseaux télécom.

Les arbitrages sur la 5G ne peuvent pas se résumer à un choix rationnel de rapport qualité/prix pour les consommateurs. Dans ces conditions, la fragmentation et la quasi-cacophonie de l'Europe vis-à-vis de Huawei rend bien plus difficile une approche cohérente à l'échelle du continent qui prend en compte non seulement les risques sécuritaires, mais aussi les enjeux géopolitiques et les rapports de puissance, pour lesquels le niveau technologique et économique est bien sûr structurant. Le principe de précaution est loin d'être appliqué partout. Les Etats européens divergent dans leurs normes et leurs standards de sécurité pour les équipements télécom – il s'agit là du deuxième grand domaine de fragmentation de l'Europe.

La Commission Européenne s'est saisie de cet enjeu critique de convergence des normes en Europe. Sa recommandation de mars 2019 décrit la sécurité de la 5G comme un enjeu « d'autonomie stratégique » pour l'UE[39]. Elle pousse la convergence de l'évaluation des risques de pays à pays, en imposant un calendrier à ceux qui n'en avaient pas pour la conduite d'une revue nationale des vulnérabilités liées à la 5G (remise des textes le 15 juillet 2019 à la Commission et à l'agence européenne de cybersécurité). Elle souligne les instruments de l'UE pour contribuer

[39] « European Commission recommends common EU approach to the security of 5G networks », *European Commission – Press Communiqué* (2019), http://europa.eu/rapid/press-release_IP-19-1832_en.htm

à la régulation de la 5G en Europe : le règlement général sur la protection des données qui définit des obligations sur l'utilisation des données personnelles, l'outil de supervision des investissements étrangers qui créent des dispositions sur la protection de l'infrastructure au sein de l'Union. La communication met en avant le rôle central de l'agence européenne de cybersécurité ENISA, et sa mise en place d'un système de certification des équipements à l'échelle du continent, qui se nourrit de pratiques nationales diverses et en pleine recomposition. Elle poursuit ainsi l'initiative entamée par l'Acte Européen de Cybersécurité de 2018, qui avait déjà créé un cadre de certification UE en matière de cybersécurité[40].

Comme dans d'autres domaines sensibles tels que l'investissement étranger ou les contrôles des exportations, l'UE est contrainte d'harmoniser des pratiques très diverses, de compiler les informations provenant des États-membres, d'identifier et de promouvoir les pratiques les plus efficaces. La Commission impose comme date butoir le 31 décembre 2019 pour établir une liste des risques sécuritaires et des possibles mesures de mitigation.

Le 15 mai 2019, Donald Trump a annoncé l'exclusion de Huawei des fournisseurs autorisés aux États-Unis, en invoquant l'*International Emergency Economic Powers Act*. Cette décision a été aussitôt suivie par le *Department of Commerce* d'un placement de l'entreprise sur la liste des entreprises *(entity list)* avec qui les entreprises américaines ne peuvent commercer sans une autorisation spéciale qu'il est quasiment impossible d'obtenir en pratique. C'est un acte décisif : très au-delà de la sécurité des réseaux, elle atteint l'ensemble des trois principaux secteurs d'activité de Huawei : équipements réseaux, smartphones et services aux entreprises. La décision place aussi les partenaires étrangers de Huawei devant un dilemme : suivre la décision américaine, ou au contraire dans certain cas bénéficier de l'effet d'aubaine tant qu'un régime de sanctions secondaires n'est pas en place. Le marché des télécommunications des États-Unis est un immense levier pour forcer les fournisseurs alternatifs, qui se trouvent à Taiwan, en Corée du Sud au Japon et parfois en Europe, à suivre la ligne américaine. Ils sont en effet étroitement imbriqués dans l'économie américaine des technologies de communication. Sur ce point, il est révélateur que le fournisseur allemand de semiconducteurs Infineon ait suspendu immédiatement après l'annonce américaine des livraisons à Huawei Technologies de produits qui incluaient des composants américains[41].

