

OCTOBRE
2022

Les réseaux télécoms “ouverts” (Open RAN)

Vers une reconfiguration de la compétition internationale dans la 5G ?



Programme
Géopolitique des
technologies

Mathilde VELLIET

L’Ifri est, en France, le principal centre indépendant de recherche, d’information et de débat sur les grandes questions internationales. Créé en 1979 par Thierry de Montbrial, l’Ifri est une association reconnue d’utilité publique (loi de 1901). Il n’est soumis à aucune tutelle administrative, définit librement ses activités et publie régulièrement ses travaux.

L’Ifri associe, au travers de ses études et de ses débats, dans une démarche interdisciplinaire, décideurs politiques et experts à l’échelle internationale.

Les opinions exprimées dans ce texte n’engagent que la responsabilité de l’auteur.

ISBN : 979-10-373-0599-2

© Tous droits réservés, Ifri, 2022

Couverture : © Diego Schtutman/Shutterstock.com

Comment citer cette publication :

Mathilde Velliet, « Les réseaux télécoms “ouverts” (Open RAN).
Vers une reconfiguration de la compétition internationale dans la 5G ? »,
Notes de l’Ifri, Ifri, octobre 2022.

Ifri

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

Tél. : +33 (0)1 40 61 60 00 – Fax : +33 (0)1 40 61 60 60

E-mail : accueil@ifri.org

Site internet : ifri.org

Auteure

Mathilde Velliet est chercheuse au sein du programme Géopolitique des technologies de l'Ifri, qu'elle a rejoint en septembre 2021. Ses travaux portent sur les enjeux internationaux liés aux nouvelles technologies, en particulier les politiques technologiques américaines et chinoises et les relations sino-américaines.

Mathilde Velliet poursuit un doctorat en civilisation américaine à l'Université de Paris : ses recherches analysent la fabrique des politiques américaines de protection des technologies stratégiques sous les administrations Obama et Trump.

Elle est diplômée d'un master en Études anglophones de l'École normale supérieure de Lyon et d'un master en Sécurité internationale de Sciences Po Paris, et a effectué deux séjours de recherche aux États-Unis, à l'université de New York puis à l'université de Boston.

Elle a notamment publié « Convaincre et contraindre : les interférences américaines dans les échanges technologiques entre leurs alliés et la Chine » (*Études de l'Ifri*, février 2022).

Résumé

Le réseau d'accès radio (RAN) est la partie radio d'un système de télécommunications mobiles qui permet la connexion entre un terminal (comme un téléphone ou un ordinateur) et le cœur de réseau. Alors que traditionnellement un seul équipementier (comme Huawei, Ericsson ou Nokia) fournit une solution dite « propriétaire », ou « fermée » pour toute cette partie du réseau, l'Open RAN (*Open Radio Access Network*) est un concept qualifiant des architectures désagrégées séparant le RAN en plusieurs briques séparées par des interfaces ouvertes. L'objectif est ainsi de permettre à l'opérateur d'acheter ces briques matérielles et logicielles à des fournisseurs variés, en étant libre de choisir pour chaque brique l'option la plus adaptée. Dans un contexte de concentration du marché 5G, dominé par trois grands équipementiers, voire de risque de duopole Ericsson-Nokia avec l'exclusion de Huawei de nombreux pays, les opérateurs télécoms soulignent la flexibilité et la diversification des fournisseurs permise par l'Open RAN, qui permettrait à la fois plus l'innovation et une réduction des coûts. Dans la lignée de leur campagne diplomatique contre les fournisseurs chinois jugés non fiables, les États-Unis ont ainsi activement promu l'Open RAN comme alternative.

