Université Paris 1

Institut national du service public

Master Science politique

Spécialité Affaires publiques

Parcours Affaires publiques européennes - Action publique en Europe

TITRE : ACTION PUBLIQUE DE L'UNION EUROPÉENNE POUR LA SÉCURITÉ NUMÉRIQUE - LE CAS DE L'ENTREPRISE CHINOISE HUAWEI

Sous la direction de

Dr. Jérôme VALLUY

Maître de conférences de Science politique

Université Paris 1 Panthéon-Sorbonne

soutenu par

UEDA Yuki

CIL Promotion Germaine Tillion (2021-2022)

À ma mère défunte

REMERCIEMENT

Je voudrais exprimer ma gratitude à mon directeur de mémoire, Dr. Jérôme VALLUY, Maître de conférences de science politique, Université Paris 1 Panthéon-Sorbonne, qui m'a donné beaucoup de conseils éclairants et inspirant. Ses perspectives académiques extraordinaires sur la science politique et les enjeux numériques m'ont permis de réaliser ce mémoire. Grâce aux échanges réguliers, j'ai pu non seulement réfléchir à la problématique mais aussi découvrir de nouveaux horizons scientifiques.

Je voudrais également remercier à M. Didier GEORGAKAKIS, Professeurs des universités de science politique, Université Paris 1 Panthéon-Sorbonne, et M. Fabrice LARAT, Chef du département de développement, des enseignements et de la recherche, Institut national du service public (INSP) pour l'organisation du parcours « Master Affaires publiques européennes - Action publique en Europe » de l'Université Paris 1 Panthéon-Sorbonne et de l'INSP.

Je remercie à tous les intervenants de ce parcours de master. Leurs cours divers et approfondis m'ont permis non seulement d'apprendre les principes importants de la science politique mais aussi de mieux connaître les actions publiques en Europe.

Avant de finir mon expression de gratitude, j'exprime mes gratitudes à tous les agents de l'Université Paris 1 et de l'INSP, en particulier, Mme Sandrine BLAISON, Responsable du pôle formations diplômantes, INSP, dont les engagements distingués étaient indispensables pour le parcours.

SOMMAIRE

LISTE DE L'ABREVIATION

AGI	Accord global d'investissements entre l'Union européenne et la Chine
APD	Aide publique au développement
APL	Armée Populaire de libération
BT	British Telecom
CCT	Conseil du Commerce et de la Technologie entre l'Union europé enne et les États-Unis
CE	Commission européenne
CEDEAO	Communauté économique des États de l'Afrique de l'Ouest
CEXIM	Export-Import Bank of China
CFIUS	Committee on Foreign Investment in the United States
EMOA	Europe, Moyen-Orient et Afrique
ESOP	Employee Stock Ownership Program
EU	European Union
FT	Financial Times
GSM	Global System for Mobile Communications
HRAEPS	Haut représentant de l'Union européenne pour les affaires étrangères et la politique de sécurité
NDAA	National Defense Authorization Act
ONU	Organisation des Nations unis
TIC	Technologies de l'information et de la communication
TUE	Traité de l'Union européenne
UA	Union africaine
UE	Union européenne
UpM	Union pour la Méditerranée
WSJ	The Wall Street Journal

INTRODUCTION

Le 19 janvier 2020, la Commission européenne a publié un document intitulé « *Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures* »[1] qui avait pour objectif d'inviter les États membres à prendre des actions pour sécuriser leurs réseaux 5G. Ce document présente les cadres et mesures actuels de l'Union européenne, tels que la Directive (UE) 2016/1148 relatif aux mesures destinées à assurer un haut niveau, commun, de sécurité des réseaux et des systèmes d'information dans l'Union[2] et le Règlement (UE) 2019/452 établissant un cadre pour le filtrage des investissements directs étrangers dans l'Union[3], tout en montrant comment planifier des mesures réduisant les risques au sein des réseaux de télécommunications. Il n'y a pas dans ce document d'expression qui mette en cause des pays ou des entreprises spécifiques en tant que menaces contre les réseaux dans l'Union mais ce dossier mentionne le règlement de l'UE pour le filtrage des investissements directs étrangers, qui traduisait déjà l'attention portée spécifiquement aux pays et entreprises hors de l'Union.

Il faut également évoquer le contexte de publication de ce document par la Commission : celui d'un marché mondial des Technologies de l'information et de la communication (TIC) perturbé par des soupçons récurrents à l'égard d'entreprises chinoises de TIC, notamment la holding Huawei, très fortement articulée politiquement à l'État chinois et massivement implantée à l'étranger (environ 67,8% du chiffre d'affaires réalisé hors de la Chine en 2011[4]). Même si « *EU Toolbox of risk mitigating*

[1] European Commission, 2020
[2] Union européenne, 2016
[3] *Ibid.*, 2019
[4] Huawei Investment & Holding Co., Ltd., 2012

measures » ne mentionne pas cette entreprise ni ce pays, il est très probable que cette action publique de l'Union pour protéger ses réseaux de télécommunication contre les capitaux étrangers, concerne Huawei.

Problématique

Aujourd'hui les TIC sont indispensables non seulement aux individus mais aussi aux organisations du secteur privé et du secteur public dans le monde. Beaucoup de consommateurs ne peuvent probablement plus imaginer la vie sans e-commerce sur Amazon. Depuis la crise sanitaire, le recours au télétravail c'est généralisé dans les entreprises et les services publics, plus rapidement que durant les années précédentes. Les États s'engagent également dans la dématérialisation de nombreux aspects d'administration publique. Cinq des quatorze pays au sommet du classement de l'« *Enquête e-gouvernement de l'ONU 2020* »[5] sont des États membres de l'Union[6]. Les modes de vie se transforment, les nouvelles technologies entraînent de nombreuses mutations sociales, économiques et politiques. Mais dans le même temps, les risques et les menaces augmentent aussi faisant apparaître de nouveaux enjeux politiques, comme celui de la protection de la vie privée, depuis de plusieurs années voire décennies. Plus récemment, l'invasion de l'Ukraine et la nouvelle géopolitique mondiale qui se dessine en relation avec ce conflit accélèrent l'inscription de ces risques et menaces sur l'agenda politique des pays occidentaux dont l'Union européenne. La protection des réseaux de télécommunication et des réseaux informatiques est d'autant plus importante que toute vulnérabilité peut entraîner des fuites de données individuelles et avec elles des informations stratégiques (ce qui fait

[5] Department of Economic and Social Affairs of the United Nations, 2020
[6] Le Danemark est classé le 1er, l'Estonie le 3ème, la Finlande le 4ème, la Suède le 6ème et les Pays-Bas 10ème.

évoluer certaines orientations politiques) ou encore, sous l'effet de cyber-attaques, la paralysie de multiples systèmes de production ou de distribution dépendant de ces réseaux, et éventuellement, l'effondrement de certains systèmes.

Afin de garantir la sécurité du réseau, sa protection nécessite des coopérations internationales intenses, car le numérique, par sa nature connective, dépasse les frontières physiques. Au sein de l'Union européenne, l'Article 24 § 1 du TUE (Traité de l'Union européenne) prévoit que « *La compétence de l'Union en matière de politique étrangère et de sécurité commune couvre tous les domaines de la politique étrangère ainsi que l'ensemble des questions relatives à la sécurité de l'Union* ». Mais, le mandat des politiques étrangères et de sécurité demeure en réalité en chaque État membre : l'Union a besoin d'obtenir un accord des États membres pour réglementer les activités dans le champ numérique. Il subsiste donc sur ce domaine une tension forte entre la volonté d'unification européenne et la persistance des souverainetés nationales ce qui amène à une première esquisse de questionnement : quelles sont les conditions de construction d'une action publique européenne de cybersécurité, dans le contexte précédemment décrit, à l'égard des entreprises et pays étrangers ?

Ce contexte étant relativement récent pour la plupart de ses aspects (concurrences commerciales intercontinentales / internationales, notamment sino-américaines, sur le numérique) et très récents pour certains d'entre eux (reconfiguration des conditions géopolitiques mondiales de cybersécurité), la bibliographie internationale de sciences sociales est souvent trop ancienne pour étudier de tels enjeux d'action publique et nécessite de s'appuyer, davantage que dans d'autres domaines de recherche, sur les investigations journalistiques et la documentation primaire issues des institutions publiques et privées. Quelques recherches de sciences sociales nous ont cependant été très utiles.

Mercedez Fuertes[7] a mis en évidence les nombreux dysfonctionnements de l'Union européenne quand il s'agit de formuler des politiques publiques communes contre les menaces numériques notamment à cause de cette tension entre intégration européenne et souverainetés nationales des États membres. Patrick Meunier[8] étudie la Directive (UE) 2016/1148 et analyse la logique employée par l'Union pour justifier ses compétences en matière numérique conformément au principe de subsidiarité malgré les garanties juridiques des États membres. Mais rien dans la littérature scientifique ne semble indiquer que les dispositifs juridiques de l'Union européenne permettent de faire face aux nouveaux enjeux de sécurité que posent les entreprises chinoises en particulier, très avancées technologiquement, adossées à un État suffisamment centralisé pour concentrer les ressources pluriannuelles de finance publique qui permettent des investissements en infrastructures de télécommunication (câbles sous-marins, satellites…) et en stockage numérique (data centers).

De nombreux articles de presses montrent les difficultés auxquelles l'Union fait face dans ce domaine ainsi que l'intensité des batailles entre Bruxelles et les États membres. Notamment les articles du *Financial Times,* de *Reuters* et d'*Euractive* informent sur cette difficile coopération en traitant, par exemple, des luttes entre le Commissaire européen chargé du commerce, Karel De Gucht, et les États membres en ce qui concerne les relations commerciales sino-européennes au début des années 2010. L'importance des TIC chinoises pour l'Europe est tangible également dans de nombreux autres organes de presse : Stephanie Mehta, dans le journal *Fortune*[9], décrit la relation très étroite c'est-à-dire le haut niveau d'interdépendances entre British

[7] Fuertes, 2021
[8] Meunier, 2017
[9] Mehta, 2013

Telecoms et Huawei ; Oliver Noyan dans *Euractive*[10] souligne la dépendance de certains pays européens à l'égard de Huawei pour le déploiement de leurs réseaux 5G. La presse révèle également le manque de coopération dans l'Union pour traiter le sujet de Huawei et l'intervention forte de Washington en ce sens, dévoilant d'une autre façon les difficultés de l'Union européenne.

Huawei n'est pas la seule holding chinoise concernée. A l'intérieur du marché chinois, Huawei est elle-même en concurrence forte avec sa principale rivale « ZTE » également articulée politiquement au gouvernement chinois. Un partage du marché interne semble se dessiner entre les deux entreprises mais probablement au prix de tensions politico-économiques fortes. Et, à l'international, c'est essentiellement Huawei qui domine l'expansion commerciale et numérique chinoise, comme si un partage implicite cantonnait ZTE au frontières chinoises : ses implantations à l'étranger, par exemple en France en 2019, paraissent discrètes et encore très marginales quant aux activités de l'entreprise. Huawei en revanche déploie massivement son activité à l'étranger.

Ces premiers constats permettent de préciser l'orientation de questionnement pour la présente recherche : De la naissance de Huawei (1987) à aujourd'hui, quels facteurs politiques, au niveau de l'Union, des États-membres et des secteurs privées européens (y compris la diplomatie externe à l'Union), amènent l'Union à développer une action publique visant implicitement les TIC chinoises, notamment en ce qui concerne l'entreprise chinoise « privée-étatique », Huawei, tant sur le territoire de l'Union que dans sa politique vers les pays tiers d'Afrique et d'Amérique latine ?

[10] Noyan, 2021 (a) et (b)

Hypothèse

Ce questionnement focalise l'attention sur les politiques européennes des TIC, en particulier les infrastructures numériques, en particulier parce que ce sont des composants produits par les entreprises chinoises qui posent le plus de problèmes pour la sécurité des réseaux de télécommunication. La spécificité des actions de l'Union européenne contre Huawei est due à des soupçons, en tant qu'entreprise privé-étatique, publiquement révélés par la presse des États américains et britanniques. Huawei, de façon générale, facilite les développements technologiques dans les pays en voie de développement et, en même temps, augmente ainsi les risques graves de fuites des données sensibles via ses produits connectés. En raison des interdépendances fortes entre de nombreux pays africains et les pays riches du bloc anglophone et de l'Union européenne, ceux-ci ne peuvent ignorer les évolutions rapides dans ce domaine sur le continent africain. Dans cette recherche, nous étudierons donc les politiques de l'Union européenne en relation avec les États membres mais aussi en relation avec les pays africains.

L'Union européenne n'a pas encore adopté de mesures d'exclusion équivalentes à celles des pays anglophones (États-Unis depuis 2018, Australie 2018, Royaume-Uni 2020…) à l'encontre de Huawei dans le déploiement du réseau 5G. L'Europe et l'Afrique, au contraire des pays anglophones, conservent des relations étroites avec les entreprises chinoises et en ont besoin pour de multiples aspects de leurs activités économiques. L'Afrique regroupant des pays très pauvres, elle est particulièrement intéressée et exposée aux avancées rapides de Huawei dans le déploiement des infrastructures de télécommunication (Huawei a déjà installé près de 60% des réseaux 3G et 4G… ce qui place l'entreprise en position avantageuse sur le réseau 5G) ainsi que dans sa commercialisation en Afrique de diverses productions connectées peu

chères.

Dans les débats politiques internes à l'Union européenne, comme nous le verrons, ainsi que dans la presse internationale, l'urgence de mesures pour sécuriser les réseaux et les données paraît évidente, tant sur le continent européen que sur le continent africain… mais ces mesures ne sont pas encore apparues. Les mêmes sources incitent à retenir une hypothèse : l'Union européenne n'arriverait pas à initier une politique commune de « cybersécurité », notamment en ce qui concerne les investissements en infrastructures de TIC, en raison de ses divisions politiques internes et de ses dépendances économiques à l'égard de la Chine (de ses producteurs et produits ou services).

Recherche

Cette recherche a été réalisée principalement entre juin et septembre 2022 même si la réflexion et l'étude ont commencé dès mars 2022 par des dialogues successifs avec le directeur de recherche en ce qui concerne la délimitation de l'objet d'étude. La formation initiale en Master à l'Institut National du Service Public (INSP) nécessite beaucoup de temps pour les cours et les travaux personnels entre janvier et juillet. La rédaction du présent mémoire a donc été intensive durant l'été 2022.

Cette recherche peut être qualifiée de principalement « documentaire », le directeur de recherche et l'auteur du présent mémoire, d'un commun accord, ayant écarté de l'agenda méthodologique d'éventuels entretiens semi-directifs… tant que la masse des informations déjà disponibles en ligne n'avait pas encore été traitée ; et même dans cette voie méthodologique, il reste beaucoup à faire…

Les documents utilisés sont d'origines, formats et statuts divers même si les sources ainsi utilisées sont relativement habituelles dans les travaux de sciences sociales : publications scientifiques, articles de presse, publications administratives

des États, des organisations publiques internationales, des entreprises privées… Au regard d'autres domaines de recherche, la littérature scientifique est relativement rare – pour les raisons précédemment indiquées – et elle est rarement aussi accessible en ligne et accès ouvert. La plupart des autres documents utilisés sont accessibles en ligne et présentent un caractère public les rendant ainsi aisément contrôlables.

De nombreuses sources « officielles », émanant des États ou assimilés (Union européenne, États membres de l'UE, État chinois, entreprises publiques-privées…) ont été utilisées en particulier pour préciser les éléments juridiques dans des configurations internationales où le droit est souvent flou par imprécision autant que par diversités des régimes juridiques. La base de données « EU-Lex » a été massivement explorée pour les informations juridiques de l'Union européenne : directives, règlements, communications de la Commission, etc. Les informations juridiques chinoises ont été acquises via la Bibliothèque nationale du Diet au Japon. Des recherches approfondies ont également été réalisée sur le site du Congrès américain notamment sur les actes juridiques américains.

D'une façon générale, nous avons considéré au premier plan les documents officiels publiés par les États puis complété l'information, mais en second plan, par des sources journalistiques sans sous-estimer les risques d'informations approximatives ou fausses dans divers organes privés de presse ni sous-estimer les intéressements politiques dans les publications officielles des institutions étatiques pas plus que les intéressements commerciaux à la diffusion d'informations éventuellement discutables dans les documents émanant des entreprises privées (Rapports annuels d'activités notamment).

Les sources journalistiques, particulièrement nécessaires dans ce domaine, ont été utilisées pour compléter de façon plus détaillée ce qui est évoqué dans les

documents officiels et aussi pour obtenir des renseignements peu ou pas officiels. Diverses précautions de contrôle ont été mises en œuvre – notamment la recherche de plusieurs sources concordantes et indépendantes l'une de l'autre – dans le traitement de médias réputés pour leur indépendance, même si cette qualification peut toujours être discutée : *BBC, Financial Times, Euractive, Le Monde, Les Échos, NHK, Politico, Reuters, Washington Post,* etc.. Enfin, la méthodologie comparative proposée par Daniele CARAMANI[11] a souvent inspirée l'analyse des politiques menées par les différents États membres de l'Union européenne, notamment en ce qui concerne le déploiement du réseau 5G.

Plan

Les premiers constats amenant à la construction de notre objet d'étude justifient une focalisation de type monographique et sociohistorique sur l'entreprise chinoise Huawei depuis sa création entre 1987 jusqu'à ses évolutions les plus récentes, d'autant que celles-ci concernent particulièrement l'Europe et l'Afrique même si les révélations et dénonciations des vols de propriété intellectuelle, les soupçons d'espionnage au service de l'État chinois et les contraintes juridiques que subit l'entreprise de la part de son État d'origine et d'appartenance ont davantage été le fait de discours politiques et médiatiques dans les pays anglophones, États-Unis d'Amérique notamment. (Première partie).

Cette monographie permet de contextualiser, l'émergence lente et oscillante des premières actions publiques de l'Union européenne depuis le début des années 2010 vis-à-vis des entreprises étrangères menaçantes, selon les formulations officielles toujours exprimées en termes généraux, mais visant de plus en plus précisément

[11] Caramani, 2011

l'expansion assez exceptionnelle de Huawei tant sur le continent européen que sur le continent africain. La recherche permet de montrer l'étendue des difficultés politiques intra-européennes pour construire une politique commune et la grande diversité d'intérêts nationaux voire plurinationaux vis-à-vis de Huawei et de la Chine, diversité observable sur les deux continents même si nous n'aborderons la situation africaine qu'à travers le prisme de la politique étrangère de l'Union européenne et des collaborations avec les États-Unis d'Amérique (Deuxième partie).

1 L'ENJEU HUAWEI COMME ELEMENT DU CONTEXTE D'ACTION PUBLIQUE EUROPEENNE

Pour comprendre ce contexte, il faut analyser sa construction sociohistorique en étudiant la nature et la caractéristique de l'enjeu de Huawei. Dans les années 1980s, Huawei n'était qu'une petite entreprise rurale en Chine mais elle est devenue une géante internationale sur le marché mondial des TIC aujourd'hui.

Ce développement spectaculaire n'a pas eu lieu sans soulever des problèmes qui se sont accumulés au cours du temps jusqu'à former un enjeu saillant sur l'agenda politique de nombreux pays, non seulement en ce qui concerne l'état mondial du marché qu'en ce qui concerne les relations internationales entre États.

Pour le montrer, la trajectoire historique de Huawei sera étudiée depuis sa création en Chine en 1987 mais surtout depuis les débuts de son expansion en Europe et en Afrique (1.1). Nous examinerons ensuite le « risque Huawei » en recensant les imputations de pratiques frauduleuses et/ou menaçantes aux USA et en Europe, ces dénonciations entraînant un vaste débat politique toujours en cours aujourd'hui quant au déploiement international de l'équipementier chinois (1.2).

1.1. Genèse de Huawei

Pour comprendre l'enjeu de Huawei, il faut d'abord revenir les conditions de son apparition en Chine parce que cette origine a souvent été critiquée comme opaque, contribuant ainsi à augmenter les soupçons envers l'entreprise. Ce n'est qu'après une première période marquée par son succès sur le marché chinois que Huawei a pu triompher ensuite sur les marchés européens et africains.

1.1.1 Création en Chine

En 1987, Huawei a été créée à Shenzhen, ville au sud de la Chine à côté de Hongkong, par un groupe d'ingénieurs chinois, y compris Ren Zhengfei, présent PDG de Huawei depuis 1988. Son curriculum vitæ n'est pas très clair, en particulier sa carrière dans l'Armée populaire de libération (APL). Selon le site internet de Huawei et quelques articles des presses, né dans un village de la Province de Guizhou, Chine, Ren Zhengfei[12] a étudié l'architecture au sein de l'Institut de l'ingénierie civile et de l'architecture de Chongqing (présente Université de Chongqing) en 1963. En tant qu'ingénieur civil, il a intégré le Corps d'ingénierie civile de l'APL de la Chine en 1974. Ses compétences ayant été bien appréciées, il a été invité à la Conférence nationale de science (全国科学大会) coorganisée par le Comité central du Parti communiste chinois et le gouvernement de PRC en 1978 au 12ème Congrès national du Parti (中国共産党全国代表大会) en 1982.

[12] NHK, 2019

Après d'avoir quitté l'APL en 1982, il a créé Huawei avec ses collaborateurs à l'âge de 43 ans, en utilisant son indemnité de retraite. Huawei a bien réussi principalement au sein des marchés ruraux chinois. Son chiffre d'affaires a atteint 1,5 milliards de yuans en 1995.

Aujourd'hui Huawei est un géant des TIC chinois mais elle n'est pas cotée en Bourse alors que d'autres grandes entreprises chinoise de TIC le sont : Alibaba en Bourse de New York et de Hongkong, ZTE en Bourse de Hongkong et de Shenzhen, Tencent en Bourse de Hongkong et Hytera en Bourse de Shenzhen. Huawei emploie un programme d'actionnariat salarié (ESOP - Employee Stock Ownership Program). Son site internet explique que l'entreprise est détenue par ses employés par le biais d'ESOP mis en place depuis sa fondation et « *Personne ne peut détenir de part sans travailler chez Huawei, et en 2018, l'entreprise comptait 96 768 employés actionnaires. Notre fondateur, Ren Zhengfei, détient une participation de 1,14 % dans l'entreprise.* »[13]. De ce fait, les activités de Huawei sont plus opaques que d'autres entreprises chinoises cotées en Bourse. Le seul document disponible en ligne est son « Annual Report » mais du fait que Huawei n'est pas cotée en Bourse, personne ne peut réellement contrôle la fiabilité de ces rapports annuels d'activités. En outre, le corpus de ces rapports annuels ne permet de suivre toute l'histoire de Huawei qui a commencé à publier son « Annual Report » seulement à partir de 2006.