[40] « Acte législatif sur la cybersécurité », *Commission européenne - Actualités* (2018), https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_fr

[41] Cheng Ting-Fang and Lauly Li, « Germany's Infineon suspends US shipments to Huawei », *Nikkei Asian Review* (2019), https://asia.nikkei.com/Economy/Trade-war/Germany-s-Infineon-suspends-US-shipments-to-Huawei

Il est clair que la décision est désormais politique, et dépasse à la fois un enjeu de sécurité déjà très complexe, et aussi la question de la compétitivité des équipements Huawei dans la 5G. Mais parce qu'elle accapare le champ politique et médiatique, la controverse ferait presque oublier qu'il existe des solutions européennes à la construction de l'infrastructure 5G. Or Ericsson et Nokia détiennent respectivement 27 % et 22 % du marché mondial des équipements 2G/3G/4G, contre 31 % pour Huawei, aidés il est vrai par la fermeture du marché des États-Unis à Huawei[42]. En 2018, Ericsson a même dépassé Huawei selon IHS Markit, atteignant 29 % de parts de marchés mondiales contre 26 % pour Huawei[43]. Les deux entreprises nordiques sont très bien positionnées sur la 5G. Toutefois, elles ne pourraient, pas plus que Huawei, se passer de l'apport de certains fabricants américains de composants.

Par contraste avec Huawei, un concurrent européen comme Ericsson investit beaucoup moins sur les relations publiques. Il construit déjà, dans une relative indifférence médiatique, des réseaux 5G pour des opérateurs aux États-Unis, en Corée du Sud, en Arabie Saoudite, en Australie – en avril 2019, 18 contrats publics avaient été signés[44]. Les premiers déploiements commerciaux de la 5G en Corée du Sud et avec Verizon aux États-Unis fonctionnent avec de la technologie Ericsson. En Chine, l'équipementier scandinave est présent dans de nombreux projets avec les opérateurs chinois, du port de Qingdao à des tests sur l'internet des objets (IoT). De même en mars 2019, Nokia a annoncé la signature d'un 30e contrat commercial de déploiement de la 5G, avec un opérateur autrichien[45]. L'équipementier finlandais est actif en Arabie Saoudite, en Afrique du Sud, aux États-Unis, en Egypte, au Japon, en Australie, en Norvège, en Finlande, en Corée du Sud et en Allemagne. Comme Ericsson, Nokia a une présence dans la 5G en Chine, en particulier dans la recherche et le développement, *via* des contrats avec China Mobile ou Tencent[46].

[42] « IHS Markit: Huawei Led Global 4G LTE Infrastructure Market which totalled $22.9B in 2018; China CAPEX bottoms out », *IEEE Communications Society Technology Blog* (2019), https://techblog.comsoc.org/2019/04/03/huawei-led-global-4g-lte-infrastructure-market-which-totalled-22-9b-in-2018/

[43] Shunsuke Tabeta and Takashi Kawakami, « US fight dethrones Huawei as top mobile equipment provider », *Nikkei Asian Review* (2019), https://asia.nikkei.com/Business/Business-trends/US-fight-dethrones-Huawei-as-top-mobile-equipment-provider

[44] « Live 5G networks and publicly announced 5G contracts », *Ericsson,* https://www.ericsson.com/en/5g/5g-networks/5g-contracts

[45] « Nokia celebrates 30th commercial 5G deal », *Nokia* (2019), https://www.nokia.com/about-us/news/releases/2019/03/28/nokia-celebrates-30th-commercial-5g-deal/

[46] « Nokia and China Mobile to set up joint AI*5G lab for further research using artificial intelligence and machine learning in 5G networks », *Nokia* (2018), https://www.nokia.com/about-us/news/releases/2018/07/06/nokia-and-china-mobile-to-set-up-joint-ai5g-lab-for-further-research-using-artificial-intelligence-and-machine-learning-in-5g-networks/ « Nokia and Tencent sign agreement to accelerate 5G webscale research and applications to benefit millions of Internet users in China », *Nokia* (2018), https://www.nokia.com/about-us/news/releases/2018/07/05/nokia-and-tencent-sign-agreement-to-accelerate-5g-webscale-research-and-applications-to-benefit-millions-of-internet-users-in-china/