Toutefois, l'Open RAN semble loin d'être la panacée pour l'Europe : outre les difficultés qui persistent en termes de maturité, sécurité, performance et transparence du processus de spécification, il risque d'accroître la dépendance européenne aux fournisseurs étrangers. Si Huawei ne fait pas partie des instances internationales travaillant sur l'Open RAN (comme le Telecom Infra Project ou l'Alliance O-RAN), de nombreuses entreprises proches des autorités politiques et militaires chinoises en font partie. Au-delà de la question de la sécurité des fournisseurs, le lobbying américain est lié à l'opportunité commerciale que représente l'Open RAN pour les entreprises américaines, leaders dans le *cloud*, le logiciel et les composants matériels génériques... alors qu'elles ne comptent pas de grand équipementier champion de la 5G. L'Open RAN est ainsi un enjeu au croisement de la géopolitique de la 5G et des standards, auquel l'Union européenne commence à apporter une réponse politique et analytique commune, malgré la diversité des positions entre les États membres.

Abstract

The Radio Access Network (RAN) is the radio part of a mobile telecommunications system that enables the connection between a mobile device (such as a phone or computer) and the core network. While traditionally a single vendor (such as Huawei, Ericsson, or Nokia) provides a « proprietary » or « closed » solution for this part of the network, Open RAN (Open Radio Access Network) is a concept describing disaggregated architectures that divide the RAN into several bricks connected by open interfaces. The objective is to allow the operator to buy these hardware and software bricks from various suppliers, and to choose freely the most suitable option for each part. In the current context of a concentrated 5G market, dominated by three major manufacturers and even facing the risk of an Ericsson-Nokia duopoly with the exclusion of Huawei from many countries, telecom operators emphasize the flexibility and diversification of suppliers allowed by Open RAN, which would allow both more innovation and cost reduction. In line with its diplomatic campaign against « unreliable » Chinese suppliers, the United States has actively promoted Open RAN as an alternative.

However, Open RAN seems far from being a panacea for Europe : in addition to the difficulties that remain in terms of maturity, security, performance and transparency of the specification process, it risks increasing European dependence on foreign suppliers. Although Huawei is not part of the international bodies working on Open RAN (such as the Telecom Infra Project or the O-RAN Alliance), many companies close to the Chinese political and military authorities are. Beyond the question of supplier security, American lobbying is linked to the commercial opportunity that Open RAN represents for American companies, currently leaders in the cloud, software and generic hardware components...even though they do not have a major 5G champion. Open RAN is therefore an issue at the crossroads of the geopolitics of 5G and standards, to which the European Union is beginning to provide a common political and analytical response, despite the diversity of positions among member states.

Sommaire

INTRODUCTION	6
CE QU'EST (ET N'EST PAS) L'OPEN RAN	8
Triple combinaison : virtualisation, automatisation, désagrégation	9
L'ouverture comme « outil discursif » :	
<i>open source, open standards, open RAN</i>.....	11
Promesses et faiblesses de l'Open RAN.....	12
LA PANACÉE POUR REMPLACER HUAWEI ? PARTICIPATION	
CHINOISE ET INTÉRÊTS AMÉRICAINS DANS L'OPEN RAN	15
L'Open RAN : sans Huawei mais pas sans la Chine	15
Intérêts et lobbying américains	17
Dépendances et réactions européennes.....	19
CONCLUSION	22

Introduction

La campagne diplomatique intense de l'administration Trump contre l'équipementier chinois Huawei, commencée dès 2019 et poursuivie par son successeur, a mis en lumière non seulement les risques en matière de sécurité des réseaux mais aussi les enjeux profondément géopolitiques associés au déploiement de la 5G dans le monde. Dans un contexte de nette augmentation du nombre de données transférées par le réseau de téléphonie mobile, de bandes fréquences utilisées et de stations de base déployées¹, trois fournisseurs représentent aujourd'hui plus de 75 % des parts de marché de ce réseau : le chinois Huawei (31 %), le suédois Ericsson (28 %) et le finlandais Nokia (17 %)². Présenté comme une solution permettant de réintroduire davantage de diversité parmi les fournisseurs tout en s'affranchissant des équipementiers chinois à risque, l'Open RAN (*Open Radio Access Network*) est un concept qualifiant des architectures de réseau dont certaines interfaces sont ouvertes, c'est-à-dire les manières d'organiser les équipements matériels et logiciels, les protocoles, etc., en un tout permettant la transmission des données au sein du réseau et vers des applications tierces. Ces nouvelles architectures dites « ouvertes » permettraient ainsi aux opérateurs de ne plus se procurer le tout auprès d'un seul fournisseur, mais de choisir librement pour chaque brique logicielle ou matérielle la solution la plus adaptée. L'Open RAN est promu à la fois par les opérateurs télécoms et par certains acteurs gouvernementaux, en particulier américains.