1.1.2 Réussite en Europe

Après son essor sur le marché intérieur chinois, Huawei a commencé ses affaires en Europe en 2000. Cette année-là, Huawei a établi un centre de R&D en Suède.

Huawei a ensuite développé son partenariat avec les entreprises de

[13] Site internet de Huawei « Qui détient Huawei ? »

télécommunication européenne. Par exemple, en 2004, Huawei a passé l'examen de qualification de France télécom[14] et l'entreprise allemande, Siemens, a signé un accord de partenariat avec Huawei[15]. L'opérateur néerlandais, Telfort, a signé, pour sa part, un contrat estimé à plus de 25 millions de dollars, en 2004, afin de développer ses réseaux de 3G[16]. Au début des années 2000s, l'Europe était déjà un champ de bataille important pour Huawei afin de réaliser son expansion mondiale parce que l'Europe est un marché important pour les TIC (forte demande solvable, non saturation américaine du marché…), et aussi parce qu'elle est le berceau de rivaux, comme Alcatel, Ericsson et Nokia.

Durant les années 2000, Huawei a été choisi comme partenaire des principaux opérateurs européens tels que Vodafone, British Telecom (BT), France Télécom (Orange), Telefonica[17]. Huawei a aussi remporté en 2006 le contrat de construction des réseaux 3G en République tchèque en partenariat avec Vodafone[18]. Elle a ouvert un « Centre de logistique européenne » en Hongrie, en 2013, qui est en charge de l'approvisionnement pour les pays en Europe, l'Asie centrale, le Moyen-Orient et Afrique[19]. Durant les années 2010 et suivantes, on peut aussi observer certaines évolutions sectorielles dans l'expansion économique de Huawei en Europe en particulier une spécialisation dans le « cloud computing » et les centre de données (« data centers »). En 2014, Huawei a construit une plateforme de cloud pour le moteur de recherche français, Qwant[20]. En 2015, des opérateurs de télécommunication comme Telefonica, Vodafone, ont intégré le système de stockage de données

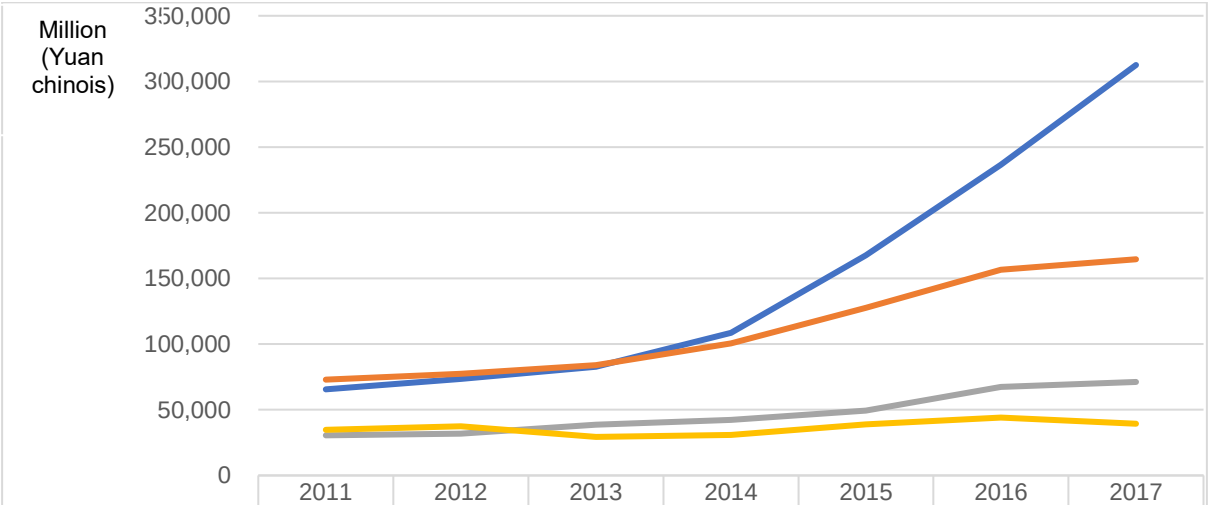
[14] Henni, 2006
[15] Silicon, 2004
[16] Harney, 2004
[17] Huawei Investment & Holding Co., Ltd., 2006
[18] Cordoue, 2006
[19] Huawei Investment & Holding Co., Ltd., 2013
[20] *Ibid.*, 2014

développé par Huawei à leur système central. La même année, SFR a obtenu « Fusionsphere Cloud Operating System » de Huawei[21]. En outre, Vodafone Italy a déployé les réseaux « Cloud-based » VoLTE (Voice over LTE), technologie de télécommunication des données, pour les usages commerciaux avec l'assistance technologique de Huawei[22]. Ainsi Criteo, entreprise française de re-ciblage publicitaire sur Internet, a employé le service du centre de données construit par Huawei[23].

Quant aux chiffres d'affaires, en 2005, les ventes hors de Chine ont, pour la première fois, dépassé celles réalisées sur le marché domestique. En 2013, l'Europe est devenue le plus grand marché dans le monde derrière la Chine[24]. La répartition géographique du chiffre d'affaires de Huawei est indiquée en 2011 dans son « Annual Report ». Il est néanmoins difficile de préciser ce qui concerne l'Europe, car celle-ci est fusionnée, dans les calculs de Huawei, avec les chiffres du Moyen-Orient et de l'Afrique au sein de la catégorie « EMOA » (Europe, Moyen-Orient et Afrique) ; en outre, la définition géographique de l'Europe dans l'« Annual Report - 2011 » de Huawei n'est pas claire. Cependant, en suivant les rapports annuels de Huawei, on peut constater la croissance forte et constante de sa revenue en EMOA, beaucoup plus forte, par comparaison, que celle observable sur les continents américains et dans la zone Asie-Pacifique (cf. : Graphique 1, ci-dessous).

[21] Huawei Investment & Holding Co., Ltd., 2015
[22] Huawei, 2015
[23] Huawei Investment & Holding Co., Ltd., 2015
[24] Nocetti et Seaman, 2019

Graphique 1 : Répartition géographique des chiffres d'affaires de Huawei de 2011 à 2017



	2011	2012	2013	2014	2015	2016	2017
Chine	65,565	73,579	82,785	108,674	167,690	236,512	312,532
EMOA	72,956	77,414	84,006	100,674	127,719	156,509	164,603
Asie Pacifique	30,546	31,846	38,691	42,409	49,403	67,500	71,199
Amériques	34,862	37,359	29,346	30,844	38,910	44,082	39,470

(Source : Annual Report de Huawei de 2012 à 2017)

L'essor de Huawei au Royaume-Uni a été particulièrement remarquable. Depuis 2006, Huawei est choisie comme fournisseur des équipements par les grands opérateurs britanniques que sont « BT » et « Vodafone ». En 2006, Vodafone a décidé de travailler avec Huawei pour construire en Espagne des réseaux commerciaux de HSDPA (High-Speed Downlink Packet Access), une sorte de réseau de 3G[25]. Lors de la construction du « broadband » (accès à Internet à très haut débit) par fibre-optique de BT au Royaume-Uni, en 2012, Huawei était le principal fournisseur de composants[26]. En 2009, Huawei a créé une co-entreprise « Huawei Marine », en partenariat avec « Global Marine Systems », fournisseur britannique des services de l'installation et du maintien de câbles sous-marins. Huawei Marine a réalisé 90 projets

[25] Huawei Investment & Holding Co., Ltd., 2006
[26] Garside, 2012

dans le monde et instauré 50 351km de de câbles sous-marins jusqu'à 2019[27]. Mais, Huawei Marine a échoué à installer un câble sous-marin entre New York et Londres en raison des oppositions de l'administration américaine en 2013[28]. En 2019, Huawei a vendu la co-entreprise à Hengtong Optic-Electric, fabricant chinois de câbles optiques.

Les activités de Huawei étaient tellement appréciées au Royaume-Uni qu'elle a reçu le prix « Boldness in Business » dans la catégorie de « Emerging Market » (marché émergent) du *Financial Times*, en 2009 avec une évaluation très laudative du journaliste Dan Bogler, membre du jury : « *En développant une entreprise prospère en Europe, elle est devenue l'une des rares entreprises chinoises - sinon la seule - à faire sensation sur la scène internationale.* »[29] [30].

En plus du *Financial Times*, une autre organe de presse britannique, *The Economist*, a remis à Huawei l'« Innovation Award » (prix d'innovation) avec une mention « Corporate use of innovation » (innovation à usage corporatif) en 2010. Le commentaire présente Huawei comme « *Le plus grand fabricant chinois d'équipements de télécommunications. Autrefois considéré uniquement comme un fournisseur à bas prix, il est désormais respecté par les opérateurs de télécommunications du monde entier pour la qualité de ses produits, remettant en cause l'idée que les entreprises chinoises ne sont que des imitateurs plutôt que des innovateurs.* » [31] [32]. Vodafone a remis à Huawei le « 2007 Global Supplier Award »

[27] Marchand, 2019
[28] Manière, 2019
[29] Financial Times, 2009
[30] « *By growing a successful business in Europe, it has become one of only a handful of Chinese companies - if not the only one - that it really making a splash on the international scene.* »
[31] The Economist, 2010
[32] « *China's largest maker of telecoms equipment. Once seen solely as a low-cost vendor, it is now respected by telecoms operators around the world for the quality of its products, challenging the notion that Chinese firms are merely imitators rather than innovators.* »

(Prix de fournisseur mondial 2007) parce ce qu'elle avait fourni les produits et les services compétitifs[33]. En 2018, Vodafone lui a encore offert le « Supplier of the Decade Award » (Prix de fournisseur de la décennie). Lors de la cérémonie de la remise du prix, Ninian Wilson, Directeur pour la Chaine mondiale d'approvisionnement et PDG de Vodafone Procurement Company (VPC) a dit :« *Huawei a pris l'initiative de s'implanter au Luxembourg pour soutenir VPC dès le début. Au cours de la dernière décennie, notre partenariat stratégique s'est développé et s'est épanoui grâce à l'engagement de Huawei à grandir main dans la main avec VPC et à établir progressivement la confiance en tant que partenaire fiable.* »[34] [35]. En 2013, le PDG de BT, Gavin Patterson, a mentionné Huawei en tant que « good partner » (bon partenaire)[36].

Par ailleurs, Huawei est très actif dans les activités pour la Responsabilité sociale de l'entreprise (Corporate Social Responsibility) et réalise beaucoup de programmes de cohésion avec des acteurs locaux au sein de l'Union. Par exemple, en 2010 en France, elle a commencé à offrir des programmes de formations aux élèves de l'École polytechnique afin de leur permettre d'effectuer leur stage au sein de l'entreprise[37].

1.1.3 Développement en Afrique

Huawei a développé ses activités commerciales depuis quelques décennies. Les

[33] Huawei Investment & Holding Co., Ltd., 2007
[34] Huawei Europe, 2018
[35] « *Huawei took the initiative to set up operations in Luxembourg to support VPC right from the very beginning. Over the past decade, our strategic partnership has grown and flourished thanks to Huawei's commitment to growing hand in hand with VPC and building trust as a reliable partner gradually over time.* »
[36] Mehta, 2013
[37] Huawei Investment & Holding Co., Ltd., 2011

opérateurs africains ont apprécié le prix bas de ses produits et services comparés à ceux des marques américaines ou européennes. Les entreprises de télécommunication chinoises, y compris ZTE, sont très actives partout en Afrique, en particulier en Afrique du Sud, Algérie, Angola, Égypte, Maroc, Nigéria et Tunisie. Aujourd'hui, les composants de Huawei occupent 70% des réseaux de 4G dans l'ensemble de l'Afrique[38].

Le premier marché par lequel Huawei a commencé ses affaires en Afrique est le Kenya[39] et puis l'Afrique du sud (1998). L'Algérie et la Tunisie sont les premiers pays nord-africains dans lesquels elle a lancé ses activités (1999). Elle a ensuite étendu ses affaires à l'Afrique occidentale, notamment en Côte d'Ivoire, et à l'Afrique centrale, en République démocratique de Congo en 2006. Comme indique le Tableau 1, Huawei a d'abord entamé ses affaires dans les pays africains plutôt développés comme le Kenya, l'Afrique du Sud, les pays maghrébins, l'Égypte. Après son implantation réussie dans ces pays, de plus en plus, elle a étendu ses activités vers les économies africaines plus fragiles et réalisé ses projets même dans les petits pays, souvent avec une aide financière offerte par les banques du développement de Pékin.

[38] Ehl, 2022
[39] Chang et al., 2009

Tableau 1 : Chronologie du développement des activités principales de Huawei en Afrique[40] [41] [42] [43]

1998	**Kenya et Afrique du sud** : Lancement des affaires de Huawei
1999	**Algérie, Maroc et Tunisie** : Lancement des affaires de Huawei
2000	**Égypte** : Lancement des affaires de Huawei
2003	**Algérie** : Expansion du réseau GSM (Global System for Mobile Communications) par Huawei
2004	**Nigéria** : Prêt de 200 millions dollars de China Development Bank pour introduire des équipements de Huawei
2005	**Afrique du Sud** : Signe du partenariat stratégique entre l'opérateur sud-africain, MTN, et Huawei
2006	**Côte d'Ivoire et République démocratique Congo** : Lancement des affaires de Huawei **Kenya** : Lancement du projet de 25 millions dollars pour développer les télécommunications rurales de Huawei
2007	**Côte d'Ivoire** : Développement du centre de donnée pour l'e-gouvernement par Huawei
2009	**Cameroun** : Signe de l'accord du prêt de 52 millions dollars avec CEXIM pour le projet d'installer la fibre optique de Huawei
2011	**Mali** : Développement du réseau de câble fibre-optique par Huawei et accord du prêt de 63 millions dollars de la CEXIM pour développer le réseau national de broadband par Huawei

[40] Chang et al., 2009
[41] IDE-JETRO, 2009
[42] Zoa Ateba, 2016
[43] Sacks, 2021

2013	**Gambie** : Signe du contrat de 33 millions dollars pour installer un câble fibre-optique qui connecte avec les autres pays de la CEDEAO
2014	**Burundi** : Lancement du développement du réseau de broadband en partenariat avec un opérateur des télécommunications régional, Onatel **Gabon** : Signature du contrat de 26 millions dollars pour construire un câble fibre-optique qui connecte avec la République du Congo
2015	**Bénin** : Signature du prêt 69 millions dollars par CEXIM pour développer l'infrastructure des télécommunications et le broadband fibre-optique de Huawei
2016	**Tanzanie** : Le déploiement du service des réseaux 4,5G par Huawei
2017	**République du Congo** : Signature de l'accord du prêt de 161 millions dollars avec CEXIM pour faire développer à Huawei le réseau des télécommunications national **Rwanda** : Signature du MOU avec Huawei pour construire des centres de données régionales et développer le service de broadband
2018	**Lybie** : Développement des réseaux de 4G par Huawei **Mozambique** : Signature de l'accord entre l'opérateur, le Mozambique Cellular et Huawei pour la désigner comme fournisseur préféré
2019	**Mauritanie** : Accord de coopération entre l'opérateur des télécommunications mauritanien, Mattel, et Huawei

Les caractéristiques de la pénétration des entreprises chinoises en Afrique sont en relation étroite avec l'État chinois et les entreprises publiques, notamment à travers des dispositifs tels que les subventions par l'État[44] ou la banque nationale pour le développement, et la pénétration au sein des réseaux de l'administration publique. Au contraire des pays occidentaux, les coopérations avec Pékin ne sont pas toujours conditionnées par la réforme politique ou économique [45] telle que la bonne gouvernance. C'est une des raisons pour lesquelles les pays africains dépendent des aides au développement de la Chine.

La Chine dispose de trois banques nationales pour l'investissement à l'étranger : China Development Bank (国家开发银行), the Export-Import Bank of China (中国进出口银行) et Agricultural Development Bank of China (中国农业发展银行). Elles relèvent directement de l'autorité chinoise et elles sont mobilisées pour impulser les politiques étrangères de la Chine. Ces banques fournissent les crédits aux entreprises chinoises et leur permettent de conduire les affaires même dans les pays à risque commercial comme les pays africains. Par exemple, le Cameroun a signé un accord de prêt préférentiel d'un montant de 52 millions dollars américains avec Export-Import Bank of China (CEXIM) en 2009 pour le projet d'installer la fibre optique qui a été réalisé par Huawei[46]. Yaoundé a également signé avec cette banque deux autres accords de prêt d'un montant de 168 millions dollars pour le projet de construction du réseau national Broadband et de celui de 65,5 millions dollars pour le projet de numérisation des affaires postales[47]. Ce dernier a été mis en œuvre par Huawei.

Quant aux domaines des activités des entreprises chinoises, un autre exemple de

[44] Donnan et Oliver, 2014
[45] Le Gouriellec, 2022
[46] Zoa Ateba, 2016
[47] *Ibid.*

Cameroun est remarquable. Le Cameroun a signé une convention de financement avec la Chine en 2013 pour le projet du plan national de télécommunications d'urgence[48]. Ce projet porte sur les réseaux des télécommunications sur l'ensemble de territoire camerounais, y compris les systèmes de vidéo conférence et de vidéo surveillance, qui permettent aux entités chinoises de capter des renseignements sensibles de l'État. Cette tendance à l'œuvre au sein de l'administration publique des autres pays est similaire en différentes exploitations par la Chine à l'étranger. Par exemple, l'Union africaine (UA) a trouvé des outils d'espionnage fabriqué par Huawei (Huawei nie ce soupçon.) au sein du bâtiment de l'UA construite par les entreprises chinoises[49]. Il faut noter que la pénétration des marchés internationaux par les entreprises chinoises n'est pas nécessairement due à la motivation purement commerciale mais aussi étatique.

1.2 Risque de Huawei

Huawei a réalisé un essor de grande ampleur au sein du marché mondial, mais elle est souvent critiquée pour plusieurs raisons et/ou soupçons. On peut remarquer que les motifs de critique semblent se multiplier au cours du développement historique de l'entreprise. Le conflit avec Huawei a commencé par un soupçon de vol de propriété intellectuelle. Ensuite les États-Unis et le Royaume-Uni ont évoqué un soupçon de l'espionnage par Pékin à travers des équipements de Huawei. En outre, la législation des lois concernant la sécurité des réseaux et du renseignement en Chine a accru les soupçons des pays occidentaux. Dans cette partie, l'on aborde la transition et l'expansion des soupçons sur Huawei.

[48] Zoa Ateba, 2016
[49] Kadiri et Tilouine, 2018

1.2.1 Vol de la propriété intellectuelle

Le premier problème causé par Huawei a été le vol illégal de la propriété intellectuelle dans les années 2000. En janvier 2003, Cisco Systems, entreprise américaine de télécommunication, a accusé Huawei de violer son brevet et de copier illégalement son code-source, ceci devant la Cour fédérale de district à Texas. Les deux parties ont réglé ce litige en dehors de la cour en juillet 2004[50] après que Huawei a reconnu avoir copier le logiciel de certains routeurs de Cisco[51].

Des doutes similaires sont apparus chez d'autres entreprises telle que Nortel, entreprise canadienne de TIC qui a fait faillite en 2009, Motorola (2010), équipementier américain de télécommunications, T-Mobile (2012 - 2013), opérateur américain de télécommunications. Motorola et T-Mobile ont individuellement attaqué Huawei en justice. Le cas de Motorola avait été réglé entre les deux parties en dehors de la cour en 2011[52] comme celui de Cisco, mais T-Mobile a attendu la sentence.

Selon l'argument de T-Mobile[53], deux employés de Huawei ont visité un laboratoire de l'opérateur américain à Bellevue, État de Washington, de 2012 à 2013 et ils ont pris des photos de Tappy, robot de T-Mobile pour tester le smartphone, dans les locaux et l'un des deux a volé son composant. T-Mobile a accusé Huawei en 2014 pour espionnage industrielle et non-respect du contrat signé entre les deux entreprises. En 2017, la Cour fédérale à Seattle a admis partiellement l'argument de T-Mobile sur l'espionnage du secret industriel commis par les employées de Huawei mais le juge a

[50] Flynn, 2004
[51] Yap et al., 2019
[52] Motorola Solutions, 2011
[53] Lerman, 2017

décidé que leurs actions n'avaient pas été « willful and malicious » (volontaires et malveillantes). De ce fait, la cour a ordonné à l'équipementier chinois de payer la réparation de 4,8 millions dollars à T-mobile due au non-respect du contrat entre les deux entreprises.

Créé à Montréal en 1895, Nortel était toujours un pionnier des TIC en ayant développé des technologies numériques de fibre optique. En 2012, Wall Street Journal a dévoilé que Nortel a pu être exposé a des cyberattaques massives en provenance de la Chine[54]. Brian Shields, alors conseiller supérieur pour la sécurité des systèmes qui a travaillé pour Nortel pendant 19 ans, a effectué en 2008 une enquête auprès des réseaux de l'entreprise et détecté des traces de pénétration probable de la Chine. Il a signalé aussi la possibilité d'hacking aux dirigeants de Nortel mais ils n'y ont pas cru[55]. L'entreprise des TIC canadienne a fait faillite en 2009. Shields prétend que les cyberattaques ont commencé au plus tard en 2000 et que les hackeurs ont volé des plans d'affaires, des rapports de R&D, des courriels d'employées[56]. Il pense que les données volées par les cyberattaques ont été transmises aux entreprises chinoises de TIC comme Huawei et ZTE et que cela a entraîné la faillite de Nortel. Il a répondu à l'interview du média canadien en 2012 que « *C'était pour le compte de Huawei et de ZTE et d'autres entreprises chinoises qui auraient pu utiliser ces informations pour nous concurrencer sur le marché. Cela leur a donné un avantage stratégique. Comment pouvez-vous survivre quand vous avez un concurrent sur place qui connaît tous vos mouvements, ce que vous faites, ce que vous voyez comme futurs produits ?* »[57] [58]. Selon OSAWA Jun, maître de recherche de l'Institut Nakasone pour

[54] Gorman, 2012
[55] Berkow, 2012
[56] CBC News, 2012
[57] Payton, 2012
[58] « *It was on behalf of Huawei and ZTE and other Chinese companies that could have used*

la paix, TONG Wen (童文) et ZHU Peiying (朱佩英), anciens employés de Nortel engagés dans la recherche sur la technologie de communication sans fil, ont intégré Huawei en 2009 et ils jouent un rôle central pour développer la recherche relative au réseau 5G[59]. Ils sont maintenant titularisés en tant que « Huawei Fellow ».