IV

CONCLUSION ET RECOMMANDATIONS : LA 5G, UNE INFRASTRUCTURE CRITIQUE EUROPÉENNE

En l'absence de marché unique des fréquences de télécommunications au sein de l'UE et malgré les efforts de la Commission pour promouvoir la convergence des normes sécuritaires, les pays européens avancent en ordre dispersé. Cela crée pour l'Europe un risque de décrochage, voire de déclassement stratégique. La certification des équipements à l'échelle européenne est un progrès louable mais insuffisant. L'Europe peut-elle développer une approche moins défensive et plus proactive, et donc plus ambitieuse ? La saturation de l'espace médiatique par la controverse Huawei risque de détourner l'Europe d'un enjeu essentiel pour sa place dans un ordre international en mutation. La construction de l'infrastructure 5G offre en effet à l'Europe une occasion de consolider une offre technologique et industrielle et de constituer ainsi un des outils pour une souveraineté européenne.

Considérer la 5G comme une infrastructure critique au service de la souveraineté européenne

L'avènement de la 5G multiplie les risques inhérents à l'absence de souveraineté européenne. La protection des données européennes et donc la promotion d'une autonomie de décision politique et la construction d'un environnement minimisant les risques pour les entreprises demande des choix allant bien au-delà du calcul des coûts pour les opérateurs et de l'intérêt immédiat des consommateurs. Le premier de ces choix est de réduire ou d'équilibrer la dépendance à l'égard des fournisseurs extérieurs. Ce d'autant qu'à la traditionnelle influence des États-Unis à travers leurs fournisseurs s'ajoute aujourd'hui le risque d'un duopole sino-américain ou même la suprématie de la Chine sur le secteur des télécommunications. Il est important aussi de réaliser que si l'interopérabilité entre fournisseurs existe (à un coût), la division de l'infrastructure 5G européenne entre zones équipées par Huawei et zones équipées par d'autres constructeurs nuit à la cohérence stratégique de l'Europe entre la Chine et les États-Unis.

Agir en fonction du principe de précaution

L'impossibilité de Huawei de démontrer l'absence de liens étroits et ineffaçables avec le parti-Etat chinois rendent nécessaire d'écarter cette entreprise des infrastructures à risque. Tout le problème reste bien sûr de déterminer l'étendue des restrictions sécuritaires. L'entreprise reste dans certains cas un aiguillon concurrentiel utile et la sécurisation des réseaux contre le risque de sabotage implique dans tous les cas de ne pas reposer sur un fournisseur unique. Si l'Europe n'est pas capable de soutenir ses entreprises qui détiennent encore une part importante du marché mondial, elle doit faire un choix par défaut en les complétant avec d'autres entreprises non européennes. Toutes poseront des questions de sécurité, mais sans doute aucune de façon aussi incontrôlable que Huawei.

Approfondir les efforts défensifs

Toutes les failles de l'architecture 5G sont susceptibles d'être exploitées par des acteurs malveillants. Il n'y a pas de ligne Maginot dans la protection des réseaux interconnectés. La formation de personnel qualifié est un investissement critique. Le renforcement des ressources humaines dans les états membres les moins bien dotés est également important. La promotion de pratiques communes par l'Union Européenne doit être soutenue par les États membres les plus avancés dans leur processus de certification des équipements 5G. La mutualisation de la R&D en matière de sécurité des réseaux doit aller plus loin car les données à protéger ne seront pas concentrées dans quelques points très précis du territoire européen. L'approche européenne centrée sur la réglementation administrative et la certification des équipements doit faire l'objet d'un échange de meilleures pratiques avec l'allié américain. L'Europe doit aussi conclure sur sa capacité à traiter le risque lié aux équipements 5G par des mesures administratives. Il est clair qu'il n'y a pas de réponse technique aujourd'hui qui soit valide avec certitude dans cinq ans tant l'équilibre entre les mesures offensives et défensives est instable.