L'Open RAN est-il vraiment la panacée promise à l'Europe pour se libérer des dépendances aux fournisseurs peu fiables et des risques de duopole ? Quels risques et opportunités présente l'Open RAN pour la souveraineté technologique européenne ?

Il est d'abord nécessaire de revenir sur la définition de l'Open RAN – car celui-ci est à la fois techniquement complexe et souvent noyé dans une rhétorique de l'« ouverture » très floue –, d'examiner les opportunités qu'il promet en matière de coût et d'innovation, et ses apparentes faiblesses sur le plan de la maturité et de la sécurité. En dépit de celles-ci et de la participation d'entreprises chinoises dans l'Open RAN, l'ouverture des réseaux a été fortement soutenue politiquement et financièrement aux États-Unis, et activement promue auprès de leurs alliés. Pour l'Europe, l'Open RAN

Pour la rédaction de ce papier, des entretiens ont été réalisés notamment avec Alix Durand, chargée d'analyses stratégiques à l'Agence nationale de la sécurité des systèmes d'information (ANSSI), le 28 juin 2022.

1. « 5G Scoreboard », European 5G Observatory, janvier 2022, disponible sur : <https://5gobservatory.eu>.

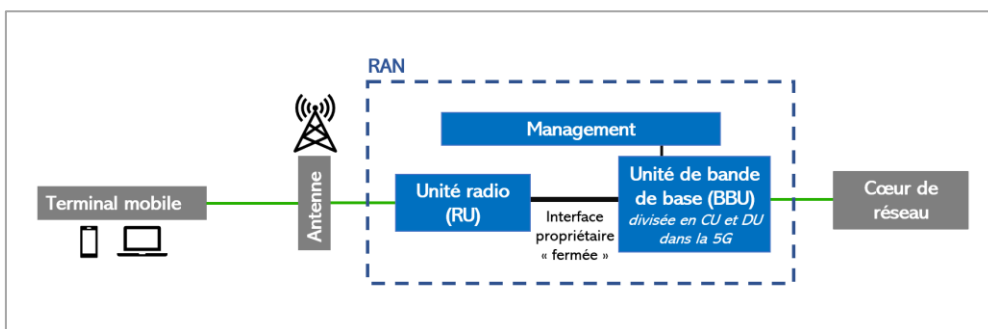
2. Dell'Oro, « World RAN Market Shares Development », 19 mai 2022.

présente toutefois le risque de créer de nouvelles dépendances à des entreprises étrangères, dans un secteur où elle compte, pour l'heure, parmi les principaux concurrents mondiaux.