1.2.2 Soupçons d'espionnage et relations avec l'État chinois

Huawei est soupçonnée d'installer un backdoor dans ses équipements et les contenus des télécommunications. Les renseignements sensibles ou les données personnelles circulant sur les réseaux peuvent fuir à Pékin à travers ses équipements. Cette inquiétude s'aggrave parce que Huawei s'engage beaucoup dans les affaires de construction des réseaux, autrement dit au cœur du système des télécommunications. La méfiance contre Huawei en matière d'espionnage et de relation avec l'État chinois a commencé dans les années 2000 au sein de l'administration et du parlement américains.

En 2005, les chercheurs de la RAND Corporation, think-tank américain, ont réalisé une étude intitulée « *A New Direction for China's Defense Industry* »[60] (Une nouvelle orientation pour l'industrie de défense de la Chine) dont l'un des auteurs est Evan Medeiros, future Conseiller spécial auprès du Président Barack Obama et Directeur supérieur pour les Affaires de l'Asie du Conseil de la sécurité nationale de la Maison blanche. C'est l'Armée de l'air des États-Unis qui a originairement financé et demandé cette étude. Le rapport analyse l'industrie militaire de la Chine et aborde la relation entre les TIC chinoises, y compris Huawei, et l'État chinois dans l'un de ses chapitres.

---

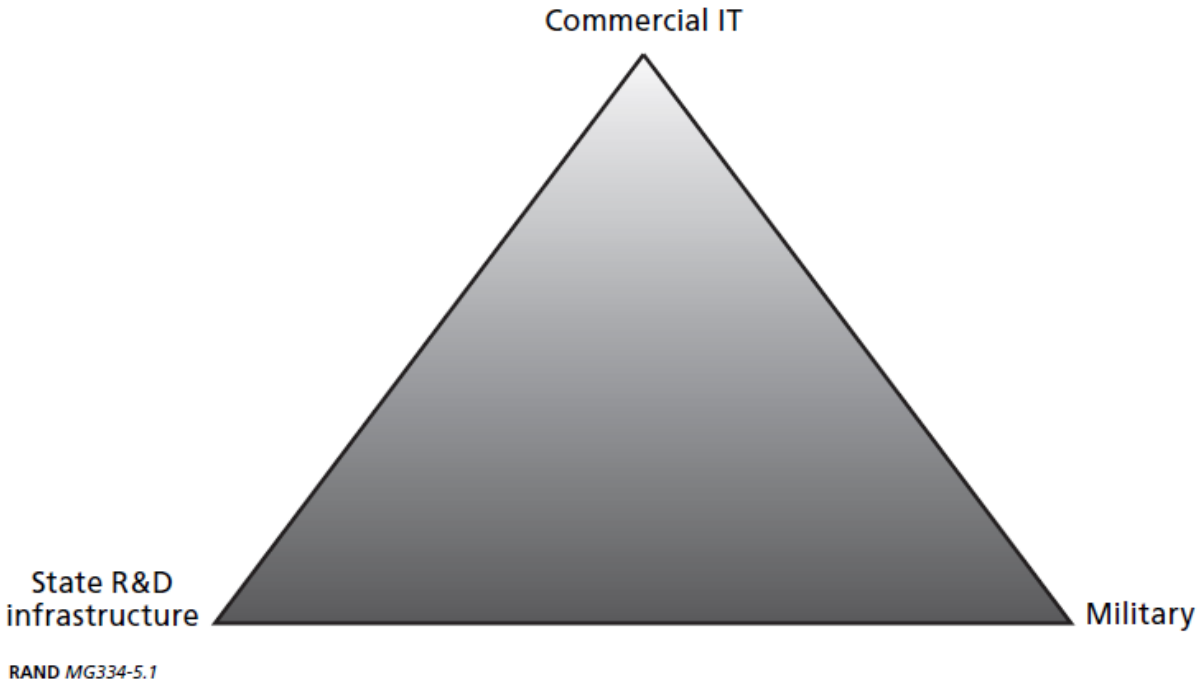
this information to compete against us in the marketplace. It gave them a strategic advantage. How can you survive when you have a competitor basically right there knowing all your moves, what you're doing, what you see as the future products? »

[59] Osawa, 2021

[60] Medeiros et al., 2005

Les auteurs soulignent la relation étroite entre Huawei et l'État chinois, notamment l'APL : « *Huawei entretient des liens étroits avec l'armée chinoise, qui joue un rôle à multiples facettes en tant que client important, ainsi qu'en tant que mécène politique et partenaire de recherche et développement de Huawei.* »[61] [62]. En outre, le rapport décrit comment l'industrie militaire chinoise se développe. Selon lui, les TIC privées chinoises, y compris Huawei, représentent une sorte de « digital-triangle model » (modèle de triangle numérique) dans lequel les TIC privées se développent en coopération étroite avec l'État chinois et les dispositifs de R&D étatiques comme esquissé dans le Graphique 2.

Graphique 2 : Les trois sommets du Triangle numérique[63]



[61] Medeiros et al., 2005 p. 218
[62] « *Huawei maintains deep ties with the Chinese military, which serves a multi-faceted role as an important customer, as well as Huawei's political patron and research and development partner.* »
[63] Medeiros et al., 2005 p. 218

Les auteurs expliquent que « *Les entreprises privées chinoises telles que Huawei, en revanche, représentent le nouveau modèle de triangle numérique, dans lequel l'armée, d'autres acteurs étatiques et leurs nombreux instituts de recherche aident à financer et à doter en personnel des entreprises à vocation commerciale qui sont désignées "champions nationaux", reçoivent des lignes de crédit des banques d'État, complètent leur financement de R&D avec de l'argent 893 dirigé et cherchent activement à gagner des parts de marché mondiales. L'armée, pour sa part, en bénéficie en tant que client privilégié et partenaire de recherche.* »[64] [65].

Le premier cas dans lequel l'administration américaine a pris une action publique s'est tenu de 2007 à 2008. En 2007, « 3Com », équipementier américain de télécommunications, est arrivé à un accord pour que « Bain Capital », géant du capital-investissement aux États-Unis, achète « 3Com » en partenariat financier avec Huawei[66]. Le Comité de pour l'Investissement étranger aux États-Unis (Committee on Foreign Investment in the United States : CFIUS), organisation interministérielle de l'administration américaine chargée d'analyser l'acquisition d'entreprises américaines par des compagnies étrangères, a lancé une enquête en raison de l'inquiétude sur l'impact de l'acquisition par l'entreprise chinoise de TIC sur la sécurité nationale des États-Unis. Les parties ont essayé de réduire les inquiétudes du CFIUS par la séparation de l'unité du logiciel de 3Com mais l'administration républicaine de George W. Bush ne l'a pas acceptée[67]. Par conséquent, la négociation de l'acquisition de

[64] Medeiros et al., 2005 p. 206
[65] « *Private Chinese companies such as Huawei, by contrast, represent the new digital-triangle model, whereby the military, other state actors, and their numbered research institutes help fund and staff commercially oriented firms that are designated "national champions," receive lines of credit from state banks, supplement their R&D funding with directed 863 money, and actively seek to build global market share. The military, for its part, benefits as a favored customer and research partner.* »
[66] Reuters, 2007
[67] Weisman, 2008

« 3Com » par Huawei a échoué en mars 2008[68].

On peut constater la même orientation politique de l'administration démocrate. En août 2010, un groupe de huit parlementaires républicains des États-Unis a envoyé au gouvernement de Barack Obama, notamment au Secrétaire du Trésor, Timothy F. Geithner, et au Général de corps aérien James R. Clapper Jr., alors Directeur du Renseignement national, une lettre qui exprimait leur inquiétude sur la participation de Huawei et ZTE à l'adjudication mené par Sprint Nextel, opérateur américain de télécommunications[69]. En dénonçant les relations étroites entre TIC chinoises et APL, ils ont écrit « *Sprint Nextel fournit des équipements importants aux forces armées américaines et aux forces de l'ordre, et propose une large gamme d'appareils, de systèmes, de logiciels et de services au secteur privé* »[70] et « *Nous craignons que la position de Huawei en tant que fournisseur de Sprint Nextel ne crée un risque substantiel pour les entreprises américaines et ne porte atteinte à la sécurité nationale des États-Unis.* »[71]. En octobre, quatre parlementaires américains, dont des auteurs de la lettre précédente - comme les Sénateurs Jon Kyl et Susan Collins - ont envoyé une autre lettre à la Commission fédéral de Communication et à la Commission de la Sécurité intérieure du Sénat qui souligne l'influence significative de l'APL aux TIC chinoises « *Nous sommes très préoccupés par le fait que ces entreprises sont financées par le gouvernement chinois et sont potentiellement soumises à une influence significative de l'armée chinoise, ce qui pourrait créer une opportunité de manipulation de commutateurs, de routeurs ou de logiciels intégrés au réseau de*

[68] Waters et Politi, 2008
[69] Barboza et al., 2010
[70] « *Sprint Nextel supplies important equipment to the U.S. military and law enforcement agencies, and it offers a broad array of devices, systems, software and services to the private sector* »
[71] « *We are concerned that Huawei's position as a supplier of Sprint Nextel could create substantial risk for U.S. companies and possibly undermine U.S. national security* »

télécommunications américain afin que les communications puissent être perturbées. , interceptées, falsifiées ou délibérément mal acheminés. Cela constituerait une menace réelle pour notre sécurité nationale. »[72] [73]. Finalement, Sprint Nextel a exclu Huawei et ZTE du contrat en octobre 2010 après un échange téléphonique entre le Secrétaire du Commerce, Gary Locke, et le PDG de Sprint Nextel, Dan Hesse, quant aux préoccupations sur la coopération avec les TIC chinoises[74].

Malgré les réactions contre les soupçons ou les engagements politiques de Huawei, la méfiance envers les TIC chinoises n'a jamais cessé à se propager aux États-Unis durant les années 2010. En 2011, le CFIUS a bloqué le deal de Huawei pour acheter « 3Leafs », en raison de l'inquiétude sur la sécurité nationale des États-Unis[75]. En 2012, Permanent Select Committee on Intelligence de la Chambre des représentants du Congrès américain a publié « *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE* » [76], en concluant que « *les risques associés à la fourniture d'équipements par Huawei et ZTE aux infrastructures critiques américaines pourraient saper les intérêts fondamentaux de la sécurité nationale des États-Unis* » [77].

Dans les années 2010, ce n'est pas seulement Washington qui a pris une position très forte contre les TIC chinoises. L'Australie a décidé d'exclure Huawei de son projet

[72] U.S. Senate Committee on Homeland Security & Governmental Affairs, 2010
[73] « *We are very concerned that these companies are being financed by the Chinese government and are potentially subject to significant influence by the Chinese military which may create an opportunity for manipulation of switches, routers, or software embedded in American telecommunications network so that communications can be disrupted, intercepted, tampered with, or purposely misrouted. This would pose a real threat to our national security.* »
[74] Lublin et Raice, 2010
[75] BBC, 2011
[76] Permanent Select Committee on Intelligence of the U.S. House of Representatives, 2013
[77] « *the risks associated with Huawei and ZTE's provision of equipment to US critical infrastructure could undermine core US national-security interests* »

de National Broadway Network en mars 2012. Selon la presse[78], Attorney General's Department (Ministère de justice australien) a rejeté Huawei pour « *la sécurité et la résilience de l'infrastructure cruciale de l'Australie* »[79], vu le conseil de Australian Security Intelligence Organization (Service du renseignement australien).

Le Canada a également rejeté Huawei de son projet de construction des nouveaux réseaux des données et des télécommunications de l'administration publique en octobre 2012, en utilisant l'exemption pour la sécurité nationale[80].

En juin 2013, Intelligence and Security Committee du parlement britannique a publié un rapport intitulé « *Foreign involvement in the critical national infrastructure* ». Il a signalé le risque de Huawei pour la sécurité des réseaux des télécommunications au Royaume-Uni de peur que Pékin utilise la vulnérabilité technologique des produits de Huawei pour espionner en Angleterre[81].

En 2018, *Le Monde* a révélé le soupçon de l'espionnage mené par Pékin à travers les produits de Huawei installés au sein du bâtiment de l'UA à Addis-Abeba[82]. Selon l'article, en 2017, les informaticiens qui travaillent au siège de l'UA à Addis-Abeba se sont rendus compte que les immenses données de ses serveurs étaient transférées aux serveurs à Shanghai. Les bâtiments du siège ont été construits en 2012 par les entreprises de construction chinoises, puis équipée également par celles de télécommunications chinoises, dont Huawei[83], qui a permis la fuite des différentes données sensibles de l'UA pendant cinq ans.

Ni Pékin ni Huawei admettent leur engagement dans ces affaires jusqu'à

[78] Lu-YueYang, 2012
[79] « *the security and resilience of Australia's critical infrastructure* »
[80] Palmer, 2012
[81] Intelligence and Security Committee of Parliament, 2013
[82] Kadiri et Tilouine, 2018
[83] Cave, 2018

aujourd'hui.

1.2.3 Obligation juridique soumise par la loi chinoise

En plus des risques technologiques liés à Huawei, en 2017, Pékin a promulgué des lois qui suscitent des inquiétudes : « Loi sur Cybersécurité » (网络安全法) et « Loi sur le Renseignement national » (国家情报法), selon lesquelles l'État chinois peut avoir un accès aux réseaux construits ou gérés par les entreprises chinoises de télécommunications[84].

À propos de la Loi sur Cybersécurité, Clyde E. Wallace, Sous-directeur adjoint (*Deputy Assistant Director*) de la Cyber Division du Bureau fédéral d'enquête (FBI) des États-Unis a dit pendant son témoignage devant le Sous-comité de la Criminalité et du terrorisme du Comité Judiciaire du Sénat en 2020 « *En juin 2017, la RPC a introduit une nouvelle loi nationale sur la cybersécurité qui oblige les entreprises étrangères à stocker les données localement et à se soumettre à des mesures de surveillance des données. (…) Pékin pourrait probablement utiliser ces autorités et politiques pour forcer l'accès aux données personnelles commerciales et sensibles des États-Unis, y compris les informations sensibles stockées ou transmises via les systèmes chinois. Les filiales américaines de sociétés et d'entités chinoises, ou les organisations aux États-Unis qui s'associent à des efforts de recherche et de développement coopératifs, font partie des entités concernées par cette loi. La loi a suscité des craintes chez ceux qui s'inquiètent du contrôle par Pékin des informations sensibles des entreprises et des possibilités accrues de voler la propriété intellectuelle.* »[85] [86]. Wallace a signalé la

[84] National Institute for Defense Studies, 2021, p. 40
[85] Federal Bureau of Investigation, 2020
[86] « *In June 2017, the PRC introduced a new national cyber security law that requires foreign firms to store data locally and submit to data surveillance measures. (...) Beijing could likely use these authorities and policies to compel access to U.S. commercial and sensitive personal*

possibilité que Pékin puisse exercer sa compétence attribuée par cette loi pour exiger des entreprises en Chine de transmettre les renseignements à l'État. Par exemple, l'article 9 de la loi - « *Les fournisseurs d'accès aux réseaux doivent observer les lois et les régulations administratives, respecter la discipline sociale, observer les morales commerciales, (…) effectuer les obligations pour assurer la sécurité des réseaux, recevoir les contrôles par l'État et par la société et soutenir la responsabilité sociale.* » [87] [88] - est tellement ambiguë qu'elle suscite la méfiance envers les opérateurs chinois[89].

L'article 7 de la Loi sur le Renseignement national stipule que les citoyens ou les entités chinois doivent « *soutenir, aider et coopérer au travail du renseignement de l'État* » [90] [91] [92]. Cela veut dire que Pékin peut obliger les peuples ou les entités chinoises à contribuer aux intérêts de l'État chinois en matière de renseignement, y compris en ce qui concerne les données personnelles et les informations sensibles.

Pour réduire la méfiance suscitée parmi d'autres pays sur la coopération potentielle avec l'État, le PDG Ren Zhengfei a déclaré que Huawei ne coopérait pas à l'espionnage de l'État même si les lois l'exigent, en répondant à l'interview de CBS en 2019[93] « *Nous ne participons jamais à l'espionnage et nous ne permettons à aucun de nos employés de commettre un tel acte. Et nous n'installons absolument jamais de*

---

data, including sensitive information stored or transmitted through Chinese systems. U.S.-based subsidiaries of Chinese corporations and entities, or organizations in the U.S. partnering on cooperative research and development efforts, are among the entities affected by this law. The law has raised fears by those concerned with Beijing's control of sensitive company information and increased opportunity to steal intellectual property. »

[87] The National People's Congress of People's Republic of China, 2016

[88] « *网络运营者开展经营和服务活动，必须遵守法律、行政法规，尊重社会公德，遵守商业道德，(…) 履行网络安全保护义务，接受政府和社会的监督，承担社会责任。* »

[89] Wagner, 2017

[90] The National People's Congress of People's Republic of China, 2017

[91] Okamura, 2017

[92] «*支持、协助和配合国家情报工作*»

[93] CBS, 2019

portes dérobées. Même si nous étions tenus par la loi chinoise, nous le refuserions fermement »[94]. En outre, lors de la conférence de presse en 2019, ZHANG Yesui, Président de la Commission des affaires étrangères du Congrès national du peuple et ancien ambassadeur chinois à Washington, a souligné la position que le travail du renseignement était mis en œuvre conformément à la loi : « *La Loi sur le Renseignement national stipule non seulement les obligations des organisations et des citoyens de soutenir, d'aider et de coopérer avec le travail de renseignement national conformément à la loi, mais stipule également que le travail de renseignement national doit être effectué conformément à la loi, respecter et protéger les droits de l'homme droits et sauvegarder les droits et intérêts légitimes des individus et des organisations.* »[95] [96].

Cependant, ces paroles ne suffissent pas pour convaincre les clients dans le monde, en particulier les pays développés, à cause du manque de transparence de l'entreprise. Du même que des chercheurs occidentaux expriment des doutes sur ces arguments [97], Keith KRACH, alors Sous-Secrétaire d'État pour l'Accroissement économique, l'énergie et l'environnement des États-Unis, a écrit dans le journal britannique « The Daily Telegraph » en 2020 et alerté sur le risque des TIC chinoises en citant la Loi sur le Renseignement national : « *Huawei et ZTE sont tous deux tenus de respecter la Loi sur le Renseignement national de la Chine, en transmettant toutes les*

[94] « *We never participate in espionage, and we do not allow any of our employees to do any act like that. And we absolutely never install backdoors. Even if we were required by Chinese law, we would firmly reject that* »
[95] The National People's Congress of People's Republic of China, 2019
[96] « *国家情报法不仅规定了组织和公民依法支持、协助和配合国家情报工作的义务，同时也规定了国家情报工作应当依法进行、尊重和保障人权、维护个人和组织合法权益的义务。* »
[97] Kharpal, 2019

données à l'État chinois sur demande. »[98] [99].

2. ACTIONS PUBLIQUES DE L'UNION EUROPÉENNE CONTRE LES ENTREPRISES DES TIC CHINOISES

Après le lancement des affaires en Europe en 2000, Huawei a rapidement occupé une position importante dans le marché européen des TIC. En même temps les soupçons de vols de propriétés intellectuelles et de relations étroites avec l'État chinois pour l'espionnage se sont développés.

Face à ces risques de sécurité économique et celle de l'Union, Bruxelles a décidé de conduire une enquête officielle contre les TIC chinoises pour leur comportement dans le marché tel que le dumping ou les subventions de Pékin, mais seulement en 2013, c'est-à-dire plus tard que les pays anglo-saxons, notamment les États-Unis qui ont bloqué le deal de Huawei pour acheter une entreprise américaine de TIC en raison de l'inquiétude sur la sécurité nationale dès 2008.

Cette action publique européenne dont l'initiative venait principalement de la Commission a eu peu d'effets pour plusieurs raisons : positions discordantes entre la Commission et les États membres, manque de coopération les entreprises européennes, dépendance économique importante de l'économie européenne au marché chinois.

Depuis la fin de cette enquête jusqu'à aujourd'hui, l'Union européenne n'a jamais pris d'initiatives spécifiques aux TIC chinoises. Même si l'enjeu 5G de Huawei a bouleversé le marché mondial des TIC, l'Union n'a pas réorienté ses politiques, ce qui

[98] Krach, 2020

[99] « *Both Huawei and ZTE are required to abide by China's National Intelligence Law, by turning over any and all data to the Chinese government upon request.* »

a entraîné des réponses diverses voire divergentes des États membres vis-à-vis de Huawei. La même observation peut être faite dans le domaine de la politique étrangère de l'Union européenne vers l'Afrique, même si l'on peut constater une évolution du partenariat entre les deux continents ces dernières années.

2.1 Début des années 2010s – sous Commissaire Karel de Gucht -

Au sein de l'Europe, Huawei était mise en cause avec d'autres entreprises chinoises de télécommunications comme ZTE dans le contexte des soupçons de dumping sur le marché européen et des subventions par l'État chinois depuis plusieurs années. L'Union européenne n'a cependant pas eu d'action publique jusqu'en 2013. Alors que les pays anglo-saxons, en particulier les États-Unis, ont graduellement orienté leur attention vers les risques d'espionnage par Huawei dans la même époque, il est remarquable que l'intérêt de l'Union européenne se focalisait toujours essentiellement sur les comportements commerciaux.

Quand l'on parle des actions publiques de l'Union, au début des années 2010, il faut noter un personnage important de la Commission, Karel De Gucht, alors Commissaire belge chargé du commerce (en fonction de février 2010 à novembre 2014). C'est lui qui a pris l'initiative pour essayer de faire adopter des mesures concrètes contre Huawei au sein de l'Union jusqu'à la fin de son mandat en 2014.