Soutenir un écosystème favorable à la compétitivité technologique en Europe

Dans le cas de la 5G, les champions européens existent déjà. La compétition prix de Huawei bénéfique à court terme au consommateur européen et aux finances

publiques qui recueillent le produit des mises aux enchères de fréquences, les handicape toutefois. Sans Huawei, une concertation européenne est nécessaire pour construire un marché à l'échelle suffisante pour rentabiliser les investissements nécessaires. On ne peut éluder non plus la question du marché américain, et donc de la coopération avec les fabricants américains – Qualcomm, Broadcomm, Nvidia pour ne citer qu'eux. D'autres aspects peuvent favoriser la construction d'un écosystème européen : les aspects de norme et de régulation des équipements ; le soutien à la recherche et au développement ; le soutien à l'émergence de champions européens dans le *cloud* ; la protection des équipementiers contre le risque d'acquisition diminuant l'autonomie industrielle européenne, ou au contraire la conclusion de nouvelles alliances industrielles transatlantiques. Cette protection ne se conçoit pas sans un investissement robuste dans les infrastructures permettant aux entreprises européennes de s'étendre.

À PROPOS DES AUTEURS

Mathieu Duchâtel, directeur du programme Asie, Institut Montaigne

Docteur en science politique de SciencesPo, Mathieu Duchâtel a été *Senior Policy Fellow* et *Deputy Director* du programme Asie de l'ECFR. De 2011 à 2015, il a également été Senior Researcher et représentant à Pékin du *Stockholm International Peace Research Institute* (SIPRI). Il a vécu neuf ans entre Shanghai (Université de Fudan), Taipei (Université Nationale de Chengchi) et Pékin. De 2006 à 2011, il est *Research fellow* à l'Asia Centre. Il a également été *Visiting Scholar* à la School of International Studies de l'Université de Pékin en 2011 et 2012, puis au Japan Institute of International Affairs en 2015.

François Godement, conseiller pour l'Asie, Institut Montaigne

François Godement est Conseiller pour l'Asie à l'Institut Montaigne. Il est également Senior non *resident fellow* du *Carnegie Endowment for International Peace,* et consultant externe au ministère de l'Europe et des Affaires étrangères français. François Godement était précédemment directeur du programme Asie de l'ECFR, professeur des universités à l'INALCO (Institut national des langues et civilisations orientales) puis à SciencesPo Paris. Il a fondé le Centre Asie de l'IFRI, le CSCAP Europe *(Council for Security Cooperation in the Asia-Pacific)* , et le *think tank* Asia Centre. Son dernier ouvrage publié est : *La Chine à nos portes – une stratégie pour l'Europe* (avec Abigael Vasselier), Odile Jacob, 2018.

Remerciements

Ce travail a bénéficié d'entretiens individuels conduits par les auteurs entre janvier et avril 2019 auprès de responsables du secteur privé et de l'administration, en France et en Europe. L'Institut Montaigne remercie les personnes qui ont contribué à ce travail pour le temps qu'elles y ont consacré.