Ce qu'est (et n'est pas) l'Open RAN

Le réseau d'accès radio (RAN) est la partie radio d'un système de télécommunications mobiles qui permet la connexion entre un terminal (comme un téléphone ou un ordinateur) et le cœur de réseau. En simplifiant, il se compose d'une antenne, d'unités radio (RU) recevant et envoyant les données, et pour la 4G d'unités de bande de base (BBU) – décomposée en unité centralisée (CU) et unité distribuée (DU) pour la 5G – traitant les données et communiquant avec le cœur de réseau de l'opérateur. Traditionnellement, c'est le même équipementier (Huawei, Ericsson, Nokia...) qui fournit une solution dite « propriétaire », ou « fermée ». Dans cette solution, les éléments matériels et logiciels qui composent la RU et la BBU sont imbriqués et non interchangeables, et les deux sont liés par une interface propriétaire. L'ensemble, parfois comparé à une « boîte noire » et représenté en bleu sur le schéma, est assuré par un seul fournisseur. En revanche, les interfaces entre l'antenne et la RU ainsi qu'entre la BBU et le cœur de réseau sont ouvertes et standardisées par le 3rd Generation Partnership Project (3GPP), instance qui réunit sept organisations mondiales développant des standards en matière de télécommunications 3G, 4G et 5G³.

Schéma 1 : l'architecture RAN classique



En vert, les interfaces ouvertes standardisées par le 3GPP.

Comme son nom l'indique, l'Open RAN reflète l'ambition de créer de nouvelles interfaces « ouvertes » entre différentes briques interopérables du réseau d'accès radio.

3. Site du 3GPP, « About 3GPP », disponible sur : www.3gpp.org.

Triple combinaison : virtualisation, automatisation, désagrégation

L'Open RAN peut être défini comme un paradigme d'architecture réseau. Ce n'est ni un standard ni une nouvelle technologie en soi, mais plutôt une combinaison de technologies existantes (intelligence artificielle [IA], composants commerciaux dits « *off-the-shelf* », interfaces ouvertes, *cloud*), au service de trois objectifs : la virtualisation, l'automatisation, et la désagrégation⁴. Il convient de les distinguer car les deux premiers sont en fait des évolutions des réseaux télécoms – qui dépassent l'Open RAN⁵ et suscitent l'adhésion des acteurs industriels – tandis que le troisième suscite davantage de débats et de réticences chez les équipementiers (en particulier Ericsson et Huawei).

La virtualisation, c'est-à-dire la séparation des éléments matériels (*hardware*) et logiciels (*software*), est une tendance de fond dans la 5G en général (et dans une moindre mesure dans les précédentes générations), qui touche à la fois le RAN (dit vRAN pour *virtual RAN*) et le cœur de réseau. La virtualisation permet ainsi de faire fonctionner sur du *hardware* commercial générique, voire dans le *cloud*, des logiciels remplissant les fonctions des équipements télécoms traditionnels⁶.

L'automatisation a pour but de rendre le RAN « intelligent » en remplaçant les tâches manuelles par des fonctionnalités automatisées (notamment grâce au *machine learning*), ce qui permet de réduire les coûts d'exploitation et d'augmenter la performance⁷. Elle est de plus en plus mise en place pour la 5G par les opérateurs (Dish, China Mobile, Vodafone...) comme par les grands équipementiers afin de parvenir à gérer un nombre croissant de données dans un réseau de plus en plus complexe⁸.

Liée à la virtualisation et l'automatisation, la désagrégation est le fait de séparer les fonctions du RAN en différentes briques interopérables. Ces architectures divisées sont déjà fonctionnellement et numériquement plus importantes dans la 5G que pour les générations antérieures, et certaines ont

4. H. Lee-Makiyama, « Open RAN: The Technology, its Politics and Europe's Response », *ECIPE Policy Brief*, n° 8, European Centre for International Political Economy, 2020 ; « Report on the Cybersecurity of Open RAN », NIS Cooperation Group, 11 mai 2022, p. 4, disponible sur : <https://ec.europa.eu>.