2.1.1 Un lancement reporté et une suspension soudaine

En 2010, De Gucht a essayé de lancer une enquête contre Huawei mais elle a été reportée plusieurs fois[100]. Finalement, le 15 mai 2013, la Commission a officiellement annoncé le lancement de l'enquête, la première action publique contre Huawei. Dans

[100] Nakashima, 2019

le communiqué, le commissaire belge a clairement dit que la Commission conduirait « *une enquête d'office antidumping et une enquête antisubventions concernant les importations de réseaux de télécommunications mobiles et de leurs éléments essentiels en provenance de Chine.* »[101] [102] avec un ton explicite voire offensif.

Cependant, l'enquête a été arrêtée le 27 mars 2014, presque une année après son lancement. Certes, la Commission a admis, dans le communiqué[103], que « *l'essentiel des problèmes posés par la concurrence chinoise sur le marché de l'UE était dû au subventionnement des réseaux de télécommunications mobiles* » mais le ton de critique de De Gucht contre les entreprises chinoises s'est bien calmé comparé à celui du 15 mai 2013. Il a expliqué la situation d'une manière plus amicale qu'en 2013 « *La décision de ce jour de refermer le volet antidumping de cette éventuelle action de défense commerciale représente un pas important vers le règlement de l'affaire des télécommunications mobiles dans sa globalité.* » mais aucune démarche concrète n'est prévue pour l'avenir.

2.1.2 Enjeu des panneaux photovoltaïques entre Bruxelles et Pékin

Il serait cependant inexact de considérer que De Gucht a été particulièrement conciliant avec la Chine puisque l'on peut observer une attitude forte de De Gucht sur l'enjeu des panneaux photovoltaïques dans la relation avec Pékin.

Après avoir reçu la requête déposée par EU Pro Sun, une association sectorielle européenne, la Commission a lancé, le 6 septembre 2012 [104], une enquête antidumping au sujet des panneaux photovoltaïques importés de Chine

[101] « *an ex officio anti-dumping and an anti-subsidy investigation concerning imports of mobile telecommunications networks and their essential elements from China* »
[102] European Commission, 2013
[103] Commission européenne, 2014
[104] *Ibid.*, 2012

Alors que De Gucht préparait la mise en œuvre de droits antidumping provisoires sur les produits chinois, compte tenu de l'enquête de mai 2013, il a fait face à la forte opposition de plusieurs États-membres, en particulier l'Allemagne, contre cette mesure[105]. Londres a envoyé une délégation menée par Greg Barker, ministre chargé de l'énergie et du changement climatique, mi-mai, pour convaincre la Commission. Et Philipp Rösler, ministre de l'Économie allemand, a publiquement exigé De Gucht de trouver une autre solution[106].

En outre, Pékin a mobilisé ses entreprises publiques pour le lobbying et il a effrayé le secteur privé européen par des représailles potentielles. Le 26 mai 2013, Li Keqiang, Premier ministre chinois, a dit « *Les affaires relatives à ces deux types de produits nuiront aux industries, aux entreprises et aux emplois chinois et porteront également atteinte aux intérêts vitaux des utilisateurs et des consommateurs européens.* » [107] [108].

Malgré l'opposition des États membres et la pression de Pékin, De Gucht a annoncé que la Commission instituerait des droits antidumping provisoires sur les panneaux photovoltaïques chinois.

2.1.3 Structure d'enjeu similaire, mais plus complexe, au sujet de Huawei

On peut observer une même structure de conflit entre la Commission - en particulier Karel De Gucht - les États membres et Pékin sur l'enjeu politique que représente l'expansion de Huawei. Mais sur cet enjeu et contrairement à ce qui s'est passé sur les panneaux photovoltaïques chinois, une solution amiable a finalement été trouvée. Pour comprendre les raisons de cette différence, il faut examiner plus

[105] Chaffin, 2013 (b)
[106] Chaffin, 2013 (a)
[107] *Ibid.*
[108] « *The cases over these two types of products will hurt Chinese industries, business and jobs and also damage the vital interests of European users and consumers.* »

facteurs qui viennent complexifier le contexte d'action publique européenne par rapport à ce qu'il était pour les panneaux photovoltaïques.

2.1.3.1 Évaluation variée entre les États membres

Au début des années 2010, les évaluations de Huawei au sein de l'Union étaient divergentes. Alors que Karel De Gucht abordait le dossier de façon offensive et que, selon la presse, la Commission s'inquiétait de la sécurité au sujet des réseaux de Huawei - à cause de la possibilité d'espionnage[109] (même si la Commission ne l'admet pas officiellement) - on peut constater une position très différente et beaucoup plus positive de quelqu'un comme Robert Sturdy, eurodéputé britannique, qui a dit, lors de la session sur l'inégalité commerciale entre l'Union et la Chine en mai 2012[110], que : « *Nous avons eu nos désaccords à propos de Huawei, mais c'est une entreprise qui a énormément investi en Europe, et je vois cela comme une énorme opportunité pour l'Union européenne.* » [111] [112]. Après l'annonce officielle de De Gucht sur l'enquête, la France, l'Espagne, la Grèce, l'Italie, la Pologne et le Portugal se sont prononcés en faveur de cette mesure tandis que l'Allemagne, le Royaume-Uni et les pays scandinaves s'y sont opposés[113]. Alors ministre suédoise de commerce, Ewa Björling, a publiquement exprimé son inquiétude au sujet de l'enquête de peur qu'elle endommage la coopération entre les entreprises suédoises et les entreprises chinoises de télécommunication[114].

[109] Bilby, 2012
[110] Commission européenne, 2010
[111] Parlement européen, 2012
[112] « *(W)e have had our disagreements about Huawei, but it is a company which has invested tremendously in Europe, and I see that as a huge opportunity for the European Union.* »
[113] Fleming, 2013
[114] Blenkinsop, 2013

2.1.3.2 Pression de Pékin

La Chine a exercé des pressions contre l'enquête : le 26 mai 2013, presque une semaine après le lancement de l'enquête sur Huawei, Li Keqiang a dit « *Les affaires concernant ces deux types de produits nuiront aux industries chinoises, (…)* »[115] et, apparemment, l'expression qu'il a utilisée - « *ces deux types de produits* »[116] - désigne les panneaux photovoltaïques d'une part et les réseaux des télécommunications d'autre part. Pendant la période de l'enquête sur Huawei, on peut constater que la tension commerciale entre l'Union et la Chine a atteint son apogée. Alors que la Commission effectuait l'enquête sur les panneaux photovoltaïques et les entreprises chinoises de télécommunication, le ministère du Commerce de Pékin (商务部) a lancé une enquête antidumping et antisubventions concernant les exportations de vin européen vers la Chine le 1er juillet 2013[117]. À la suite de l'annonce de l'enquête de Pékin, le Comité européen des Entreprises vins (CEEV), une association qui représente l'industrie viticole européenne a signalé que la viticulture européenne était prise en otage dans cette dispute commerciale et a exigé que l'Union et la Chine négocient pour trouver des solutions amiables aussitôt que possible[118]. Il est très probable que l'objectif était de réorienter les États membres qui s'étaient prononcés en faveur de l'enquête - comme la France, l'Italie, l'Espagne, le Portugal, grands producteurs de vin - vers une opposition à l'enquête.

2.1.3.3 Peur des représailles de la Chine entre les entreprises européennes

Il est également remarquable que les entreprises européennes de

[115] « *The cases over these two types of products will hurt Chinese industries, (…)* »
[116] « *these two types of products* »
[117] Commission européenne, 2014 (a)
[118] Gardner, 2013

télécommunications, Nokia, Alcatel Lucent ou Ericsson[119], en compétition avec celles de la Chine au sein du marché mondial étaient réticentes à coopérer à l'enquête menée pour le marché européen[120]. Elles avaient peur de représailles par Pékin[121], car la fermeture ou la limitation potentielle de leur accès au marché chinois pourraient avoir un grand impact sur leurs affaires en Chine.

2.1.3.4 Accord global d'investissements entre l'Union et la Chine

En outre, il faut noter que, pendant cette époque, la Commission était au début des négociations pour l'Accord global d'investissements (AGI) entre l'Union et la Chine. En mai 2010, De Gucht est arrivé à un accord avec son homologue chinois, Chen Deming, pour lancer un groupe de travail conjoint sur les investissements entre l'Union et la Chine afin d'évaluer des possibilités de négociations potentielles qui prolongeraient cet accord[122]. Le 18 octobre 2013, le Conseil de l'Union a adopté un mandat pour que la Commission négocie l'AGI avec la Chine, en tant que représentant de l'Union. Une négociation officielle a été lancée en novembre 2013 et la première négociation a eu lieu en janvier 2014. De Gucht avait souligné, à Bruxelles en juin 2012, la nécessité des investissements en de provenance de Chine pour l'Europe : « *Le rapport prédit que la Chine réalisera entre 800 milliards et 1 600 milliards d'euros de nouveaux investissements à l'étranger entre 2010 et 2020. C'est une énorme opportunité. (…) L'Europe reçoit nettement plus d'investissements, passant d'un apport moyen de moins d'un milliard d'euros entre 2003 et 2008 à plus de sept milliards l'an dernier. (…) Notamment le fait qu'une Chine plus intégrée a un intérêt plus important dans une économie internationale ouverte. (…) Il y a des avantages massifs*

[119] Honoré, 2014
[120] Nakashima, 2019
[121] Fleming, 2013
[122] Grieger, 2021

pour l'économie européenne à ces entrées accrues. L'Europe doit être de la partie alors que la Chine devient un acteur mondial majeur de l'investissement direct étranger au cours des prochaines années. »[123] [124].

En résumé, la Commission, en particulier Karel De Gucht, était sous forte pression imposée non seulement par les États membres et la Chine mais aussi par les secteurs privés européens, l'industrie viticole et celle des télécommunications, et la nécessité de négociation pour un plus grand accord commercial, en tant que commissaire.

Lors de l'annonce de la suspension de l'enquête, De Gucht a dit : « *Je me réjouis que l'UE et la Chine aient récemment été en mesure de résoudre un certain nombre de différends commerciaux, notamment ceux concernant le polysilicium et le vin, pour lesquels la Chine a clôturé son enquête sans instituer de droit. »* [125]. Il est très probable que la Commission a dû prioriser les accords du polysilicium, c'est-à-dire les panneaux photovoltaïques, et du vin avec la Chine plutôt que l'enjeu de cybersécurité.

2.1.3.5 La fin du mandat de Karel De Gucht

En octobre 2014, la Commission a officiellement conclu l'enquête sur Huawei[126]. De Gucht a quitté la Commission un mois après. Bruxelles s'endormait encore jusqu'à l'éclat de Huawei sur les réseaux 5G. Quant à l'AIG, la Commission a continué la négociation jusqu'au 30 décembre 2020 pour arriver à l'accord. Cependant le

[123] « *The report predicts that China will make between 800 billion and 1.6 trillion euros worth of new investments abroad between 2010 and 2020. That is a massive opportunity. (…) Europe is receiving significantly more investment, moving from an average inflow of less than one billion euro between 2003 and 2008 to over seven billion last year. (…) Not least the fact that a more integrated China has a larger stake in an open international economy. (…) (T)here are massive benefits to the European economy from these increased inflows. Europe needs to be in the game as China becomes a major global player on foreign direct investment over the next few years.* »
[124] European Commission, 2012
[125] Commission européenne, 2014 (b)
[126] Honoré, 2014

Parlement a adopté une résolution indiquant qu'il ne discuterait pas de l'AGI jusqu'à ce que la Chine enlève la sanction imposée contre l'Union (suite à la sanction européenne), en raison des violations des droits de l'homme à Hongkong après l'entrée en vigueur de la Loi de la Sécurité nationale pour Hongkong (香港特别行政区维护国家安全法) et de celle à Xinjiang[127].

2.2 Actions publiques de l'Union après le choc de 5G

Alors que les pays dans le monde faisaient prospérer leurs intérêts vers la nouvelle génération des TIC reliées aux réseaux 5G, l'inquiétude sur la sécurité des réseaux offerts par les TIC chinoises ont augmenté en particulier aux États-Unis.

La technologie de pointe 5G (cinquième génération) permet de réaliser un réseau « *extrêmement réactif - quasi-instantané en réalité - capable de gérer des millions d'objets à la fois* »[128], ce qui peut transformer l'infrastructure socio-économique. La 5G peut faire évoluer « l'Internet des objets » (*Internet of Things : IoT*) grâce à son réseau quasi-instantané et capable de gérer un grand volume de données. L'évolution de l'« IoT » permet, par exemple, de concevoir des véhicules autonomes, des villes intelligentes, des soins et de la chirurgie en distance. En revanche, plus le rôle les TIC devient important, plus la sécurité des réseaux le devient aussi, car une attaque contre l'infrastructure de télécommunication aurait des effets destructeurs non seulement sur l'économie mais aussi sur la société. La vulnérabilité des réseaux est désormais un risque majeur pour la sécurité nationale. C'est ce qui explique l'accroissement de l'inquiétude envers les TIC chinoises dans les pays occidentaux.

Face à ce risque, Washington a pris des mesures rapides et fortes contre les TIC

[127] European Parliament, 2022
[128] Dumoulin, 2019

chinoises tandis que l'Union européenne hésitait et avançait d'une manière différente de celle de l'époque du Commissaire Karel De Gucht.

2.2.1 Actions publiques hors de l'Union

En raison du risque d'espionnage par Pékin à travers les produits de Huawei et de l'inquiétude sur la Loi sur le Renseignement national, Washington a d'abord pris une mesure tendant à bloquer Huawei, ceci avec le soutien des deux grands partis américains. Devenu Président des États-Unis, Donald Trump, a signé, le 18 mars 2018, le « *John S. McCain National Defense Authorization Act for Fiscal Year 2019* » qui interdit aux chefs des ministères fédéraux et des entreprises publiques de se procurer ou de renouveler un contrat pour obtenir des équipements, systèmes, ou services employant les produits de Huawei ou de ZTE, pour les composants essentiels[129]. En outre, le Président Trump a également signé l'« *Executive Order 13873 of May 15, 2019* » qui interdit les activités commerciales impliquant des ennemis étrangers parce qu'elles suscitent des inquiétudes sur la sécurité nationale. Ces politiques subsistent même après la passation de pouvoir au Président Joe Biden. Lors du tour en Afrique (Afrique du Sud, Angola et Gabon) en mai 2022, Wendy Sherman, Secrétaire adjointe d'État des États-Unis, a clairement expliqué la position de l'administration Biden sur Huawei : « *Il ne s'agit pas de jeter de l'ombre sur Huawei. (…) Nous croyons que lorsque des pays choisissent Huawei, ils renoncent potentiellement à leur souveraineté. Ils transfèrent leurs données à un autre pays. Ils peuvent se retrouver à apporter une capacité de surveillance dont ils ne savaient même pas qu'elle était là. Nous avons donc fait part très publiquement de nos préoccupations concernant Huawei, et nous sommes donc heureux qu'Africell puisse fournir au peuple angolais un outil sûr et*

[129] Section 889, John S. McCain National Defense Authorization Act for Fiscal Year 2019

capable entre ses mains pour atteindre le monde. » [130] [131].

À la suite des États-Unis, l'Australie a également expulsé Huawei du développement des réseaux 5G en août 2018[132]. Au Royaume-Uni, Huawei était un partenaire très important pour les opérateurs britanniques, notamment BT, Vodafone, mais Londres a finalement décidé d'expulser les équipements de Huawei de ses réseaux 5G le 14 juillet 2020[133].

2.2.2 Actions publiques par la Commission, sans cible spécifique

Au sein de l'Union européenne, après l'enquête menée par Karel De Gucht, aucune action publique ciblant spécifiquement Huawei ou d'autres entreprises des télécommunications chinoises n'a été prise jusqu'à aujourd'hui. À propos des réseaux 5G, le 19 janvier 2020, la Commission a publié « *Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures* » pour inviter les États membres à faire attention aux risques des réseaux 5G mais cela n'a aucune force contraignante sur les États membres.

En 2016, l'Union avait promulgué une directive pour renforcer la sécurité des réseaux[134]. L'article 1er § 2 a) et d) de la Directive oblige les États-membres d'adopter « *une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information* » et la Directive « *établit des exigences en matière de sécurité et de*

[130] Department of State of the United States of America, 2022
[131] « *It's not about throwing shade on Huawei. (...) We believe that when countries choose Huawei, they are potentially giving up their sovereignty. They are turning over their data to another country. They may find themselves bringing in a surveillance capability they didn't even know was there. So we've been very public about our concerns about Huawei, and so we are glad that Africell can provide to the people of Angola a safe, capable tool in their hands to reach out to the world.* »
[132] BBC, 2018
[133] U.K. Government, 2020
[134] Directive (UE) 2016/1148

notification pour les opérateurs de services essentiels et pour les fournisseurs de service numérique ».

De plus, la Commission a déposé la proposition de directive «*concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148*. », le 16 décembre 2020, pour élargir le champ d'application de la directive, notamment au secteur public[135]. La Commission a déjà reçu des avis sur la directive de la part des institutions européennes concernées (Comité économique et social européen, Banque Centrale européenne), ceci depuis le 17 décembre 2020, mais aucune conclusion n'a encore été adoptée jusqu'à aujourd'hui.

Ainsi, ne peut-on pas dire que l'Union, en particulier la Commission, n'a rien fait pour protéger les réseaux européens. Cependant les mesures adoptées par Bruxelles ne parviennent pas à aligner la réponse de tous les États membre contre Huawei.

2.2.3 Critiques de Huawei au sein du Parlement européen

En revanche, les critiques contre Huawei au sein du Parlement européen se sont développées en 2019. Le 13 février 2019, le Parlement a organisé un débat intitulé « Les menaces pour la sécurité liées à la présence technologique croissante de la Chine dans l'UE et les actions possibles à l'échelle de l'UE pour les réduire » [136]. Le 12 mars 2019, il a adopté une résolution qui signalait les préoccupations sur les équipementiers de pays tiers, en précisant le contexte : celui de l'adoption de la Loi sur Renseignement national de la Chine. Et il invitait la Commission à évaluer l'effectivité du cadre juridique de l'Union, notamment de la Directive (UE) 2016/1148

[135] Commission européenne, 2020
[136] Parlement européen, 2019 (b)

pour la cybersécurité de l'Union[137].

La session du 13 février 2019 a commencé par une déclaration de George Ciamba, représentant du Président du Conseil de l'Union et alors ministre délégué aux Affaires européennes de la Roumanie, qui a dénoncé la Chine pour l'accès limité au marché chinois et les vols de propriétés intellectuelles par les entreprises chinoises. Cependant le ministre roumain n'a pas abordé le risque de cybersécurité avec la Chine. Julian King, alors Commissaire à la Sécurité de l'Union, n'a jamais non plus dénoncé la Chine dans sa déclaration sauf par une allusion à la Loi sur le Renseignement national et sa parole était peu précise. Il a souligné l'effectivité des droits européens actuels, notamment la Régulation (UE) sur les investissements directs étrangers et la Directive (UE) 2016/1148. Il a indiqué que « *le règlement établira un mécanisme permettant aux États membres et à la Commission de s'entraider lorsqu'un investissement étranger dans des infrastructures technologiques critiques (…) pourrait affecter la sécurité ou l'ordre public d'autres États membres ou de l'Union elle-même. La Commission pourra également émettre des avis, en particulier lorsque des projets et programmes de l'Union sont potentiellement à risque. (…) Il y a des mesures en place pour renforcer la cybersécurité au niveau de l'UE. Par exemple, la plupart des États membres ont déjà transposé en droit national la directive sur la sécurité des réseaux et des systèmes d'information (SRI). C'était la première législation à l'échelle de l'UE dans ce domaine, et pour tous les États membres qui ne l'ont pas encore transposée, je pense qu'ils seraient bien avisés de le faire.* »[138] [139]. En revanche,

[137] Parlement européen, 2019 (c)
[138] Parlement européen, 2019 (b)
[139] « *The regulation will establish a mechanism enabling Member States and the Commission to assist each other where a foreign investment in critical technology infrastructure (...) could affect the security or public order interests of other Member States or of the Union itself. The Commission will also be able to issue opinions – in particular when Union projects and programmes are potentially at risk. (...) (T)here are measures in place to boost cybersecurity*

plusieurs eurodéputés ont spécifiquement dénoncé Huawei. Jiří Pospíšil, eurodéputé tchèque (PPE), a critiqué la parole de Julian King comme très générale et il a présenté l'avertissement émis par l'autorité nationale tchèque en charge de cybersécurité contre les menaces de Huawei et ZTE pour la sécurité des réseaux. De plus, il a exigé une « réponse européenne » à ce sujet. Peter Kouroumbashev, eurodéputé bulgare (S&D), a renchérit sur la parole de cet eurodéputé tchèque quant à la nécessité d'une « réponse européenne ». Reinhard Bütikofer, eurodéputé allemand (Vert/ALE), a exprimé la méfiance contre Huawei dans le contexte de la Loi sur le Renseignement national et il a insisté sur la nécessité d'expulser les entreprises des télécommunications chinoises des réseaux 5G comme Canberra l'avait fait. Gilles Lebreton, eurodéputé français (ENL), a également abordé la nécessité de l'exclusion de Huawei.

En plus de la session sur le risque des réseaux des télécommunication chinois, lors du débat en plénière à Strasbourg sur le Règlement (UE) 2019 établissant un Cadre pour le filtrage des investissements directs étrangers dans l'Union en février 2019, Christofer Fjellner, eurodéputé suédois (PPE), a aussi exprimé son inquiétude envers Huawei en ce qui concerne la sécurité des réseaux des télécommunications[140]. Agnes Jongerius, eurodéputée néerlandaise (S&D), a signalé d'éventuelles acquisitions d'entreprises européenne par Huawei et Dita Charanzová, eurodéputée tchèque (ADLE), a dit « *Je conviens qu'il s'agit d'un texte législatif important, qui répond à certaines des préoccupations actuellement liées aux investissements dans des secteurs sensibles en Europe. Ces préoccupations existent, divers États membres*

at EU level. For example, most Member States have already transposed into national law the Security of Network and Information Systems (NIS) Directive. That was the first EU—wide legislation in this area, and for any Member States who have not yet transposed this, I think they would be well advised to do so. »

[140] Parlement européen, 2019 (a)

y sont confrontés (…) si nous avions ce règlement en place aujourd'hui, nous pourrions proposer une approche plus coordonnée à certaines des entreprises chinoises, Huawei par exemple. »[141].