LES PUBLICATIONS DE L'INSTITUT MONTAIGNE

- L'Europe et la 5G : passons la cinquième ! (partie 1) (mai 2019)
- Media polarization « à la française »? comparing the French and American ecosystems (mai 2019)
- Travailleurs des plateformes : liberté oui, protection aussi (mai 2019)
- Energie solaire en Afrique : un avenir rayonnant ? (février 2019)
- IA et emploi en santé : quoi de neuf docteur ? (janvier 2019)
- Cybermenace : avis de tempête (novembre 2018)
- Partenariat franco-britannique de défense et de sécurité : améliorer notre coopération, (novembre 2018)
- Sauver le droit d'asile (octobre 2018)
- Industrie du futur, prêts, partez ! (septembre 2018)
- La fabrique de l'islamisme (septembre 2018)
- Protection sociale : une mise à jour vitale (mars 2018)
- Innovation en santé : soignons nos talents (mars 2018)
- Travail en prison : préparer (vraiment) l'après (février 2018)
- ETI : taille intermédiaire, gros potentiel (janvier 2018)
- Réforme de la formation professionnelle : allons jusqu'au bout ! (janvier 2018)
- Espace : l'Europe contre-attaque ? (décembre 2017)
- Justice : faites entrer le numérique (novembre 2017)
- Apprentissage : les trois clés d'une véritable transformation (octobre 2017)
- Prêts pour l'Afrique d'aujourd'hui ? (septembre 2017)
- Nouveau monde arabe, nouvelle « politique arabe » pour la France (août 2017)
- Enseignement supérieur et numérique : connectez-vous ! (juin 2017)
- Syrie : en finir avec une guerre sans fin (juin 2017)
- Énergie : priorité au climat ! (juin 2017)
- Quelle place pour la voiture demain ? (mai 2017)
- Sécurité nationale : quels moyens pour quelles priorités ? (avril 2017)
- Tourisme en France : cliquez ici pour rafraîchir (mars 2017)
- L'Europe dont nous avons besoin (mars 2017)
- Dernière chance pour le paritarisme de gestion (mars 2017)
- L'impossible État actionnaire ? (janvier 2017)
- Un capital emploi formation pour tous (janvier 2017)
- Économie circulaire, réconcilier croissance et environnement (novembre 2016)
- Traité transatlantique : pourquoi persévérer (octobre 2016)
- Un islam français est possible (septembre 2016)
- Refonder la sécurité nationale (septembre 2016)
- Bremain ou Brexit : Europe, prépare ton avenir ! (juin 2016)
- Réanimer le système de santé - Propositions pour 2017 (juin 2016)
- Nucléaire : l'heure des choix (juin 2016)
- Un autre droit du travail est possible (mai 2016)

- Les primaires pour les Nuls (avril 2016)
- Le numérique pour réussir dès l'école primaire (mars 2016)
- Retraites : pour une réforme durable (février 2016)
- Décentralisation : sortons de la confusion / Repenser l'action publique dans les territoires (janvier 2016)
- Terreur dans l'Hexagone (décembre 2015)
- Climat et entreprises : de la mobilisation à l'action / Sept propositions pour préparer l'après-COP21 (novembre 2015)
- Discriminations religieuses à l'embauche : une réalité (octobre 2015)
- Pour en finir avec le chômage (septembre 2015)
- Sauver le dialogue social (septembre 2015)
- Politique du logement : faire sauter les verrous (juillet 2015)
- Faire du bien vieillir un projet de société (juin 2015)
- Dépense publique : le temps de l'action (mai 2015)
- Apprentissage : un vaccin contre le chômage des jeunes (mai 2015)
- Big Data et objets connectés. Faire de la France un champion de la révolution numérique (avril 2015)
- Université : pour une nouvelle ambition (avril 2015)
- Rallumer la télévision : 10 propositions pour faire rayonner l'audiovisuel français (février 2015)
- Marché du travail : la grande fracture (février 2015)
- Concilier efficacité économique et démocratie : l'exemple mutualiste (décembre 2014)
- Résidences Seniors : une alternative à développer (décembre 2014)
- Business schools : rester des champions dans la compétition internationale (novembre 2014)
- Prévention des maladies psychiatriques : pour en finir avec le retard français (octobre 2014)
- Temps de travail : mettre fin aux blocages (octobre 2014)
- Réforme de la formation professionnelle : entre avancées, occasions manquées et pari financier (septembre 2014)
- Dix ans de politiques de diversité : quel bilan ? (septembre 2014)
- Et la confiance, bordel ? (août 2014)
- Gaz de schiste : comment avancer (juillet 2014)
- Pour une véritable politique publique du renseignement (juillet 2014)
- Rester le leader mondial du tourisme, un enjeu vital pour la France (juin 2014)
- 1 151 milliards d'euros de dépenses publiques : quels résultats ? (février 2014)
- Comment renforcer l'Europe politique (janvier 2014)
- Améliorer l'équité et l'efficacité de l'assurance-chômage (décembre 2013)