5. « Report on the Cybersecurity of Open RAN », *op. cit.*

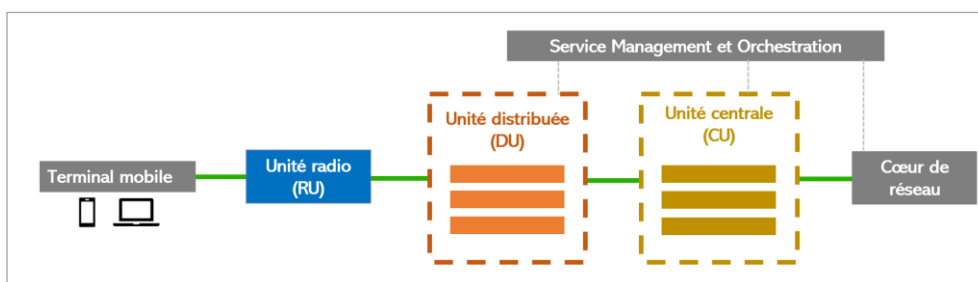
6. R. Loukhil, « L'Europe face à la révolution Open RAN », *L'Usine Nouvelle*, n° 3707, juin 2022 ; R. Loukhil, « Le Royaume-Uni sonne la migration de ses réseaux mobiles vers la technologie Open RAN », *L'Usine Nouvelle*, 26 février 2022 ; H. Lee-Makiyama, « Open RAN: The Technology, its Politics and Europe's Response », *op. cit.* ; S. Dumoulin, « Les équipementiers alternatifs ont le vent en poupe », *Les Échos*, 17 juin 2021.

7. S. Pongratz, « The Role of Intelligent RAN and Automation », Dell'oro Group, 15 juin 2022, disponible sur : www.delloro.com ; « Ericsson Intelligent RAN Automation », Ericsson, 25 août 2022, disponible sur : www.ericsson.com.

8. *Ibid* ; Laurent Leboucher cité dans J. Taaffe, « How Orange's CTO Is Driving Network Transformation », Inform, janvier 2022, disponible sur : <https://inform.tmforum.org>.

déjà été normalisées par le 3GPP⁹. La proposition de l'Open RAN est d'aller encore plus loin en proposant une dizaine de nouvelles interfaces ouvertes entre les briques, par exemple entre l'unité radio (RU) et l'unité distribuée (DU).

Schéma 2 : architecture « ouverte »



En vert, les interfaces ouvertes normalisées par les standards 3GPP ou les spécifications O-RAN.

L'objectif est ainsi de permettre à l'opérateur d'acheter ces briques matérielles et logicielles à des fournisseurs variés, de choisir pour chaque brique l'option la plus performante en panachant librement les solutions différentes. L'interopérabilité entre les briques est assurée par les spécifications complémentaires (et dépendantes) des standards développés par le 3GPP : les spécifications développées par l'Alliance O-RAN¹⁰.

L'Alliance O-RAN a été fondée en 2018 par cinq grands opérateurs mobiles (AT&T, China Mobile, Deutsche Telekom, NTT Docomo et Orange) – qui y gardent une place prépondérante – spécifiquement pour « re-façonner l'industrie RAN vers des réseaux mobiles plus intelligents, ouverts, virtualisés et totalement interopérables¹¹ ». Les principales missions de cette alliance s'articulent autour de trois axes : proposer des spécifications pour l'Open RAN, développer des logiciels pour le RAN (*O-RAN Software Community*), et soutenir les tests et intégration des solutions Open RAN¹². Cette alliance collabore avec le Telecom Infra Project (TIP), un consortium industriel avec un groupe dédié à l'accélération de l'innovation et de la commercialisation de solutions Open RAN.

9. Comme celle divisant l'unité de bande de base (BBU) en deux unités, l'unité distribuée (DU) et l'unité centrale (CU), définie par la 3GPP Release 15. Voir « Study on CU-DU Lower Layer Split for NR », *3GPP Technical Report* 38.816, 2017, disponible sur : <https://portal.3gpp.org> et O. Andersson, « Functional Splits: The foundation of an Open 5G RAN », *5G Technology World*, 17 mai 2021, disponible sur : www.5gtechnologyworld.com.

10. R. Layton, « OpenRAN: American Trade Policy Masquerading As Security », *Forbes*, 3 décembre 2021.

11. « About Us », O-RAN Alliance, disponible sur : www.o-ran.org.