En outre, pendant la session sur la stratégie de cybersécurité de l'Union organisé le 9 juin 2021, Raphaël Glucksmann, eurodéputé français (S&D) a critiqué la Chine dans le contexte des cyberattaques : « *Chers collègues, nous ne sommes pas attaqués par des hackers isolés, mais par des régimes autoritaires hostiles (…) Jusqu'ici, le coût imposé aux régimes russes ou chinois pour leurs attaques est risible. (…) Pour être dissuasif, il ne faut pas simplement sanctionner les hackers, il faut sanctionner les États qui sont derrière les hackers.* » [142].

Il est remarquable que les groupes politiques principaux du Parlement, PPE et S&D ont publiquement critiqué Huawei et Pékin et ont souligné la nécessité de prendre une « réponse européenne » pour la sécurisation des réseaux des télécommunication de l'Union alors que la Commission et le Conseil de l'Union ont évité la dénonciation de Huawei ou même de la Chine.

2.2.4 Réponses divisées entre les États membres

Les entreprises européennes comme Audi, BMW, Daimler, Ericsson, Intel, Nokia Huawei ont créé l' « Association automobile 5G » (5G Automotive Association) avec Huawei en septembre 2016[143]. En outre son chiffre d'affaires en Europe, Moyen Orient et Afrique a continué d'augmenter de 2016 à 2019 ainsi qu'en Chine, 156.509 million

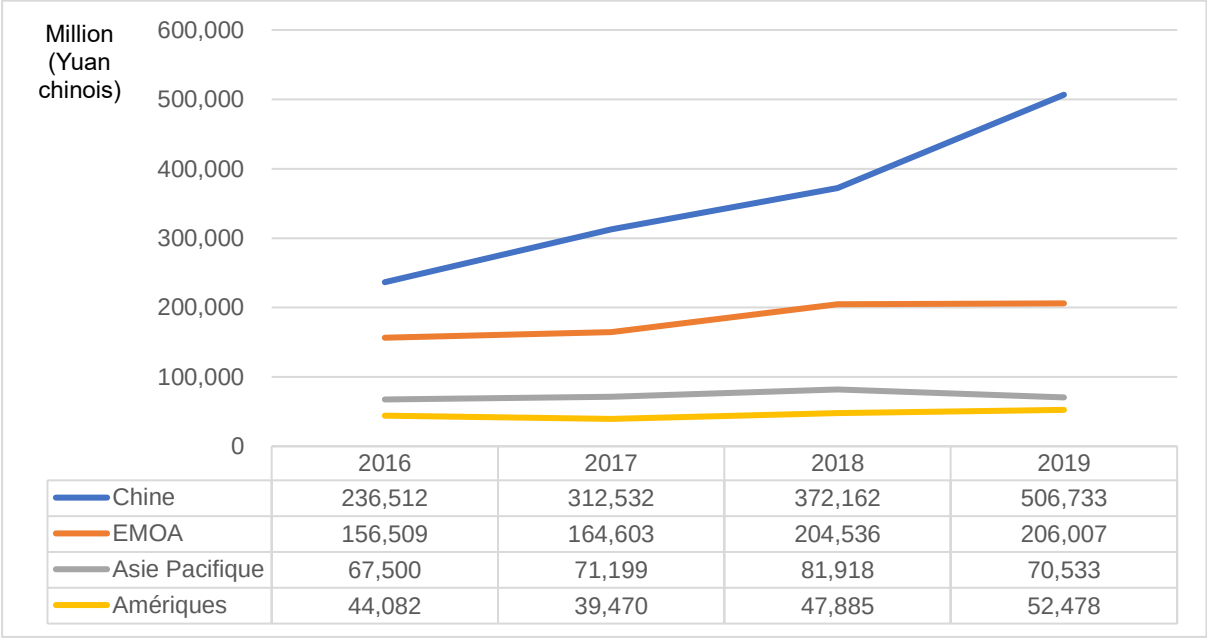
[141] « *I agree that this is an important piece of legislation, which addresses some of the concerns currently related to investments coming to sensitive sectors in Europe. These concerns exist, various Member States face (...) if we had this regulation in place today, we could have come up with a more coordinated approach to some of the Chinese companies, Huawei for instance.* »

[142] Parlement européen, 2021

[143] Huawei Investment & Holding Co., Ltd., 2016

yuans en 2016, 163.854 million yuans (4,7% plus que l'année précédente) en 2017, 204.536 million yuans (24,3%) en 2018 et 206,007 million yuans (0,7%) en 2019 comme indiqué dans le Graphique 3 alors que celui aux Amériques et en Asie-Pacifique stagne pendant ces quatre ans.

Graphique 3 : Répartition géographique des chiffres d'affaires de Huawei de 2016 à 2019



	2016	2017	2018	2019
Chine	236,512	312,532	372,162	506,733
EMOA	156,509	164,603	204,536	206,007
Asie Pacifique	67,500	71,199	81,918	70,533
Amériques	44,082	39,470	47,885	52,478

(Source : Annual Report de Huawei de 2016 à 2019)

2.2.4.1 États membres en coopération avec Huawei

La coopération sino-hongroise est très étroite et Huawei continue ses affaires actives en Hongrie. Huawei y a construit son centre d'approvisionnement en Europe en 2009[144]. Huawei est admis en tant que « Authorized Economic Operater » en Hongrie depuis 2017[145]. Vodafone Hungary, en partenariat avec Huawei, a lancé le

[144] Reuters, 2011
[145] Huawei Investment & Holding Co., Ltd., 2017

premier réseau commercial de 5G en Hongrie en octobre 2019[146]. En outre, Vodafone Hungary a commencé avec Huawei le projet ferroviaire intelligent qui utilise les réseaux 5G en octobre 2021[147].

L'Autriche compte également sur Huawei pour lancer les réseaux de 5G[148]. Vienne a précisé dans sa stratégie 5G en 2018 que l'expansion du réseau devait être impulsée par une étroite coopération économique et de recherche avec les pays asiatiques, y compris la Chine.

2.2.4.2 États membres durs contre Huawei - pays scandinave -

Les pays scandinaves et ceux de l'Europe de l'est prennent une position forte[149]. Le 20 octobre 2020, Stockholm a demandé aux opérateurs domestiques d'éliminer les produits de Huawei de leurs réseaux compte tenu des évaluations effectuées par les Armées et le service de sécurité de la Suède[150]. Gao Feng, le porte-parole du ministère du Commerce de la Chine, pendant la conférence de presse au 21 janvier 2021[151] a critiqué Stockholm en disant que les actions suédoises aux fins de sécurité national manquaient de fondement. Puis il a ajouté « *La Chine exhorte la Suède à corriger immédiatement la mauvaise pratique (…) La Chine prendra toutes les mesures nécessaires pour sauvegarder les intérêts légitimes des entreprises chinoises.* »[152]. En outre, Huawei a intenté un procès contre un opérateur suédois après son expulsion des réseaux suèdes. Cependant, de même que la Cour avait admis la légitimité des

[146] Department of Commerce of the United States of America, 2020
[147] Global Times, 2021
[148] Noyan, 2021 (b)
[149] Noyan, 2021
[150] Cerulus, 2020
[151] Ministry of Commerce of China, 2021
[152] « *China urges Sweden to immediately correct the wrong practice (...) China will take any necessary measures to safeguard the legitimate interest of Chinese businesses.* »

actions publiques prises par l'État le 22 juin 2021[153], la Cour administrative d'appel a également soutenu cette décision le 22 juin 2022[154]. Selon la presse suède, Börje Ekholm, PDG d'Ericsson, entreprise des télécommunications suédoise, a exercé une pression sur Anna Hallberg, ministre du Commerce de Stockholm, afin de faire lever la restriction[155]. En juin 2020, Trine Bramsen, le ministre de la Défense danois a annoncé que Copenhague expulserait Huawei de facto, en disant « *Afin de protéger le Danemark et les Danois, nous voulons collaborer avec quelqu'un avec qui nous avons déjà des alliances* » [156] [157].

2.2.4.3 États membres durs contre Huawei – Europe de l'est -

Comme Jiří Pospíšil l'avait dit au sein du Parlement, la Tchéquie avait interdit aux fonctionnaires de l'État d'utiliser des portables de Huawei dès décembre 2018[158]. Prague a également signé la déclaration conjointe avec les États-Unis sur la coopération des réseaux des télécommunication, qui conduira la Tchéquie à expulser effectivement Huawei de ses réseaux[159]. Washington a signé des accords similaires avec d'autres pays de l'Europe de l'est : la Roumanie le 20 août 2019[160], la Pologne le 2nd septembre 2019[161], l'Estonie le 1er novembre 2019[162], la Lettonie le 27 février

[153] Ahlander et Mukherjee, 2021
[154] Mukherjee, 2022
[155] Lau, 2021
[156] « *In order to protect Denmark and the Danes, we want to collaborate with someone with whom we already have alliances* »
[157] Reuters, 2020 (b)
[158] Kenety, 2018
[159] Reuters, 2020
[160] Presidency of Romania, 2019
[161] Charlish et Goclowski, 2019
[162] U.S. Embassy in Estonia, 2019

2020[163], la Slovène le 13 août 2020[164], la Lituanie en septembre 2020[165], la Bulgarie[166] et le Slovaquie[167] le 23 octobre 2020. En Roumanie, Président Klaus Iohannis a signé une loi conformément à la déclaration conjointe avec les États-Unis afin d'interdire Huawei de participer au développement des réseaux 5G dans ce territoire le 11 juin 2021[168].

En résultat, les États membres de l'Europe de l'est et baltiques sauf la Hongrie et la Croatie, sont en train d'élaborer la sécurité de leurs réseaux des télécommunications[169]. Cependant, il faut noter que ce sont les États-Unis qui ont réalisé les efforts de signer les déclarations conjointes ou les mémorandums de coopération avec ces pays particulièrement vulnérables face aux menaces numériques. En outre, il faut souligner que ceux qui ont signé l'accord avec Washington sont également des États membre de l'OTAN. Cela s'explique par l'inquiétude des États-Unis en ce qui concerne les réseaux militaires des États membres ; c'est ce qui a motivé Washington pour prendre des actions de grande ampleur avec les États d'Europe de l'est. Karol Okonski, ministre des Affaires numériques de la Pologne a ainsi répondu aux questions du journal The Washington Post: « *This is the cost that either the telecom operators have to cover by themselves or it would have to be covered by the state* » « *In the latter case, we as Poland are not able to afford it.* »[170]. L'Union a essayé de sécuriser les réseaux mais au contraire le résultat montre l'incapacité de l'Union à prendre les mesures.

[163] Department of State of the United States of America, 2020 (a)
[164] Republic of Slovenia, 2020
[165] Department of State of the United States of America, 2020 (b)
[166] *Ibid.*, 2020 (c)
[167] *Ibid.*, 2020 (d)
[168] Reuters, 2021
[169] Seferiadis, 2020
[170] Nakashima, 2019

2.2.4.4 Autres États membres

En France, le Président Macron a signé « la 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 », qui renforce le contrôle de sécurité des réseaux de télécommunication par l'État. Alors que SFR et Bouygues Telecom ont attaqué l'État sur cette législation, particulièrement « le décret n° 2019-1300 du 6 décembre 2019 relatif aux modalités de l'autorisation préalable de l'exploitation des équipements de réseaux radioélectriques prévue à l'article L. 34-11 du code des postes et des communications électroniques » et « l'arrêté du 6 décembre 2019 fixant la liste des appareils prévue par l'article L. 34-11 du code des postes et

des communications électroniques »[171]. Le Conseil constitutionnel[172] et le Conseil d'État[173] ont rejeté les requêtes des entreprises françaises.

L'Allemagne n'expulse pas explicitement mais, le 23 avril 2021, le Bundestag a adopté une loi « IT Security Law 2.0 » qui limite le recours aux fournisseurs peu fiables et demande aux opérateurs des réseaux des télécommunications de notifier à l'État quand ils signent un contrat pour des composants centraux des réseaux 5G[174]. Cette

[171] Article L34-11 du code des postes et des communications électroniques
I.-Est soumise à une autorisation du Premier ministre, dans le but de préserver les intérêts de la défense et de la sécurité nationale, l'exploitation sur le territoire national des appareils, à savoir tous dispositifs matériels ou logiciels, permettant de connecter les terminaux des utilisateurs finaux au réseau radioélectrique mobile, à l'exception des réseaux de quatrième génération et des générations antérieures, qui, par leurs fonctions, présentent un risque pour la permanence, l'intégrité, la sécurité, la disponibilité du réseau, ou pour la confidentialité des messages transmis et des informations liées aux communications, à l'exclusion des appareils installés chez les utilisateurs finaux ou dédiés exclusivement à un réseau indépendant, des appareils électroniques passifs ou non configurables et des dispositifs matériels informatiques non spécialisés incorporés aux appareils.
L'autorisation mentionnée au premier alinéa du présent I n'est requise que pour l'exploitation, directe ou par l'intermédiaire de tiers fournisseurs, d'appareils par les opérateurs mentionnés à l'article L. 1332-1 du code de la défense, ainsi désignés en vertu de leur activité d'exploitant d'un réseau de communications électroniques ouvert au public.
La liste des appareils dont l'exploitation est soumise à l'autorisation mentionnée au premier alinéa du présent I est fixée par arrêté du Premier ministre, pris après avis de l'Autorité de régulation des communications électroniques et des postes. Cette liste énumère les différents appareils concernés en référence à la terminologie utilisée dans les standards internationaux associés aux réseaux radioélectriques mobiles de cinquième génération et des générations ultérieures.

(…)

NOTA : Conformément à l'article 3 de de la loi n° 2019-810 du 1er août 2019 : Le présent article est applicable à l'exploitation des appareils mentionnés au I de l'article L. 34-11 du code des postes et des communications électroniques installés depuis le 1er février 2019.
Les opérateurs qui, à la date de publication de la présente loi, exploitent des appareils soumis à autorisation en vertu du même article L. 34-11 disposent d'un délai de deux mois pour déposer la demande d'autorisation préalable prévue audit article L. 34-11. Ce délai court à compter de la date de publication la plus tardive de l'arrêté mentionné au I ou du décret mentionné au II du même article L. 34-11, et au plus tard à compter de la fin du deuxième mois suivant la publication de la présente loi.
[172] Décision n° 2020-882 QPC du 5 février 2021
[173] Conseil d'État, 2ème - 7ème chambres réunies, 08/04/2021, n° 442120
[174] Cerulus, 2021

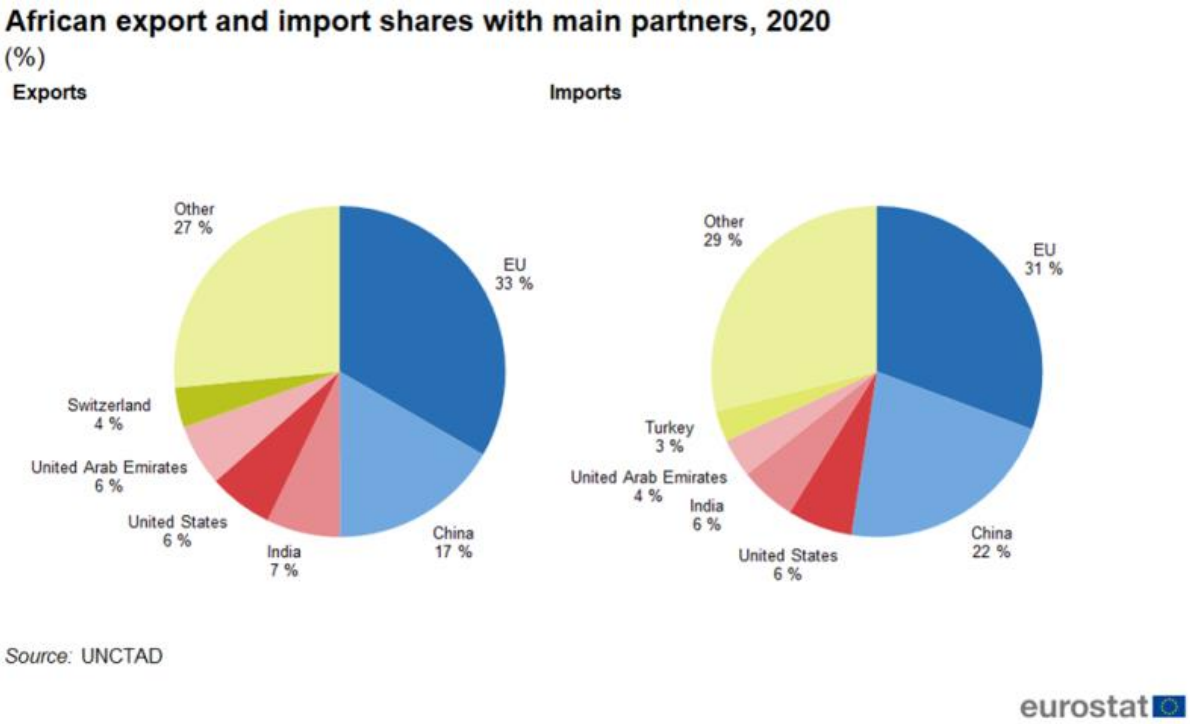
législation est néanmoins tardive, comparée à celles d'autres États membres notamment la France (2019) et la Suède (2020).

2.3 Actions publique de l'Union en Afrique

Pour l'Afrique, l'Union européenne est le plus grand donateur dans l'aide au développement et un partenaire économique de première importance dans le monde. Selon l'OCDE, en 2020, la proportion de l'APD bilatérale des institutions européennes vers l'Afrique représente 40,9% c'est à dire la plus grande partie de l'APD bilatérale des institutions européennes (cf. : celle de l'Europe est à 23,6%.)[175]. En outre, selon Eurostat, l'Union européenne représente 33% du montant total des exportations africaines et 31% de celui des importations africaines (cf. Graphique 3).

[175] Organisation de Coopération et de développement économiques, 2022

Graphique 4 : Proportion de l'export et de l'import de l'Afrique avec ses partenaires principaux en 2020[176]



La relation étroite des deux continents accentue le besoin de garanties quant à la circulation de données sécurisées et la fuite des données depuis des réseaux africains particulièrement vulnérables.

Du même que l'Union européenne face l'enjeu des réseaux 5G, l'Afrique n'a pas pris de mesures ciblant spécifiquement Huawei ou les entreprises des TIC chinoises. Cependant, en partenariat avec les États-Unis, l'Union européenne s'engage dans la sécurisation des réseaux des télécommunications en Afrique.

2.3.1 Politiques de l'Union en Afrique en matière numérique

Alors que l'Union dispose des dispositifs politiques comme celle des partenariats

[176] Eurostat, 2022

internationaux et celle de voisinage et des enveloppes qui les soutiennent, notamment le Fonds européen de Développement pouvant influencer les pays africains, Bruxelles n'a pas mis la pression sur les autres pays pour faire expulser Huawei de leurs réseaux des télécommunications.

Cependant, l'Union européenne a eu l'occasion de souligner l'importance de la sécurité des réseaux en Afrique aussi.

2.3.1.1 Sommets UE-Afrique de 2000 à 2010

Bruxelles organise régulièrement une réunion avec l'ensemble des pays africains (le Sommet UE-Afrique (UA)). Dans la « Stratégie commune Afrique-UE »[177] adoptée lors du deuxième Sommet UE-Afrique à Lisbonne en décembre 2007, les deux parties mentionnent l'importance du numérique : « *L'Afrique et l'UE renforceront leur coopération et leur assistance pour combler la fracture numérique et favoriser l'émergence d'une économie de la connaissance ouverte à tous (…)* » [178]. Cependant le centre d'intérêt en matière de TIC de cette stratégie est la réduction de la fracture numérique plutôt que la sécurité des réseaux des télécommunications. C'est la même orientation que l'on retrouve dans le deuxième « Plan d'action 2011-2013 »[179] adopté lors du troisième Sommet UE-Afrique à Tripoli en novembre 2010.

2.3.1.2 Montée de cybersécurité - Sommets UE-Afrique 2013 et 2017

Le mot de la cybersécurité apparaît pour la première fois dans la Feuille de Route 2014-2017 [180] adoptée lors du quatrième Sommet à Bruxelles en avril 2014 : « *a) l'harmonisation et l'alignement des aspects concernés des politiques et des cadres réglementaires africains et européens en matière de communications électroniques, y*

[177] Conseil de l'Union européenne, 2007
[178] Paragraphe 85. de la Stratégie commune Afrique-UE en 2007
[179] Conseil de l'Union européenne, 2011
[180] *Ibid.*, 2014

compris la cyber sécurité. »[181].

De fait, c'est en février 2013 que la Commission a publié la première stratégie de cybersécurité de l'Union : « *Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé* »[182], présentée par la Haute représentante de l'Union pour les affaires étrangères et la politique de sécurité. Ensuite la Commission a proposé la Directive (UE) 2016/1148 au Conseil de l'Union et au Parlement [183]. Il est probable que l'idée de la cybersécurité a été également prospéré dans la feuille de route après la montée des enjeux de cybersécurité au sein de l'Union.

La Déclaration[184] adoptée lors du cinquième Sommet à Abidjan en novembre 2017 mentionne également la cybersécurité : « *Nous saisirons les opportunités qu'offrent l'évolution technologique et l'économie numérique, en continuant notamment à collaborer dans les domaines concernant les cadres juridiques et réglementaires mesurables en matière de TIC, y compris la cybersécurité et la biométrie, en appuyant les investissements dans les infrastructures numériques, et l'intégration du numérique (…)* »[185]. Le contexte est le même que celui de la Feuille de route 2014-2017.

2.3.1.3 Vers une coopération plus poussée : Sommet en 2022

L'on peut constater l'évolution de l'idée de la cybersécurité ou de la sécurité des réseaux au sixième Sommet à Bruxelles.