- Santé : faire le pari de l'innovation (décembre 2013)
- Afrique-France : mettre en œuvre le co-développement
  Contribution au XXVI[e] sommet Afrique-France (décembre 2013)
- Chômage : inverser la courbe (octobre 2013)
- Mettre la fiscalité au service de la croissance (septembre 2013)
- Vive le long terme ! Les entreprises familiales au service de la croissance et de l'emploi (septembre 2013)
- Habitat : pour une transition énergétique ambitieuse (septembre 2013)
- Commerce extérieur : refuser le déclin
  Propositions pour renforcer notre présence dans les échanges internationaux (juillet 2013)
- Pour des logements sobres en consommation d'énergie (juillet 2013)
- 10 propositions pour refonder le patronat (juin 2013)
- Accès aux soins : en finir avec la fracture territoriale (mai 2013)
- Nouvelle réglementation européenne des agences de notation : quels bénéfices attendre ? (avril 2013)
- Remettre la formation professionnelle au service de l'emploi et de la compétitivité (mars 2013)
- Faire vivre la promesse laïque (mars 2013)
- Pour un « New Deal » numérique (février 2013)
- Intérêt général : que peut l'entreprise ? (janvier 2013)
- Redonner sens et efficacité à la dépense publique
  15 propositions pour 60 milliards d'économies (décembre 2012)
- Les juges et l'économie : une défiance française ? (décembre 2012)
- Restaurer la compétitivité de l'économie française (novembre 2012)
- Faire de la transition énergétique un levier de compétitivité (novembre 2012)
- Réformer la mise en examen Un impératif pour renforcer l'État de droit (novembre 2012)
- Transport de voyageurs : comment réformer un modèle à bout de souffle ? (novembre 2012)
- Comment concilier régulation financière et croissance :
  20 propositions (novembre 2012)
- Taxe professionnelle et finances locales : premier pas vers une réforme globale ? (septembre 2012)
- Remettre la notation financière à sa juste place (juillet 2012)
- Réformer par temps de crise (mai 2012)
- Insatisfaction au travail : sortir de l'exception française (avril 2012)
- Vademecum 2007 – 2012 : Objectif Croissance (mars 2012)
- Financement des entreprises : propositions pour la présidentielle (mars 2012)
- Une fiscalité au service de la « social compétitivité » (mars 2012)
- La France au miroir de l'Italie (février 2012)
- Pour des réseaux électriques intelligents (février 2012)

- Un CDI pour tous (novembre 2011)
- Repenser la politique familiale (octobre 2011)
- Formation professionnelle : pour en finir avec les réformes inabouties (octobre 2011)
- Banlieue de la République (septembre 2011)
- De la naissance à la croissance : comment développer nos PME (juin 2011)
- Reconstruire le dialogue social (juin 2011)
- Adapter la formation des ingénieurs à la mondialisation (février 2011)
- « Vous avez le droit de garder le silence… » Comment réformer la garde à vue (décembre 2010)
- Gone for Good? Partis pour de bon ? Les expatriés de l'enseignement supérieur français aux États-Unis (novembre 2010)
- 15 propositions pour l'emploi des jeunes et des seniors (septembre 2010)
- Afrique - France. Réinventer le co-développement (juin 2010)
- Vaincre l'échec à l'école primaire (avril 2010)
- Pour un Eurobond. Une stratégie coordonnée pour sortir de la crise (février 2010)
- Réforme des retraites : vers un big-bang ? (mai 2009)
- Mesurer la qualité des soins (février 2009)
- Ouvrir la politique à la diversité (janvier 2009)
- Engager le citoyen dans la vie associative (novembre 2008)
- Comment rendre la prison (enfin) utile (septembre 2008)
- Infrastructures de transport : lesquelles bâtir, comment les choisir ? (juillet 2008)
- HLM, parc privé Deux pistes pour que tous aient un toit (juin 2008)
- Comment communiquer la réforme (mai 2008)
- Après le Japon, la France… Faire du vieillissement un moteur de croissance (décembre 2007)
- Au nom de l'Islam… Quel dialogue avec les minorités musulmanes en Europe ? (septembre 2007)
- L'exemple inattendu des Vets Comment ressusciter un système public de santé (juin 2007)
- Vademecum 2007-2012 Moderniser la France (mai 2007)
- Après Erasmus, Amicus Pour un service civique universel européen (avril 2007)