12. *Ibid.*

L'ouverture comme « outil discursif » : *open source, open standards, open RAN*

L'une des difficultés liée à la compréhension de l'Open RAN est l'utilisation du concept d'ouverture comme « outil discursif » par l'industrie et les acteurs gouvernementaux assurant sa promotion¹³. Celle-ci crée en effet un imaginaire associé à la transparence, la confiance et la liberté – par opposition aux « boîtes noires » que sont les solutions propriétaires – et amalgame souvent trois réalités différentes :

- ▀ les interfaces ouvertes (c'est-à-dire non propriétaires) entre les briques du réseau,
- ▀ l'open source,
- ▀ les « standards ouverts¹⁴ ».

Comme expliqué précédemment, l'Open RAN implique effectivement la création de davantage d'interfaces ouvertes, c'est-à-dire permettant l'interopérabilité entre les briques du réseau, par opposition à une interface propriétaire dite « fermée ». Dans l'Open RAN, mais aussi plus largement dans des réseaux virtualisés et/ou dans le *cloud*, certaines de ces briques peuvent être composées de logiciels libres développés collectivement – l'Alliance O-RAN travaille d'ailleurs en coopération avec la Fondation Linux afin de développer des logiciels *open source* pour le RAN¹⁵. Mais la plupart des composants de l'Open RAN restent toutefois des technologies propriétaires¹⁶.

Enfin, l'argumentaire autour des « standards ouverts » de l'Open RAN est ambigu. Ce terme est utilisé pour désigner les décisions techniques standardisant les interfaces ouvertes. Toutefois, dans le cas de l'Alliance O-RAN, le processus lui-même par lequel sont élaborées ces spécifications est peu ouvert. Son manque de transparence a d'ailleurs été critiqué dans le rapport de l'agence européenne de cybersécurité¹⁷, d'une part car les spécifications O-RAN ne sont pas toutes publiquement disponibles, et d'autre part car le processus de développement des spécifications ne respecte pas les principes fondateurs de l'Organisation mondiale du commerce (OMC) sur le développement des standards internationaux¹⁸.

13. J.-C. Plantin, « The Geopolitical Hijacking of Open Networking », *European Journal of Communication*, vol. 36, n° 4, 2021.

14. Termes utilisés par exemple dans : « O-RAN Alliance Conducts First Global Plugfest to Foster Adoption of Open and Interoperable 5G Radio Access Networks », O-RAN Alliance, 19 décembre 2019, disponible sur : <https://www.o-ran.org> ; Open RAN Policy Coalition, « Open RAN Policy Coalition Releases New Policy Roadmap », 1^{er} décembre 2020, disponible sur : www.openranpolicy.org ; M. Rasser et A. Riikonen, « Open Future: The Way forward on 5G », Center for a New American Security, 28 juillet 2020.

15. « About Us », O-RAN Alliance, disponible sur : www.o-ran.org.

16. J.-C. Plantin, « The Geopolitical Hijacking of Open Networking », *op. cit.*

17. « Report on the Cybersecurity of Open RAN », *op. cit.*, p. 14.

18. Principes élaborés en 2000 par le Comité sur les barrières techniques au commerce (Technical Barriers to trade, TBT) de l'Organisation mondiale du commerce : « Principes devant régir l'élaboration de normes, guides et recommandations internationaux », Organisation mondiale du commerce, disponible sur : www.wto.org.

Promesses et faiblesses de l'Open RAN

Plus de diversité pour plus d'innovation à moindre coût ?