Dans les précédents documents adoptés, la « cybersécurité » apparaît dans le contexte de la coopération pour élaborer les cadres juridiques mais l'emploi de ce mot

[181] Paragraphe 50. de la Feuille de Route 2014-2017
[182] Commission européenne et Haute représentante de l'Union pour les affaires étrangères et la politique de sécurité, 2013
[183] Commission européenne, 2013 (b)
[184] Conseil de l'Union européenne, 2017
[185] Paragraphe 63. de la Déclaration du Sommet en 2017

évolue dans la déclaration du Sommet[186] : « ***Une coopération renouvelée et renforcée pour la paix et la sécurité.*** *(…) Nos deux continents entretiennent une coopération de longue date dont le principe fondateur est la recherche de solutions africaines aux problèmes africains, (…), conçu pour lutter contre l'instabilité, la radicalisation, l'extrémisme violent et le terrorisme, (…) Nous exprimons notre détermination à approfondir notre coopération en fournissant un soutien en faveur de formations, d'un renforcement des capacités et d'équipements adéquats, afin de renforcer et d'intensifier les opérations de paix autonomes menées par les forces de défense et de sécurité africaines, (…) Nous intensifierons notre coopération en matière de sécurité, y compris dans le domaine de la cybersécurité. (…)* ».

Dans ce document, les deux parties n'emploient pas le mot pour désigner simplement la sécurité des réseaux mais cet objectif est exprimé dans un autre paragraphe sur la stratégie « Global Gateway », paquet d'investissement de 150 milliards d'euros pour l'Afrique. Le paragraphe 4 explique le contenu et la priorité de la stratégie : « *Le paquet encouragera les investissements durables à grande échelle, avec le soutien des initiatives de l'Équipe Europe, en tenant dûment compte des priorités et des besoins des pays africains, y compris : i) des investissements dans (…) les infrastructures numériques (…) iv) la transformation numérique au service d'une connectivité de confiance par des investissements dans les infrastructures (…)* ». Pour réaliser une « connectivité de confiance » comme c'est écrit, il est nécessaire de disposer de réseaux sécurisés. Il se peut que cette expression reflète une intention de l'Union européenne plus continuée et plus concrète qu'auparavant.

L'un des six piliers d'« *UE-Afrique : paquet d'investissement « Global Gateway »* » est « la transition numérique ». L'Union met en avant le projet de la construction

[186] Conseil de l'Union européenne, 2022

« L'EurAfrica Gateway Cable » (câble à fibres optiques sous-marin international connectant l'UE à l'Afrique) et l'amélioration de la connectivité numérique par le programme européen de communications par satellite sécurisées[187]. Ces projets permettront la sécurité des réseaux des télécommunications entre l'Union et l'Afrique.

2.3.2 L'Afrique du nord

L'Union européenne met en œuvre les politiques de voisinage pour la transition numérique dans les pays de l'Afrique du nord (Algérie, Égypte, Libye, Maroc, Mauritanie et Tunisie). La Commission reconnaît l'importance du numérique dans le cadre des politiques de voisinage[188].

Au sein de cette région, l'Union travaille étroitement avec l'Union pour la Méditerranée (UpM) en plus de l'UA. En septembre 2014, l'Union européenne a coprésidé avec la Jordanie la Réunion ministérielle de l'UpM sur l'économie numérique à Bruxelles[189].

En outre, la Commission a publié les termes d'« *Un partenariat renouvelé avec le voisinage méridional* » [190] qui précise les priorités politiques. On peut observer, en matière numérique, que ce partenariat conduit à un projet avec le Maroc : « *Dans le cadre du partenariat numérique UE-Maroc, l'UE aidera le Maroc à devenir membre associé du programme de recherche Horizon Europe. Parallèlement au financement par l'UE des infrastructures numériques et au renforcement de leur fiabilité, de leurs capacités et de leur sécurité, l'UE soutiendra l'écosystème*

[187] Commission européenne, 2022
[188] Commission européenne, 2020 (a)
[189] Union pour la Méditerranée, 2014
[190] Commission européenne et Haut représentant de l'Union pour les affaires étrangères et la politique de sécurité, 2021

numérique/d'innovation. »[191].

2.3.3 Coopération avec Washington

En coopération avec les États-Unis, l'Union est en train d'élaborer un dispositif financier aux pays tiers pour la sécurisation des réseaux des télécommunications.

Le débat a été lancé par le « Conseil du Commerce et de la Technologie (CCT) entre l'Union européenne et les États-Unis » (The EU-US Trade and Technology Council (TTC)) co-présidé par Margrethe Vestager, Vice-présidente exécutifs de la Commission chargée d'« Une Europe adaptée à l'ère du numérique », Valdis Dombrovskis, Vice-président exécutif de la Commission chargé d'« Une économie au service des personnes », Antony Blinken, Secrétaire d'État, Gina Raimondo, Secrétaire du Commerce et Katherine Tai, Représentante au Commerce des États-Unis, qui a originellement pour l'objectif de résoudre les disputes dans les domaines politiques entre l'Union et les États-Unis[192]. Le premier CCT a eu lieu à Pittsburgh (États-Unis) le 29 septembre 2021 aboutissant à une « Communication conjointe inaugurale du Conseil du Commerce et de la Technologie entre l'Union européenne et les États-Unis » [193], dans laquelle les partenaires ont exprimé leur intention de « *promouvoir une connectivité numérique internationale sûre et durable* »[194] [195] et créé un Groupe de travail 4 (Group de travail pour la technologie et le service de l'information et des télécommunication) dont la mission est d'« *œuvrer pour assurer la sécurité, la diversité, l'interopérabilité et la résilience tout au long de la chaîne*

[191] Commission européenne. 2021
[192] Stupp, 2022
[193] European Commission, 2021
[194] Paragraphe 3., Section 1. de « EU-US Trade and Technology Council Inaugural Joint Statement »
[195] « *promote secure and sustainable international digital connectivity* »

d'approvisionnement des TIC, y compris les domaines sensibles et critiques tels que la 5G, les câbles sous-marins, les centres de données et l'infrastructure cloud »[196], « *explorer une coopération concrète en matière de financement du développement pour une connectivité numérique sécurisée et résiliente dans les pays tiers* »[197] et « *chercher à renforcer la coopération en matière de recherche et d'innovation pour les systèmes au-delà de la 5G et de la 6G* »[198].

Après des consultations entre les deux réunions, la deuxième CCT s'est tenu à Paris-Saclay le 16 mai 2022. Thierry Breton, Commissaire au Marché intérieur, y a participé. Les partenaire ont également publié une communication conjointe[199], dans laquelle ils se sont félicités du «*lancement d'un groupe de travail dédié au financement public des chaînes d'approvisionnement sécurisées et résilientes en matière de connectivité et de TSIC (Technologie et service de l'information et de la communication) dans les pays tiers.* »[200] [201] en tant que progrès réalisé après le premier CCT. Cette équipe d'étude et d'action, lancée par le Groupe de travail 4 inauguré par la première communication conjointe, « *a pour objectif de promouvoir l'utilisation de fournisseurs de confiance / du risque non-élevé, de partager des informations sur nos efforts respectifs pour soutenir des projets ICTS sûr, résilient et respectueux des droits dans les pays tiers, et de collaborer au financement public conjoint des États-Unis et de l'UE*

[196] « *to work towards ensuring security, diversity, interoperability and resilience across the ICT supply chain, including sensitive and critical areas such as 5G, undersea cables, data centres, and cloud infrastructure* »
[197] « *to explore concrete cooperation on development finance for secure and resilient digital connectivity in third countries* »
[198] « *to seek to reinforce cooperation on research and innovation for beyond 5G and 6G systems* »
[199] Department of Commerce of the United States of America, 2022
[200] Paragraphe v., Section 19. de « U.S.-EU Joint Statement of the Trade and Technology Council 16 May 2022 »
[201] « *The launch of a dedicated taskforce on public financing for secure and resilient connectivity and ICTS supply chains in third countries* »

de projets TSIC dans des pays tiers basés sur des principes généraux communs.»[202] et «*déterminera également comment des partenaires et des institutions financières internationales partageant les mêmes idées, y compris au niveau des États membres, le cas échéant, peuvent renforcer notre capacité à fournir le financement dont nos partenaires ont besoin pour améliorer leur infrastructure ICTS et fournir des services numériques sûrs et fiables à leurs citoyens.* » [203]. Selon l'article de *Wall Street Journal*[204], les pays d'Afrique et d' Amérique latine sont probablement ceux qui sont désignés comme pays tiers à soutenir. Les projets initiaux seront mis en œuvre jusqu'à la fin de l'année 2022. En outre, les agents de l'Union européenne et des États-Unis impliqués dans le CCT pensent que les entreprises des réseaux des télécommunications chinoises, notamment Huawei, peuvent menacer la sécurité des données. Il est très probable que les mots « *fournisseurs du risque élevé* » (*high-risk suppliers*) dans la communication désignent les équipementiers chinois. En outre, cette équipe d'étude et d'action est censé soutenir les initiatives amirales d'infrastructure de l'Union et des États-Unis pour « *impulser et prioriser les projets d'infrastructure ICTS de haute qualité qui promeuvent les principes généraux suivants : a. Soutenir un Internet ouvert, interopérable, sécurisé et fiable, b. S'abstenir de financer des achats auprès de fournisseurs non fiables / du risque élevé, (…) h. Utiliser des politiques et des cadres de cybersécurité solides.* » [205].

---

[202] « *has the objective to promote the use of trusted/non-high-risk suppliers, share information on our respective efforts to support secure, resilient, and rights-respecting ICTS projects in third countries, and collaborate on joint U.S.-EU public financing of ICTS projects in third-countries based on common overarching principles* »

[203] « *will also determine how like-minded partners and international financial institutions, including at the Member State level as appropriate, can strengthen our ability to provide the financing that our partners need to improve their ICTS infrastructure and provide secure, trusted digital services to their citizens.* »

[204] Stupp, 2022

[205] « *advance and prioritize high-quality ICTS infrastructure projects that promote the following overarching principles: a. Support an open, interoperable, secure, and reliable*

Le Groupe de travail 4 a souligné dans sa propre communication[206] « *l'importance de traiter les risques de sécurité des fournisseurs du risque élevé et de favoriser la sécurité, la diversité et l'interopérabilité* » [207]. La communication mentionne « *EU's 5G Cybersecurity Toolbox* » et « *the U.S. Secure and Trusted Communications Networks Act of 2019* » en tant que signe de la compréhension commune entre l'Union et les États-Unis, qui peut se traduire la position de Bruxelles alignée avec Washington pour la sécurisation des réseaux en Afrique.

CONCLUSION

Créé en 1987, Huawei a développé ses activités en Europe et Afrique à partir des années 2000s. Cependant, les soupçons de vols de propriétés intellectuelles et d'espionnages ainsi que le caractère « privé-étatique » de cette entreprise étroitement liée à l'État chinois suscitent des inquiétudes quant à son influence sur la sécurité des réseaux des télécommunications dans le monde, en particulier dans les pays occidentaux. L'introduction des réseaux 5G a intensifié ces inquiétudes compte tenu de l'ampleur des influences que cette technologie de pointe, avec les objets connectés, peut avoir sur la société notamment en ce qui concerne la sécurité nationale.

L'Union européenne a essayé de prendre des mesures spécifiques aux TIC chinoises à l'époque du Commissaire Karel De Gucht a fait. En outre, elle a promulgué une directive pour renforcer le niveau de sécurité des outils numériques utilisés dans les États membres. Mais, l'Union européenne n'a pas réussi à prendre des initiatives

Internet, b. Refrain from financing purchases from untrusted/high-risk suppliers, (…) h. Use sound cybersecurity policies and frameworks. »

[206] Trade and Technology Council Statement on the Importance of Security, Diversity, Interoperability, and Resilience for Information and Communications Technology and Services (Annexe iv de « U.S.-EU Joint Statement of the Trade and Technology Council 16 May 2022 »)

[207] « *the importance of addressing security risks from high-risk suppliers and fostering security, diversity, interoperability* »

fortes pour lutter contre les géants des télécommunications chinois, ni à initier une politique commune de « cybersécurité » pour l'Union. Les divisions politiques internes et les dépendances économiques à l'égard de la Chine et de ses producteurs, ont entraîné des réponses divergentes face l'enjeu de Huawei de la part de États membres. C'est surtout Washington qui a exercé la puissance normative et technologique la plus forte notamment à destination des pays de l'Europe centrale et orientale via ses engagements diplomatiques.

Parallèlement, l'Union n'a pas pris d'action publique en Afrique pour empêcher la pénétration des TIC chinoises sur ce continent, mais, depuis quelques années, l'Union renforce la coopération avec les pays africains pour diminuer la vulnérabilité de leurs réseaux de télécommunications à travers son propre projet stratégique d'investissement en Afrique comme l'on peut constater dans le Sommet UE-UA en 2022. En outre, Bruxelles s'engage pour la sécurisation des réseaux de télécommunications dans les pays tiers en coopération avec Washington, qui pourrait apporter une influence importante sur champ de bataille.

ANNEXE

Bibliographie

Littérature scientifique

BOULLIER Dominique, *Sociologie du numérique*, Armand Colin, 2016.

CARAMANI Daniele (dir.), *Comparative politics*, New York, Oxford University Press, 2011.

FUERTES Mercedez, *European Digital Sovreignty*, Espagne, Eolas ediciones, 2021.

LE GOURIELLEC Sonia, *Géopolitique de l'Afrique*, Que sais-je ?, 2022.

MEUNIER Patrick, « Les compétences de l'Union européenne et la souveraineté numérique », in TÜRK Pauline et VALLAR Christian (dir.), *La souveraineté numérique : le concept et les enjeux*, mare et martin, 2017, pp. 197 - 218.

ZOA ATEBA Yves Barthélémy, « Huawei et ZTE : expansion de deux grands opérateurs chinois des télécommunications au Cameroun », in MBABIA Olivier et WASSOUNI François (dir.), *La présence chinoise en Afrique francophone*, Monde Global éditions nouvelles, 2016, pp. 56 – 71.

Sources journalistiques

AHLANDER Johan et MUKHERJEE Supantha, « Swedish court upholds ban on Huawei selling 5G network gear », *Reuters*, 2021, Disponible sur https://www.reuters.com/technology/swedish-court-upholds-ban-huawei-selling-5g-network-gear-2021-06-22/, consulté le 6/8/2022.

BARBOZA David, APPELBAUM Binyamin et MARKOFF John, «Scrutiny For Chinese Telecom Bid », *The New York Times*, 2010, Disponible sur https://www.nytimes.com/2010/08/23/business/global/23telecom.html, consulté le 6/8/2022.

BBC, «Huawei and ZTE handed 5G network ban in Australia », *BBC*, 2018, Disponible sur https://www.bbc.com/news/technology-45281495, consulté le 6/8/2022.

BERKOW Jameson, « Nortel hacked to pieces », *Financial Post*, 2012, Disponible sur https://financialpost.com/technology/nortel-hacked-to-pieces, consulté le 7/9/2022.

BILBY Ethan, « EU report urges action against Chinese telecom firms », *Reuters*, 2012, Disponible sur https://www.reuters.com/article/eu-china-telecoms-idCNL5E8NBAB220121212, consulté le 17/6/2022.

BLENKINSOP Philip, « EU resistant to China telecoms trade case : Sweden », *Reuters*, 2013, Disponible sur https://www.reuters.com/article/us-eu-trade-china-idUSBRE93H11Q20130418, consulté le 17/6/2022.

CBC News, « Nortel collapse linked to Chinese hackers », *CBC News*, 2012. Disponible sur https://www.cbc.ca/news/business/nortel-collapse-linked-to-chinese-hackers-1.1260591, consulté le 4/9/2022.

CBS, « Huawei founder says he would defy Chinese law on intelligence gathering », *CBS*, 2019. Disponible sur https://www.cbsnews.com/news/huawei-president-ren-zhengfei-says-he-would-defy-chinese-law-on-intelligence-gathering/, consulté le 13/6/2022.

CERULUS Laurens, « Sweden bans Huawei, ZTE equipment from key parts of 5G network », *Politico*, 2020, Disponible sur https://www.politico.eu/article/sweden-bans-huawei-zte-from-key-5g-parts/, consulté le 6/8/2022.

CERULUS Laurens, « Germany falls in line with EU on Huawei », *Politico*, 2021, Disponible sur https://www.politico.eu/article/germany-europe-huawei-5g-data-privacy-cybersecurity/, consulté le 6/8/2022.

CHAFFIN Joshua, « China's premier Li Keqiang warns Europe over trade war », *Financial Times*, 2013

(a), Disponible sur https://www.ft.com/content/7f9f608e-c5f2-11e2-99d1-00144feab7de, consulté le 6/8/2022.

CHAFFIN Joshua, « Karel De Gucht: Frustrated and outflanked », *Financial Times*, 2013 (b), Disponible sur https://www.ft.com/content/aa79490a-f8f6-11e2-86e1-00144feabdc0, consulté le 6/8/2022.

CHANG Christine, CHENG Amy, KIM Susan, KUHN-OSIUS Johanna, REYES Jesús et TURGEL Daniel, «Huawei Technologies: A Chinese Trail Blazer in Africa», *Knowledge at Wharton*, 2009, Disponible sur https://knowledge.wharton.upenn.edu/article/huawei-technologies-a-chinese-trail-blazer-in-africa/, consulté le 6/9/2022.

CHARLISH Alan et GOCLOWSKI Marcin, « U.S. and Poland urge tougher checks on foreign influence over 5G networks », *Reuters*, 2019, Disponible sur https://www.reuters.com/article/us-poland-usa-5g-idUSKCN1VN174, consulté le 6/8/2022.

CORDOUE Elian, «Huawei va fournir le réseau 3G de Vodafone en Tchéquie», *Le Monde Informatique*, 2006, Disponible sur https://www.lemondeinformatique.fr/actualites/lire-huawei-va-fournir-le-reseau-3g-de-vodafone-en-tchequie-19099.html, consulté le 6/9/2022.

DONNAN Shawn et OLIVER Christian, « EU commissioner attacks China's telecoms subsidies », *Financial Times*, 2014, Disponible sur https://www.ft.com/content/d6d0bcc6-b5cb-11e3-b40e-00144feabdc0, consulté le 6/8/2022.

DUMOULIN Sébastien, « Le monde fabuleux de la 5G », *Les Échos*, 2019, Disponible sur https://www.lesechos.fr/weekend/business-story/le-monde-fabuleux-de-la-5g-1211757, consulté le 12/9/2022.

EHL David, « Africa embraces Huawei technology despite security concerns », *Deutsche Welle*, 2022, Disponible sur https://www.dw.com/en/africa-embraces-huawei-technology-despite-security-concerns/a-60665700, consulté le 6/8/2022.

Financial Times, « Boldness in Business 2009 », *Financial Times*, 2009, Disponible sur https://www.ft.com/content/2955ced8-226d-11df-a93d-00144feab49a, consulté le 6/8/2022.

FLEMING Jeremy, « De Gucht juggles politics, diplomacy in high-stakes China gambit », *Euractive*, 2013, Disponible sur https://www.euractiv.com/section/digital/news/de-gucht-juggles-politics-diplomacy-in-high-stakes-china-gambit/?_ga=2.95104095.236320884.1660040244-387510964.1660040243, consulté le 6/8/2022.

FLYNN Laurie, «Technology Briefing Hardware: Cisco Drops Patent Infringement Suit », *The New York Times*, 2004, Disponible sur https://www.nytimes.com/2004/07/29/business/technology-briefing-hardware-cisco-drops-patent-infringement-suit.html, consulté le 6/8/2022.

GARDNER Andrew, « China investigating EU wine », *Politico*, 2013, Disponible sur https://www.politico.eu/article/china-investigating-eu-wine/, consulté le 6/8/2022.

GARSIDE Juliette, « Huawei's relationship with BT under investigation by MPs », *The Gardian*, 2012, Disponible sur https://www.theguardian.com/technology/2012/oct/10/huawei-international-blacklisting, consulté le 6/9/2022.

Global Times, « Hungary to build Europe's first 5G smart railway port together with Huawei », *Global Times*, 2021, Disponible sur https://www.globaltimes.cn/page/202110/1235745.shtml, consulté le 6/8/2022.

GORMAN Siobhan, « Chinese Hackers Suspected In Long-Term Nortel Breach », *Wall Street Journal*, 2012, Disponible sur https://www.wsj.com/articles/SB10001424052970203363504577187502201577054, consulté le 6/9/2022.

HARNEY Alexandra, « Huawei wins 3G contract from Telfort », *Financial Times*, 2004. Disponible sur https://www.ft.com/content/7b42f14e-4a0a-11d9-b065-00000e2511c8, consulté le 13/6/2022.

HENNI Jamal, «Le chinois Huawei veut doubler ses ventes en Europe», *Les Échos*, 2014. Disponible sur https://www.lesechos.fr/2006/07/le-chinois-huawei-veut-doubler-ses-ventes-en-europe-575710, consulté le 7/9/2022.

HONORÉ Renaud, « Télécoms : l'Europe et la Chine font la paix », *Les Échos*, 2014. Disponible sur

https://www.lesechos.fr/2014/10/telecoms-leurope-et-la-chine-font-la-paix-312162, consulté le 7/8/2022.

IDEISHI Tadashi, «Denshi seifu senshinkoku Kankoku no torikumi » (Iniatives prises par la République de la Corée, pays développé en matièere d'e-gouvernement), *NHK*, 2020. Disponible sur https://www.nhk.or.jp/kaisetsu-blog/900/437077.html, consulté le 7/8/2022.

KADIRI Ghalia et TILOUINE Joan, « À Addis-Abeba, le siège de l'Union africaine espionné par Pékin », *Le Monde*, 2018. Disponible sur https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html, consulté le 7/8/2022.

KENETY Brian, « Czech PM bans use of Huawei mobile phones by Government Office », *Radio Prague*, 2018. Disponible sur https://english.radio.cz/czech-pm-bans-use-huawei-mobile-phones-government-office-8143076, consulté le 7/8/2022.

KHARPAL Arjun, « Huawei says it would never hand data to China's government. Experts say it wouldn't have a choice », *CNBC*, 2019. Disponible sur https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html, consulté le 13/6/2022.

KRACH Keith, «The free world must unite against Huawei », The Daily Telegraph, 2020. Disponible sur https://www.telegraph.co.uk/news/2020/06/25/free-world-must-unite-against-huawei/, consulté le 13/9/2022.

LAU Stuart, « Sweden faces Chinese blowback over Huawei ban », *Politico*, 2021. Disponible sur https://www.politico.eu/article/sweden-faces-chinese-blowback-over-huawei-ban/, consulté le 7/8/2022.