- Quelle politique de l'énergie pour l'Union européenne ? (mars 2007)
- Sortir de l'immobilité sociale à la française (novembre 2006)
- Avoir des leaders dans la compétition universitaire mondiale (octobre 2006)
- Comment sauver la presse quotidienne d'information (août 2006)
- Pourquoi nos PME ne grandissent pas (juillet 2006)
- Mondialisation : réconcilier la France avec la compétitivité (juin 2006)
- TVA, CSG, IR, cotisations…
  Comment financer la protection sociale (mai 2006)
- Pauvreté, exclusion : ce que peut faire l'entreprise (février 2006)
- Ouvrir les grandes écoles à la diversité (janvier 2006)
- Immobilier de l'État : quoi vendre, pourquoi, comment
  (décembre 2005)
- 15 pistes (parmi d'autres…) pour moderniser la sphère publique
  (novembre 2005)
- Ambition pour l'agriculture, libertés pour les agriculteurs (juillet 2005)
- Hôpital : le modèle invisible (juin 2005)
- Un Contrôleur général pour les Finances publiques (février 2005)
- Les oubliés de l'égalité des chances (janvier 2004 - Réédition septembre 2005)

Pour les publications antérieures se référer à notre site internet :
www.institutmontaigne.org

INSTITUT
MONTAIGNE

ABB FRANCE
ACCURACY
ADIT
AIR FRANCE - KLM
AIRBUS GROUP
ALLEN & OVERY
ALLIANZ
ALVAREZ & MARSAL FRANCE
ARCHERY STRATEGY CONSULTING
ARCHIMED
ARDIAN
ASTRAZENECA
A.T. KEARNEY
AUGUST DEBOUZY
AXA
BAKER & MCKENZIE
BANK OF AMERICA MERRILL LYNCH
BEARINGPOINT
BESSÉ
BNI FRANCE ET BELGIQUE
BNP PARIBAS
BOLLORÉ
BOUYGUES
BPCE
BRUNSWICK
CAISSE DES DÉPÔTS
CAPGEMINI
CAPITAL GROUP
CARBONNIER LAMAZE RASLE & ASSOCIÉS
CAREIT
CARREFOUR
CASINO
CHAÎNE THERMALE DU SOLEIL
CHUBB
CIS
CISCO SYSTEMS FRANCE
CMA CGM
CNP ASSURANCES
COHEN AMIR-ASLANI
COMPAGNIE PLASTIC OMNIUM
CONSEIL SUPÉRIEUR DU NOTARIAT
CORREZE & ZAMBEZE
CRÉDIT AGRICOLE
CRÉDIT FONCIER DE FRANCE
D'ANGELIN & CO. LTD
DENTSU AEGIS NETWORK
DE PARDIEU BROCAS MAFFEI
DRIVE INNOVATION INSIGHTS - DII
EDF
ELSAN
ENGIE
EQUANCY
EURAZEO
EUROGROUP CONSULTING
EUROSTAR
FIVES
FONCIÈRE INEA
FONDATION ROCHE
GALILEO GLOBAL EDUCATION FRANCE
GIDE LOYRETTE NOUEL
GOOGLE
GRAS SAVOYE
GROUPAMA
GROUPE EDMOND DE ROTHSCHILD
GROUPE M6
GROUPE ORANGE
HAMEUR ET CIE
HENNER
HSBC FRANCE
IBM FRANCE
IFPASS
ING BANK FRANCE
INSEEC
INTERNATIONAL SOS
IONIS EDUCATION GROUP
ISRP
JEANTET ASSOCIÉS
KANTAR
KPMG S.A.
LA BANQUE POSTALE
LA PARISIENNE ASSURANCES
LAZARD FRÈRES
LINEDATA SERVICES
LIR
LIVANOVA

SOUTIENNENT L'INSTITUT MONTAIGNE

INSTITUT
MONTAIGNE

LVMH - MOËT-HENNESSY - LOUIS VUITTON
MACSF
MALAKOFF MÉDÉRIC
MAREMMA
MAZARS
MCKINSEY & COMPANY FRANCE
MÉDIA-PARTICIPATIONS
MEDIOBANCA
MERCER
MERIDIAM
MICHELIN
MICROSOFT FRANCE
MITSUBISHI FRANCE
NEHS
NATIXIS
NESTLÉ
OBEA
ODDO BHF
ONDRA PARTNERS
OPTIGESTION
ORANO
ORTEC GROUP
PAI PARTNERS
PIERRE ET VACANCES
PRICEWATERHOUSECOOPERS
PRUDENTIA CAPITAL
RADIALL
RAISE
RAMSAY GÉNÉRALE DE SANTÉ
RANDSTAD
RATP
RELX GROUP
RENAULT
REXEL
RICOL, LASTEYRIE CORPORATE FINANCE
RIVOLIER
ROCHE
ROLAND BERGER
ROTHSCHILD MARTIN MAREUL
SAFRAN
SANTÉCLAIR
SCHNEIDER ELECTRIC
SERVIER
SGS
SIA PARTNERS
SIACI SAINT HONORÉ
SIEMENS
SIER CONSTRUCTEUR
SNCF
SNCF RÉSEAU
SODEXO
SOFINORD-ARMONIA
SOLVAY
SPRINKLR
SUEZ
SYSTEMIS
TECNET PARTICIPATIONS SARL
TEREGA
THE BOSTON CONSULTING GROUP
TILDER
TOTAL
UBS FRANCE
VEOLIA
VINCI
VIVENDI
VOYAGEURS DU MONDE
WAVESTONE
WENDEL
WILLIS TOWERS WATSON
WORDAPPEAL

SOUTIENNENT L'INSTITUT MONTAIGNE

INSTITUT
MONTAIGNE

INSTITUT
MONTAIGNE

IL N'EST DÉSIR PLUS NATUREL QUE LE DÉSIR DE CONNAISSANCE

L'Europe et la 5G : le cas Huawei

Quels choix pour l'infrastructure 5G en Europe ? Le cas Huawei a pris une dimension polémique qui révèle des enjeux stratégiques cruciaux pour l'Europe entre la Chine et les Etats-Unis. La 5G est une infrastructure critique qui transformera l'activité économique, engendrant un saut générationnel pour certaines entreprises, pénalisant les acteurs restant en dehors de son déploiement, et soulevant de nouveaux défis en matière de protection des données et de sécurité nationale.

Or l'Europe avance en ordre dispersé et la saturation de l'espace médiatique par la controverse Huawei la détourne d'un enjeu essentiel pour sa place dans un ordre international en mutation. D'une part, il est nécessaire d'agir en fonction du principe de précaution face à Huawei, une entreprise dans l'impossibilité de démontrer l'absence de liens étroits et ineffaçables avec le cœur de l'appareil d'Etat chinois. D'autre part, la construction des réseaux 5G est une opportunité pour consolider une offre technologique et industrielle en Europe et construire un outil pour une souveraineté européenne.

Cette note du programme Asie de l'Institut Montaigne analyse les risques liés à l'offre Huawei pour l'Europe et souligne l'importance de soutenir un écosystème favorable à la compétitivité technologique en Europe.

Institut Montaigne
59, rue La Boétie - 75008 Paris
Tél. +33 (0)1 53 89 05 60
www.institutmontaigne.org

ISSN 1771-6756
Mai 2019