LERMAN Rachel, « Jury awards T-Mobile $4.8M in trade-secrets case against Huawei », *The Seattle Times*, 2017. Disponible sur https://www.seattletimes.com/business/technology/july-awards-t-mobile-48m-in-trade-secrets-case-against-huawei/, consulté le 7/8/2022.

LUBLIN, Joann S. et RAICE Shayndi, « Security Fears Kill Chinese Bid in U.S. », *Wall Street Journal*, 2010. Disponible sur https://www.wsj.com/articles/SB10001424052748704353504575596611547810220, consulté le 7/9/2022.

LU-YUEYANG Maggie, « Australia blocks China's Huawei from broadband tender », *Reuters*, 2012. Disponible sur https://www.reuters.com/article/us-australia-huawei-nbn-idUSBRE82P0GA20120326, consulté le 7/8/2022.

MANIÈRE Pierre, « Câbles sous-marins : Huawei jette l'éponge », *La Tribune*, 2019. Disponible sur https://www.latribune.fr/technos-medias/telecoms/cables-sous-marins-huawei-jette-l-eponge-819305.html, consulté le 13/9/2022.

MARCHAND Leïla, « Dans la tourmente, Huawei cède son activité de câbles sous-marins », *Les Échos*, 2019. Disponible sur https://www.lesechos.fr/tech-medias/hightech/dans-la-tourmente-huawei-cede-son-activite-de-cables-sous-marins-1026134, consulté le 13/9/2022.

MEHTA Stephanie, « BT CEO: Huawei is a "good partner" », *Fortune*, 2013. Disponible sur https://fortune.com/2013/10/25/bt-ceo-huawei-is-a-good-partner/, consulté le 13/6/2022.

MUKHERJEE Supantha, « Swedish court upholds ban on Huawei sale of 5G gear », *Reuters*, 2022, Disponible sur https://www.reuters.com/business/media-telecom/swedish-court-upholds-ban-huawei-sale-5g-gear-2022-06-22/, consulté le 6/8/2022.

NAKASHIMA Ellen, « U.S. pushes hard for a ban on Huawei in Europe, but the firm's 5G prices are nearly irresistible », *The Washington Post*, 2019. Disponible sur https://www.washingtonpost.com/world/national-security/for-huawei-the-5g-play-is-in-europe--and-the-us-is-pushing-hard-for-a-ban-there/2019/05/28/582a8ff6-78d4-11e9-b7ae-390de4259661_story.html, consulté le 7/8/2022.

NHK, « Kachū no Huawei sōgyōsha ni semaru » (Approche au fondateur de Huawei en trouble), *NHK*, 2019. Disponible sur https://www3.nhk.or.jp/news/special/45th_president/articles/trade-friction/features/2019-0123-01.html, consulté le 4/7/2022.

NOYAN Oliver, « EU countries keep different approaches to Huawei on 5G rollout », *Euractive*, 2021 (a).

Disponible sur https://www.euractiv.com/section/digital/news/eu-countries-keep-different-approaches-to-huawei-on-5g-rollout/, consulté le 7/8/2022.

NOYAN Oliver, « L'Autriche compte sur Huawei pour le déploiement de son réseau 5G », *Euractive*, 2021 (b). Disponible sur https://www.euractiv.fr/section/avenir-de-lue/news/lautriche-compte-sur-huawei-pour-le-deploiement-de-son-reseau-5g/?_ga=2.97088411.543544825.1660574104-387510964.1660040243, consulté le 7/8/2022.

PALMER Randall, « Former Canadian spy sees Huawei risk as manageable », *Reuters*, 2012. Disponible sur https://www.reuters.com/article/us-usa-china-huawei-canada-idUSBRE8981CB20121010, consulté le 4/7/2022.

PAYTON Laura, « Former Nortel exec warns against working with Huawei », *CBC News*, 2012. Disponible sur https://www.cbc.ca/news/politics/former-nortel-exec-warns-against-working-with-huawei-1.1137006, consulté le 4/9/2022.

Reuters, « 3Com to be acquired by Bain, Huawei for $2 billion: report », *Reuters*, 2007. Disponible sur https://www.reuters.com/article/us-3com-buyout-idUSN2837468820070928, consulté le 7/9/2022.

Reuters, « China's Huawei picks Hungary for logistics centre », *Reuters*, 2011. Disponible sur https://www.reuters.com/article/huawei-hungary-idUSLDE7571T420110608, consulté le 7/8/2022.

Reuters, « Czechs sign joint 5G security declaration with United States », *Reuters*, 2020 (a). Disponible sur https://www.reuters.com/article/us-czech-usa-5g-idUKKBN22I33O, consulté le 7/8/2022.

Reuters, « Denmark wants 5G suppliers from closely allied countries, says defence minister », *Reuters*, 2020 (b). Disponible sur https://www.reuters.com/article/us-telecoms-5g-denmark-idUSKBN23F1IT, consulté le 7/8/2022.

Reuters, « Romanian president signs bill into law to ban Huawei from 5G », *Reuters*, 2021. Disponible sur https://www.reuters.com/business/media-telecom/romanian-president-signs-bill-into-law-ban-huawei-5g-2021-06-11/, consulté le 7/8/2022.

SEFERIADIS Giannis, « Greece joins 'anti-Huawei camp' as US seals stronger ties », *Nikkei Asia*, 2020. Disponible sur https://asia.nikkei.com/Spotlight/Huawei-crackdown/Greece-joins-anti-Huawei-camp-as-US-seals-stronger-ties, consulté le 7/8/2022.

Silicon, « Siemens et Huawei renforcent leur partenariat », *Silicon*, 2004. Disponible sur https://www.silicon.fr/siemens-et-huawei-renforcent-leur-partenariat-7085.html#, consulté le 13/6/2022.

STUPP Catherine, « U.S., EU Plan Joint Foreign Aid for Cybersecurity to Counter China », *Wall Street Journal*, 2022. Disponible sur https://www.wsj.com/articles/u-s-eu-plan-joint-foreign-aid-for-cybersecurity-to-counter-china-11655285401, consulté le 13/6/2022.

The Economist, « And the winners were... », *The Economist*, 2010. Disponible sur https://www.economist.com/technology-quarterly/2010/12/11/and-the-winners-were, consulté le 7/9/2022.

WAGNER Jack, « China's Cybersecurity Law: What You Need to Know », *The Diplomat*, 2017. Disponible sur https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/, consulté le 8/8/2022.

WATERS Richard et POLITI James, « Huawei-3Com deal finally collapses », *Financial Times*, 2008. Disponible sur https://www.ft.com/content/c2091814-f6b5-11dc-bda1-000077b07658, consulté le 8/9/2022.

WEISMAN Steven R., « Sale of 3Com to Huawei is derailed by U.S. security concerns », *The New York Times*, 2008. Disponible sur https://www.nytimes.com/2008/02/21/business/worldbusiness/21iht-3com.1.10258216.html, consulté le 8/9/2022.

YAP Chuin-Wei, STRUMPF Dan, VOLZ Dustin, O'KEEFFE Kate et VISWANATHA Aruna, « Huawei's Yearslong Rise Is Littered With Accusations of Theft and Dubious Ethics », *Wall Street Journal*, 2019. Disponible sur https://www.wsj.com/articles/huaweis-yearslong-rise-is-littered-with-accusations-of-theft-and-dubious-ethics-11558756858, consulté le 8/8/2022.

Documents officiels et privés

CAVE Danielle, « The African Union headquarters hack and Australia's 5G network », *Strategist*, Australian Strategic Policy Institute, 2018. Disponible sur https://www.aspistrategist.org.au/the-african-union-headquarters-hack-and-australias-5g-network/, consulté le 7/8/2022.

Commission européenne, « L'UE ouvre une enquête antidumping sur les importations de panneaux solaires en provenance de Chine », 2012. Disponible sur https://ec.europa.eu/commission/presscorner/detail/fr/MEMO_12_647, consulté le 7/8/2022.

Commission européenne, « Mémo: l'UE institue des droits antidumping provisoires sur les panneaux solaires chinois », 2013 (a). Disponible sur https://ec.europa.eu/commission/presscorner/detail/fr/MEMO_13_497, consulté le 7/8/2022.

Commission européenne, « Proposition de Directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union », 2013 (b). Disponible sur https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=COM%3A2013%3A0048%3AFIN, consulté le 7/8/2022.

Commission européenne, « La Commission européenne se félicite de l'accord intervenu entre les industries vinicoles européenne et chinoise qui mettra un terme aux procédures antidumping et antisubventions engagées par la Chine », 2014 (a). Disponible sur https://ec.europa.eu/commission/presscorner/detail/fr/IP_14_301, consulté le 7/8/2022.

Commission européenne, « L'UE ne poursuivra pas l'enquête antidumping sur les importations de réseaux de télécommunications mobiles en provenance de Chine », 2014 (b). Disponible sur https://ec.europa.eu/commission/presscorner/detail/fr/IP_14_339, consulté le 17/7/2022.

Commission européenne, « Communication de la Commission au Parlement européen et du Conseil, au Comité Économique et social européen et au Comité des Régions Façonner l'avenir numérique de l'Europe COM/2020/67 final », 2020 (a). Disponible sur https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52020DC0067&qid=1660928211569, consulté le 7/8/2022.

Commission européenne, « Proposition de Directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE) 2016/1148 », 2020 (b). Disponible sur https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52020PC0823&qid=1660485302772, consulté le 7/8/2022.

Commission européenne, « Document de travail conjoint des services Partenariat renouvelé avec le voisinage méridional Plan économique et d'investissement en faveur du voisinage méridional accompagnant le document: Communication conjointe au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des Régions Un partenariat renouvelé avec le voisinage méridional Un nouveau programme pour la Méditerranée SWD/2021/23 final », 2021. Disponible sur https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52021SC0023&qid=1661625145126, consulté le 7/8/2022.

Commission européenne, *UE-Afrique : paquet d'investissement « Global Gateway » – Transition numérique*, 2022. Disponible sur https://ec.europa.eu/commission/presscorner/detail/fr/fs_22_1117, consulté le 17/7/2022.

Commission européenne et Haute représentante de l'Union pour les affaires étrangères et la politique de sécurité, « Communication conjointe au Parlement européen et au Conseil au Comité économique et social européen et au Comité des Régions Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé - JOIN(2013) 01 final », 2013, Disponible sur https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52013JC0001&qid=1661611415863, consulté le 17/8/2022.

Commission européenne et Haut représentant de l'Union pour les affaires étrangères et la politique de sécurité, « Communication conjointe au Parlement européen et au Conseil - La stratégie de cybersécurité de l'UE

pour la décennie numérique - JOIN(2020) 18 final », 2020, Disponible sur https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52020JC0018&from=EN, consulté le 17/6/2022.

Commission européenne et Haut représentant de l'Union pour les affaires étrangères et la politique de sécurité, « Communication conjointe au Parlement européen et au Conseil, au Comité Économique et social européen et au Comité des Régions Un partenariat renouvelé avec le voisinage méridional Un nouveau programme pour la Méditerranée JOIN/2021/2 final », 2021, Disponible sur https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52021JC0002, consulté le 17/8/2022.

Conseil constitutionnel, « Décision n° 2020-882 QPC du 5 février 2021 », *Légifrance*, 2021. Disponible sur https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043100136, consulté le 17/7/2022.

Conseil d'État, « Conseil d'État, 2ème - 7ème chambres réunies, 08/04/2021, 442120 », *Légifrance*, 2021. Disponible sur https://www.legifrance.gouv.fr/ceta/id/CETATEXT000043358785?dateDecision=01%2F04%2F2021+%3E+30%2F04%2F2021&page=1&pageSize=10&query=Bouygues+Telecom&searchField=ALL&searchType=ALL&sortValue=DATE_DESC&tab_selection=cetat, consulté le 17/7/2022.

Conseil de l'Union européenne, « Le Partenariat stratégique Afrique-UE une stratégie commune Afrique-UE », 2007. Disponible sur https://data.consilium.europa.eu/doc/document/ST-16344-2007-INIT/fr/pdf, consulté le 17/8/2022.

Conseil de l'Union européenne, « Le Partenariat stratégique Afrique - Union européenne Relever ensemble les défis d'aujourd'hui et de demain », 2011. Disponible sur https://www.consilium.europa.eu/media/31038/qc3111092frc.pdf, consulté le 17/8/2022.

Conseil de l'Union européenne, « Quatrième Sommet UE-Afrique 2-3 Avril 2014, Bruxelles Feuille de Route 2014-2017 », 2014. Disponible sur https://www.consilium.europa.eu/media/21519/142099.pdf, consulté le 17/8/2022.

Conseil de l'Union européenne, « Investir dans la jeunesse pour une croissance inclusive accélérée et le développement durable Déclaration », 2017. Disponible sur https://www.consilium.europa.eu/media/54379/33573-pr-sc21052_f_-_final_decl_5th_au-eu_summit.pdf, consulté le 17/8/2022.

Conseil de l'Union européenne, «Sixième sommet Union européenne – Union africaine: une vision commune pour 2030 », 2022. Disponible sur https://www.consilium.europa.eu/media/54411/final-declaration-fr.pdf, consulté le 17/8/2022.

Department of Commerce of the United States of America, « Hungary ICT - 5G Development », 2020. Disponible sur https://www.trade.gov/market-intelligence/hungary-ict-5g-development, consulté le 7/8/2022.

Department of Commerce of the United States of America, « U.S.-EU Joint Statement of the Trade and Technology Council », 2022. Disponible sur https://www.commerce.gov/news/press-releases/2022/05/us-eu-joint-statement-trade-and-technology-council, consulté le 22/8/2022.

Department of Economic and Social Affairs of the United Nations, *E-Government Survey 2020*, New York, 2020. Disponible sur https://publicadministration.un.org/en/Research/UN-e-Government-Surveys, consulté le 7/9/2022.

Department of State of the United States of America, « Joint Statement on United States-Latvia Joint Declaration on 5G Security », 2020 (a). Disponible sur https://2017-2021.state.gov/joint-statement-on-united-states-latvia-joint-declaration-on-5g-security/index.html, consulté le 7/8/2022.

Department of State of the United States of America, « United States – Republic of Lithuania Memorandum of Understanding on 5G Security », 2020 (b). Disponible sur https://2017-2021.state.gov/united-states-republic-of-lithuania-memorandum-of-understanding-on-5g-security/index.html, consulté le 7/8/2022.

Department of State of the United States of America, « United States – Republic of Bulgaria Joint Declaration on 5G Security », 2020 (c). Disponible sur https://2017-2021.state.gov/united-states-republic-of-

bulgaria-joint-declaration-on-5g-security/index.html, consulté le 7/8/2022.

Department of State of the United States of America, « United States – Slovak Republic Joint Declaration on 5G Security », 2020 (d). Disponible sur https://2017-2021.state.gov/united-states-slovak-republic-joint-declaration-on-5g-security/index.html, consulté le 7/8/2022.

Department of State of the United States of America, « Digital Briefing with Deputy Secretary of State, Wendy Sherman », 2022. Disponible sur https://www.state.gov/digital-briefing-with-deputy-secretary-of-state-wendy-sherman/, consulté le 23/8/2022.

European Commission, « Karel De Gucht European Commissioner for Trade EU-China Investment: A Partnership of Equals Bruegel Debate: China Invests in Europe Patterns Impacts and Policy Issues, Brussels 7 June 2012 », 2012. Disponible sur https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_12_421, consulté le 17/6/2022.

European Commission, « Statement by EU Trade Commissioner Karel De Gucht on mobile telecommunications networks from China », 2013. Disponible sur https://ec.europa.eu/commission/presscorner/detail/en/MEMO_13_439, consulté le 17/6/2022.

European Commission, *Cybersecurity of 5G networks EU Toolbox of risk mitigating measures*, 2020. Disponible sur https://digital-strategy.ec.europa.eu/fr/node/1215, consulté le 17/6/2022.

European Commission, « EU-US Trade and Technology Council Inaugural Joint Statement », 2021. Disponible sur https://ec.europa.eu/commission/presscorner/detail/fr/STATEMENT_21_4951, consulté le 17/8/2022.

European Parliament, « EU-China Comprehensive Agreement on Investment (EU-CHINA CAI) », Legislative Train Schedule, 2022. Disponible sur https://www.europarl.europa.eu/legislative-train/theme-a-stronger-europe-in-the-world/file-eu-china-investment-agreement, consulté le 8/8/2022.

Eurostat, « Africa-EU - international trade in goods statistics », 2022. Disponible sur https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Africa-EU_-_international_trade_in_goods_statistics, consulté le 8/9/2022.

Federal Bureau of Investigation, « Dangerous Partners: Big Tech and Beijing », 2020. Disponible sur https://www.fbi.gov/news/testimony/dangerous-partners-big-tech-and-beijing, consulté le 8/8/2022.

Federal Register, « Executive Order 13873 of May 15, 2019 Securing the Information and Communications Technology and Services Supply Chain», 2019. Disponible sur https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain, consulté le 8/8/2022.

GRIEGER Gisela, « EU-China Comprehensive Agreement on Investment - Levelling the playing field with China - », European Parliamentary Research Service, 2021. Disponible sur https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/679103/EPRS_BRI(2021)679103_EN.pdf, consulté le 8/8/2022.

IDE-JETRO (Institute of Developing Economies, Japan External Trade Organization), « China in Africa: A Strategic Overview », 2009. Disponible sur https://www.ide.go.jp/English/Data/Africa_file/Manualreport/cia.html, consulté le 17/6/2022.

Huawei, « Informations d'entreprise ». Disponible sur https://www.huawei.com/fr/corporate-information, consulté le 4/7/2022.

Huawei, « Qui détient Huawei ? ». Disponible sur https://www.huawei.com/fr/facts/question-answer/who-owns-huawei, consulté le 4/9/2022.

Huawei, « Huawei Helped Vodafone Commercially Deploy the World's First Cloud-based VoLTE Network in Italy », 2015. Disponible sur https://carrier.huawei.com/en/success-stories/wireless-network/volte/2, consulté le 4/9/2022.

Huawei Europe, « Huawei Honoured with Vodafone 'Supplier of the Decade' Award », 2018. Disponible sur https://huawei.eu/press-release/huawei-honoured-vodafone-supplier-decade-award, consulté le 4/9/2022.

Huawei Investment & Holding Co., Ltd., *Realize Your Potential Annual Report 2006*, 2006. Disponible sur https://www.huawei.com/en/annual-report, consulté le 28/8/2022.

Huawei Investment & Holding Co., Ltd., *Annual Report 2007 Enriching Life Through Communication*, 2007. Disponible sur https://www.huawei.com/en/annual-report, consulté le 28/8/2022.

Huawei Investment & Holding Co., Ltd., *Connected Possibilities 2011 Annual Report*, 2011. Disponible sur https://www.huawei.com/en/annual-report, consulté le 28/8/2022.

Huawei Investment & Holding Co., Ltd., *2013 Annual Report*, 2013. Disponible sur https://www.huawei.com/en/annual-report, consulté le 28/8/2022.

Huawei Investment & Holding Co., Ltd., *Building a Better Connected World 2014 Annual Report*, 2014. Disponible sur https://www.huawei.com/en/annual-report, consulté le 28/8/2022.

Huawei Investment & Holding Co., Ltd., *Building a Better Connected World 2015 Annual Report*, 2015. Disponible sur https://www.huawei.com/en/annual-report, consulté le 28/8/2022.

Huawei Investment & Holding Co., Ltd., *2016 Annual Report*, 2016. Disponible sur https://www.huawei.com/en/annual-report, consulté le 28/7/2022.

Huawei Investment & Holding Co., Ltd., *2017 Annual Report*, 2017. Disponible sur https://www.huawei.com/en/annual-report, consulté le 28/7/2022.

Huawei Investment & Holding Co., Ltd., *2018 Annual Report*, 2018. Disponible sur https://www.huawei.com/en/annual-report, consulté le 28/7/2022.

Huawei Investment & Holding Co., Ltd., *2019 Annual Report*, 2019. Disponible sur https://www.huawei.com/en/annual-report, consulté le 28/7/2022.

Huawei Investment & Holding Co., Ltd., *2021 Annual Report*, 2022. Disponible sur https://www.huawei.com/en/annual-report/2021, consulté le 17/7/2022.

Intelligence and Security Committee of Parliament, *Foreign involvement in the critical national infrastructure*, 2013. Disponible sur https://www.gov.uk/government/publications/foreign-involvement-in-the-critical-national-infrastructure-intelligence-and-security-committee-report, consulté le 7/8/2022.

MEDEIROS Evan S., CLIFF Roger, CARNE Keith et MULVENON James C., *A New Direction for China's Defense Industry*, Santa Monica, RAND Corporation, 2005. Disponible sur https://www.rand.org/pubs/monographs/MG334.html, consulté le 8/9/2022.

Ministry of Commerce of China, « Regular Press Conference of MOFCOM (January 21, 2021) », 2021. Disponible sur http://english.mofcom.gov.cn/article/newsrelease/press/202101/20210103034674.shtml, consulté le 8/8/2022.

Motorola Solutions, « Motorola Solutions and Huawei Issue Joint Statement », 2011. Disponible sur https://www.motorolasolutions.com/newsroom/press-releases/motorola-solutions-and-huawei-issue-joint-statement.html, consulté le 8/9/2022.

National Institute for Defense Studies, *NIDS China Security Report 2021 - China's Military Strategy in the New Era -*, 2021. Disponible sur http://www.nids.mod.go.jp/publication/chinareport/pdf/china_report_EN_web_2021_A01.pdf, consulté le 8/8/2022.

NOCETTI Julien et SEAMAN John, « L'affaire Huawei. Un miroir de la guerre technologique sino-américaine », in DE MONTBRIAL Thierry (dir.), *Ramses 2020 Un monde sans boussole ?*, Paris, Institut français des relations internationales, 2019, pp. 294-297. Disponible sur https://www.cairn.info/--9782100801138-page-294.htm, consulté le 9/9/2022.

Organisation de Coopération et de développement économiques, *Les profils de coopération au développement*, Paris, Éditions OCDE, 2022. Disponible sur https://doi-org.ena.idm.oclc.org/10.1787/5cd4ba84-fr,

consulté le 17/9/2022.

OKAMURA Shigako, « Chugoku no Kokka Jōhō Hō » (La Loi sur le Renseignement national de la Chine), *Gaikoku no Rippō (Législation à l'étranger)*, vol. 274, Tokyo, Direction générale de la Recherche et de la considération législative, Bibliothèque nationale de la Diète, 2017. pp. 64 – 75. Disponible sur https://dl.ndl.go.jp/view/download/digidepo_11000634_po_02740005.pdf?contentNo=1&alternativeNo=, consulté le 17/6/2022.

OSAWA Jun, « Chūgoku to digital techno haken no yume » (Chine et le rêve de l'hégémonie de la technologie numérique), Tokyo, Mita Hyōron Online, 2021. Disponible sur https://www.mita-hyoron.keio.ac.jp/features/2021/08-4_2.html, consulté le 6/9/2022.

Parlement européen, « 2010/2301(INI) UE - Chine: échange inégal ? », 2010. Disponible sur https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=fr&reference=2010/2301(INI), consulté le 6/8/2022.

Parlement européen, « 13. L'UE et la Chine: un déséquilibre commercial? (débat) », 2012. Disponible sur https://www.europarl.europa.eu/doceo/document/CRE-7-2012-05-22-ITM-013_FR.html, consulté le 6/8/2022.

Parlement européen, « 21. Cadre pour le filtrage des investissements directs étrangers dans l'Union européenne (débat) », 2019 (a) Disponible sur https://www.europarl.europa.eu/doceo/document/CRE-8-2019-02-13-ITM-021_FR.html, consulté le 6/8/2022.

Parlement européen, « 27. Menaces pour la sécurité liées à la présence technologique croissante de la Chine dans l'UE et actions possibles à l'échelle de l'UE pour les réduire (débat) », 2019 (b). Disponible sur https://www.europarl.europa.eu/doceo/document/CRE-8-2019-02-13-ITM-027_FR.html, consulté le 6/8/2022.

Parlement européen, « Résolution du Parlement européen du 12 mars 2019 sur les menaces pour la sécurité liées à la présence technologique croissante de la Chine dans l'Union et les actions possibles à l'échelle de l'UE pour les réduire (2019/2575(RSP)) », 2019 (c). Disponible sur https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:52019IP0156&qid=1660476963481, consulté le 6/8/2022.

Parlement européen, « 13. Cyberattaques récentes contre des institutions européennes et des institutions nationales sensibles, publiques comme privées - Stratégie de cybersécurité de l'Union pour la décennie numérique (débat) », 2021. Disponible sur https://www.europarl.europa.eu/doceo/document/CRE-9-2021-06-09-ITM-013_FR.html, consulté le 6/8/2022.

Permanent Select Committee on Intelligence of the U.S. House of Representatives, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, 2013. Disponible sur https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=96, consulté le 7/8/2022.

Presidency of Romania, « Joint Statement from President of the United States Donald J. Trump and President of Romania Klaus Iohannis », 2019. Disponible sur https://www.presidency.ro/en/media/press-releases/joint-statement-from-president-of-the-united-states-donald-j-trump-and-president-of-romania-klaus-iohannis, consulté le 6/8/2022.

Republic of Slovenia, « Slovenia and the US sign a Joint Declaration on 5G Security », 2020. Disponible sur https://www.gov.si/en/news/2020-08-13-slovenia-and-the-us-sign-a-joint-declaration-on-5g-security/, consulté le 6/8/2022.

SACKS David, « China's Huawei Is Winning the 5G Race. Here's What the United States Should Do To Respond », Council on Foreign Relations, 2021. Disponible sur https://www.cfr.org/blog/china-huawei-5g, consulté le 6/8/2022.

The National People's Congress of People's Republic of China (中华人民共和国全国人民代表大会), « 中华人民共和国网络安全法 » (Loi sur la Cybersécurité de la République populaire de la Chine), 2016. Disponible sur https://flk.npc.gov.cn/detail2.html?MmM5MDlmZGQ2NzhiZjE3OTAxNjc4YmY4Mjc2ZjA5M2Q%3D, consulté le 6/9/2022.

The National People's Congress of People's Republic of China (中华人民共和国全国人民代表大会), « 中华人民共和国国家情报法 » (Loi sur le Renseignement national de la République populaire de la Chine), 2017. Disponible sur https://flk.npc.gov.cn/detail2.html?MmM5MDlmZGQ2NzhiZjE3OTAxNjc4YmY4NDk4ZDA5ZjE%3D, consulté le 6/9/2022.

The National People's Congress of People's Republic of China (中华人民共和国全国人民代表大会), « 十三届全国人大二次会议新闻发布会 » (Conférence de presse de la deuxième session du 13ème Congrès national du peuple, 2019. Disponible sur http://www.npc.gov.cn/zgrdw/npc/zhibo/zzzb44/node_381.htm, consulté le 6/9/2022.

U.K. Government, « Huawei to be removed from UK 5G networks by 2027 », 2020. Disponible sur https://www.gov.uk/government/news/huawei-to-be-removed-from-uk-5g-networks-by-2027, consulté le 6/8/2022.

Union européenne, « Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union », *Journal officiel de l'Union européenne* L 194, 19 juillet 2016, p.1. Disponible sur https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016L1148&qid=1661610548324, consulté le 17/7/2022.

Union européenne, « Règlement (UE) 2019/452 du Parlement européen et du Conseil du 19 mars 2019 établissant un cadre pour le filtrage des investissements directs étrangers dans l'Union », *Journal officiel de l'Union européenne* L 79 du 21 mars 2019, pp.1 - 14. Disponible sur https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32019R0452&qid=1662395207414, consulté le 17/9/2022.

Union pour la Méditerranée, « Les ministres de l'Union pour la Méditerranée (UpM) en charge de l'économie numérique lancent de nouvelles initiatives de coopération numérique », 2014. Disponible sur https://ufmsecretariat.org/fr/union-for-the-mediterranean-ufm-ministers-in-charge-of-the-digital-economy-launch-new-digital-cooperation-initiatives/, consulté le 17/7/2022.

United States Congress, « John S. McCain National Defense Authorization Act for Fiscal Year 2019 », *Congress Library*, 2018. Disponible sur https://www.congress.gov/bill/115th-congress/house-bill/5515/text?q=%7B%22search%22%3A%5B%22national+defense+authorization+act+2019%22%2C%22national%22%2C%22defense%22%2C%22authorization%22%2C%22act%22%2C%222019%22%5D%7D&r=2&s=4, consulté le 17/7/2022.

U.S. Embassy in Estonia, « United States – Estonia Joint Declaration on 5G Security », 2019. Disponible sur https://ee.usembassy.gov/joint-declaration-on-5g/, consulté le 17/7/2022.

U.S. Senate Committee on Homeland Security & Governmental Affairs, « Congressional Leaders Cite Telecommunications Concerns with Firms that Have Ties with Chinses Government », 2010. Disponible sur https://www.hsgac.senate.gov/media/minority-media/congressional-leaders-cite-telecommunications-concerns-with-firms-that-have-ties-with-chinese-government, consulté le 7/9/2022.

Chronologie

Année	Presse	Huawei	Gouvernement	Tribunaux	Note
1963		Fin de la formation de Ren Zhengfei à l'Institut de l'Ingénierie civile et de l'architecture de Chongqing			
1974		Ren Zhengfei intègre l'APL.			
1982		La fin du service à l'APL de Ren Zhengfei			
1987		**Établissement à Shenzhen**			
1988		Ren Zhengfei devient PDG.			
1995		Réussitte dans le marché rural de la Chine			
1998		**Lancement des affaires au Kenya et en Afrique du Sud**			
1999		Lancement des affaires en Algérie, au Maroc et en Tunisie			
2000		**Lancement des affaires en Europe** et Égypte Suède : Établissement d'un centre R&D			
2003		Algérie : Expansion du réseau GSM			
janvier 2003				Cisco Systems accuse Huawei de violation de son brevet et de copie de son code-source.	
2004		Qualification par France Télécom	Nigéria : Prêt de 200 M ($) de China Development Bank pour introduire des équipements de Huawei		
juillet 2004		Règlement de l'appel par Cisco Huawei a admis la copie de son logiciel.			
février 2004		Établissement d'une co-entreprise avec Siemens			
le 2 décembre 2004		Contrat avec Telfort (Premier contrat significatif en Europe)			
le 10 décembre 2004	FT : « Huawei wins 3G contract from Telfort »				
2005		Les commandes de contrats internationaux dépassent les ventes en Chine pour la première fois. Afrique du Sud : Signe du partenariat stratégique avec l'opérateur sud-africain, MTN			Publication de « A New Direction for China's Defense Industry » par RAND Corporation

le 28 avril 2005		Sélectionné comme fournisseur du programme 21 Century Network BT			
2006		Commencement de la publication de « Annual Report » Un contrat-cadre international avec Vodafone Lancement des affaires en Côte d'Ivoire et République démocratique de Congo	Kenya : Lancement du projet de 25 millions dollars pour développer les télécommunications rurales de Huawei		
2007		Établissement d'une co-entreprise avec Symantec Remise du Prix « 2007 Global Supplier » par Vodafone Partenariat avec l'ensemble des opérateurs majeurs en Europe fin 2007. Côte d'Ivoire : Développement du centre de donnée pour l'e-gouvernement			
septembre 2007		Arrivée à l'accord de l'achat de 3Com en partenariat avec Bain Capital	États-Unis : Lancement de l'enquête par CFIUS sur l'accord de l'achat de 3Com		
décembre 2007			UE et Afrique : Le deuxième Sommet UE-Afrique à Lisbonne (Adoption de la « Stratégie commune Afrique-UE »)		
2008					Un employé de Nortel effectue une enquête sur les cyberattaques en provenance de la Chine.
mars 2008		Annulation du projet de l'achat de 3Com			
2009	Reuter (Établissement de la Centre logistique européenne de Huawei en Hongrie) FT : « Boldness in Business 2009 » (Remise du prix à Huawei)	Établissement de « Huwei Marine », co-entreprise avec Global Marine Hongrie : Construction du centre de d'approvisionnement en Europe. Norvège : Construction du réseau commercial LTE/EPC pour TeliaSonera	Cameroun : Signe de l'accord du prêt de 52 M ($) avec CEXIM pour le projet d'installer la fibre optique de Huawei		Faillite de Nortel Les anciens employés de Nortel, TONG Wen et WHU Peiying, intègrent Huawei.
2010		Établissement de son Centre pour l'évaluation de la cybersécurité au Royaume-Uni. France : Lancement du programme de formation et de stage pour les élèves de l'École polytechnique		Motorola accuse Huawei de vol de la propriété intellectuelle	
mai 2010			CE et la Chine : Accord pour lancer la négociation pour l'AGI		

août 2010			États-Unis : Des parlementaires américains envoient une lettre à l'administration pour exprimer leur préoccupation sur la participation des TIC chinoises à l'adjudication de Sprint Nextel.		
octobre 2010			États-Unis : Des parlementaires américains envoient une autre lettre à l'administration et à la commission du Congrès pour exprimer leur préoccupation sur la participation des TIC chinoises à l'adjudication de Sprint Nextel.		.
novembre 2010			UE et Afrique : Le troisième Sommet UE-Afrique à Tripoli (Adoption du « Plan d'action 2011-2013 »)		
le 5 novembre 2010	WSJ : «Security Fears Kill Chinese Bid in U.S. » (Sprint Nextel a exclu Huawei et ZTE du contrat après une échange téléphonique entre le Secrétaire du Commerce et le PDG.)				
le 11 décembre 2010	The Economist : « And the winners were... » (Remise du « Prix de l'innovation à usage corporatif »)				
2011		Mali : Développement du réseau de câble fibre-optique	États-Unis : CFIUS bloque le deal de Huawei pour acheter 3Leafs. Mali : Accord du prêt de 63 M ($) de la CEXIM pour développer le réseau national de broadband par Huawei		
le 13 avril 2011				Règlement de l'appel de Motorola contre Huawei	
2012					Construction des bâtiments du siège de l'UA à Addis-Abeba par les aides chinoises
le 14 février 2012	WSJ : « Chinese Hackers Suspected In Long-Term Nortel Breach »				
le 15 février 2012	CBC News : « Nortel collapse linked to Chinese hackers »				
mars 2012			**Australie : Expulsion de Huawei du projet de National Broadband Network**		

26 mars 2012	Reuters : « Australia blocks China's Huawei from broadband tender » (Canberra rejette Huawei de ses réseaux compte tenu du conseil du service du renseignement australien.)				
le 6 septembre 2012			**CE : Lancement de l'enquête antidumping sur les panneaux photovoltaïques importés de la Chine**		
octobre 2012			Canada : Expulsion de Huawei du projet des réseaux des données et des télécommunications de l'administration publique		
le 8 octobre 2012			États-Unis : Publication du rapport sur Huawei et ZTE par Permanent Select Committee on Intelligence de la Chambre des représentants du Congrès		
le 10 octobre 2012	The Guardian : « Huawei's relationship with BT under investigation by MPs » Reuters : « Former Canadian spy sees Huawei risk as manageable »				
le 11 octobre 2012	CBC News : « Former Nortel exec warns against working with Huawei »				
2013		**L'Europe devient plus grand marché derrière la Chine.** Gambie : Signe du contrat de 33 millions dollars pour installer un câble fibre-optique qui connecte avec les autres pays de la CEDEAO	États-Unis : Opposition contre la construction d'un câble sous-marin entre New York et Londres Cameroun : Signe de la convention de financement avec la Chine pour le projet du plan national de télécommunications d'urgence		
février 2013			CE et HRAEPS : Publication de « Stratégie de cybersécurité de l'Union européenne : un cyberespace ouvert, sûr et sécurisé »		
avril 2013			Suède : Ministre du Commerce exprime son inquiétude sur l'enquête sur les TIC chinoises		

mai 2013			Allemagne : Le ministre de l'Economie exige Karel DE GUCHT de trouver une autre solution. Royaume-Uni : Le ministre chargé de l'énergie et du changement climatique visite Bruxelles pour convaincre le Commissaire Karel DE GUCHT.		
le 6 mai 2013	Euractive : « De Gucht juggles politics, diplomacy in high-stakes China gambit »				
le 15 mai 2013			**CE : Décision d'e lancer une enquête antidumping et antisubventions sur les TIC chinoises, annoncée par le Commissaire Karel DE GUCHT**		
le 26 mai 2013			Chine : Premier ministre exprime l'inquiétude sur les enjeux commerciaux entre l'UE et la Chine.		
juin 2013			Royaume-Uni : Publication du rapport « Foreign Involvement in the critical infrastructure » par Intelligence and Security Committee du parlement		
le 1er juillet 2013			Chine : Le Ministère du Commerce lance une enquête antidumping et antisubventions sur les vins européens.		
octobre 2013	Fortune : PDG de BT "Huawei is a "good partner" "				
novembre 2013			UE et la Chine : Lancement de la négociation officielle pour l'AGI		
2014		Construction d'une plateforme de cloud pour Qwant Burundi : Lancement du développement du réseau de broadband en partenariat avec un opérateur des télécommunications régional, Onatel Gabon : Signe du contrat de 26 M ($) pour construire un câble fibre-optique qui connecte avec la République du Congo		T-Mobile accuse Huawei de l'espionnage industrielle	
janvier 2014			UE et la Chine : Première négociation de l'AGI		

le 27 mars 2014			**CE : Décision de ne pas poursuivre l'enquête sur les TIC chinoises, annoncée par Karel DE GUCHT**		
avril 2014			UE et Afrique : Le quatrième Sommet UE-Afrique à Bruxelles (Adoption de la Feuille de Route 2014-2017)		
septembre 2014			UE et UpM : Réunion ministérielle de l'UpM sur l'économie numérique à Bruxelles		
octobre 2014			CE : Fin officielle de l'enquête sur les TIC chinoises		
le 20 octobre 2014	Les Échos : « Télécoms : l'Europe et la Chine font la paix » (Les TIC européennes n'étaient pas positives pour la coopération avec la CE pour l'enquête sur celles de la Chine.)				
novembre 2014			CE : Fin du mandat du Commissaire Karel DE GUCHT		
2015	Media 24 (Construction du nouveu siège régional "Afrique francophone" en Maroc par Huawei)	Introduction du système de stockage de données à Telefonica et Vodafone, de « Fusionsphere Cloud Operating System » à SFR et du service du centre de données à Criteo Assistance à Vodafone Italy pour déployer les réseaux « Cloud-based » VolTE	Bénin : Signe du prêt 69 M ($) par CEXIM pour développer l'infrastructure des télécommunications et le broadband fibre-optique de Huawei		
2016		Tanzanie : Le déploiement du service des réseaux 4,5G par Huawei			
juillet 2016			**UE : Entrée en vigueur de la Directive 2016/1148**		
2017		Rwanda : Signe du MOU pour construire des centres de données régionales et développer le service de broadband	**Chine : Entrée en vigueur de la « Loi sur Cybersécurité » et de la « Loi sur le Renseignement national »** République du Congo : Signe de l'accord du prêt de 161 M ($)avec CEXIM pour faire développer Huawei le réseau des télécommunications national		
le 17 mai 2017				**La Cour fédérale à Seattle a admis partiellement l'argument de T-Mobile sur l'espionnage du secret industriel.**	
novembre 2017			UE et UA : Le cinquième Sommet UE-UA à Abidjan		

2018		Lybie : Développement des réseaux de 4G Mozambique : Signe de l'accord avec l'opérateur, Mozambique Cellular, pour désigner Huawei en tant que fournisseur préféré			
janvier 2018	**Le Monde : de « A Addis-Abeba, le siège de l'Union africaine espionné par Pékin »**				
le 18 mars 2018			**États-Unis : Entrée en vigueur de NDAA 2019 (Interdiction de l'utilisation des produits de Huawei au sein de la fonction publique fédérale)**		
mai 2018		Remise de « Supplier of the Decade Award » par Vodafone			
août 2018			**Australie : Expulsion de Huawei du développement des réseaux 5G**		
décembre 2018			Tchéquie : Interdiction de l'utilisation des portables de Huawei aux fonctionnaire de l'État		
2019		Vente de « Huawei Marine » Mauritanie : Accord de coopération entre l'opérateur des télécommunications mauritanien, Mattel			
le 20 février 2019	CBS : « Huawei founder says he would defy Chinese law on intelligence gathering »				
mars 2019			UE: Entrée en vigueur du Règlement (UE) 2019/452		
le 4 mars 2019	CNBC : « Huawei says it would never hand data to China's government. Experts say it wouldn't have a choice »		Chine : ZHANG Yesui, Président de la Commission des Affaires étrangères du Congrès national du people, nie les préoccupations sur la législation chinoise pendant la conférence de presse.		
le 3 août 2019			**France : Entrée en vigueur de la loi "Huawei" (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))**		

le 20 août 2019			**États-Unis et Roumanie : Déclaration conjointe sur la coopération des réseaux des télécommunications**		
le 2nd 2019			**États-Unis et Pologne : Déclaration conjointe sur la coopération des réseaux des télécommunications**		
octobre 2019		**Hongrie : Ouverture du premier réseau commercial de 5G en partenariat avec Vodafone Hungary**			
le 1er novembre 2019			**États-Unis et Estonie : Déclaration conjointe sur la coopération des réseaux des télécommunications**		
le 6 décembre 2019			**France : Décret n° 2019-1300 relatif aux modalités de l'autorisation préalable de l'exploitation des équipements de réseaux radioélectriques**		
le 29 janvier 2020			**CE : Publication de "Cybersecurity of 5G networks EU Toolbox of risk mitigating measures"**		
le 27 février 2020			**États-Unis et Lettonie : Déclaration conjointe sur la coopération des réseaux des télécommunications**		
mai 2020			**États-Unis et République tchèque : Déclaration conjointe sur la coopération des réseaux des télécommunications**		
juin 2020			**Danemark : Le ministre de la Défense annonce l'expulsion de Huawei.**		
le 25 juin 2020	The Daily Telegraph : « The free world must unite against Huawei » rédigé par le Sous-Secrétaire d'État américain				
le 14 juillet 2020			**Royaume-Uni : Décision d'expulser Huawei de ses réseaux de 5G**		

le 13 août 2020			**États-Unis et Slovène : Déclaration conjointe sur la coopération des réseaux des télécommunications**		
septembre 2020			**États-Unis et Lituanie : Déclaration conjointe sur la coopération des réseaux des télécommunications**		
le 20 octobre 2020			**Suède : Expulsion de Huawei de ses réseaux des télécommunications**		
le 23 octobre 2020			**États-Unis et Bulgarie : Déclaration conjointe sur la coopération des réseaux des télécommunications** **États-Unis et Slovaquie : Déclaration conjointe sur la coopération des réseaux des télécommunications**		
décembre 2020			UE et Chine : Arrivée à l'accord sur l'AGI		
le 16 décembre 2020			CE : Proposition de la nouvelle directive qui remplace la Directive (UE) 2016/1148 UE (Joint Communication to the EP and the CE - The EU's Cybersecurity Strategy for the Digital Decade)		
janvier 2021	Politico : « Sweden faces Chinese blowback over Huawei ban »				
février 2021			CE et HRAEPS : Publication de « Un partenariat renouvelé avec le voisinage méridional »		
le 5 février 2021				**France : Conseil constitutionnel prend une décision sur la constitutionnalité.**	
le 8 avril 2021				**France : Conseil d'État rejette le recours par les opérateurs français.**	
le 23 avril 2021			**Allemagne : Le Bundestag passe « IT Security Law 2.0 ».**		

le 19 mai 2021	Euractive : Différentes réponses des EM de l'UE contre 5G de Huawei				
le 22 juin 2021				**Suède : La cour admet la légalité de la décision de l'État pour expulser Huawei.**	
le 29 septembre 2021			**UE et États-Unis : Premier CCT à Pittsburgh**		
le 29 octobre 2021	Euractive : « L'Autriche compte sur Huawei pour le déploiement de son réseau 5G »				
février 2022			**UE et UA : Le sixième Sommet UE-UA à Bruxelles (Publication de « Global Gateway »)**		
mai 2022			États-Unis : La Secrétaire d'État adjointe exprime les préoccupations sur Huawei lors de son tour aux pays africains.		
le 16 mai 2022			**UE et États-Unis : Le deuxième CCT à Paris-Saclay**		
le 15 juin 2022	WSJ (Plan de la cooperation entre les États-Unis et l'UE pour l'infrastructure numérique dans le pays en développement)				
le 22 juin 2022				**Suède : La cour administrative d'appel soutient la décision du 22 juin 2021 de la cour.**	