Dans un contexte de concentration du marché 5G, dominé par trois grands équipementiers, voire de risque de duopole Ericsson-Nokia avec l'exclusion de Huawei de nombreux pays, les opérateurs télécoms soulignent la flexibilité et la diversification des fournisseurs permise par l'Open RAN¹⁹. Les interfaces ouvertes permettent à de nouveaux acteurs d'entrer sur le marché en proposant des solutions sur certaines briques, et aux opérateurs de mettre en concurrence les fournisseurs en se libérant des contraintes liées aux ensembles de technologies propriétaires des grands équipementiers. Cet environnement 5G plus compétitif fournirait ainsi des solutions plus innovantes et moins coûteuses, alors que la domination du marché par un petit nombre d'entreprises est accusée d'être responsable de prix élevés et d'une innovation lente²⁰. Ces avantages se cumulent avec ceux de la virtualisation et de l'automatisation : utilisation d'équipements matériels génériques moins coûteux, mutualisation des ressources, maintenance facilitée et simplifiée, adaptation plus rapide et meilleure résilience du réseau, etc.²¹

Toutefois, l'Open RAN n'est pas considéré comme une solution mature à court terme²². L'intégration de toutes ces briques désagrégées est à la fois techniquement complexe et coûteuse²³. Comme le soulignent certains opérateurs et équipementiers, il n'est pas sûr que les opérateurs choisiront de multiplier le nombre de fournisseurs par site, ni que ce système permettra des économies conséquentes²⁴.

De nombreux acteurs remettent également en question les améliorations de performance promises par l'ouverture de nouvelles interfaces. Le matériel dit « *commercial off-the-shelf* » n'est en effet pas

19. Voir par exemple : Deutsche Telekom, Orange, Telefónica et Vodafone, « Memorandum of Understanding on the Implementation of Open RAN Based Networks in Europe », janvier 2021.

20. *Ibid* ; D. Rinaldo, « Leading the Wireless Future: Securing American Network Technology », audience devant la Chambre des Représentants, 21 avril 2021.

21. J. Taaffe, « How Orange's CTO Is Driving Network Transformation », *Inform*, janvier 2022 ; R. Loukhal, « Le Royaume-Uni sonne la migration de ses réseaux mobiles vers la technologie Open RAN », *op. cit.* ; H. Lee-Makiyama, « Open RAN: The Technology, its Politics and Europe's Response », *op. cit.*

22. J.-C. Plantin, « The Geopolitical Hijacking of Open Networking », *op. cit.* ; C. Sbeglia Nin, « Open RAN Reality Check: "We Don't Have Open RAN, We Have Highly Coordinated RAN" », *RCR Wireless News*, 27 mai 2022, disponible sur : www.rcrwireless.com ; R. Loukil, « L'Europe va-t-elle rater le coche de la révolution Open RAN des réseaux mobiles », *L'Usine Nouvelle*, 30 mars 2022.

23. Entretien avec Viktor Arvidsson, directeur de la stratégie et des affaires publiques d'Ericsson France, Paris, 30 mai 2022 ; R. Loukil, « L'Europe va-t-elle rater le coche de la révolution Open RAN des réseaux mobiles », *op. cit.* ; H. Lee-Makiyama et R. Baker, « TTC and Pre-Emptying the Next Transatlantic Tech War », mai 2022, disponible sur : <https://ecipe.org>.

24. *Ibid.* ; « Nokia's Mobile Chief: Open RAN Progress Is Too Slow, Implementation Complex and Costly », *Communications Day*, n° 6397, 16 mai 2022 ; I. Morris, « BT Takes Aim at Open RAN Myths », *LightReading*, 12 novembre 2021, disponible sur : www.lightreading.com.

encore capable de rivaliser en matière de performance (y compris énergétique) avec les composants électroniques des solutions propriétaires, optimisés pour leurs tâches spécifiques²⁵. Cet enjeu de l'efficacité énergétique sera déterminant pour l'Open RAN²⁶. Plus largement, la version actuelle des spécifications sur les interfaces ouvertes contraint les fonctions réalisables de chaque côté de l'interface (au niveau de la RU et la DU par exemple), ce qui peut affecter la performance du réseau²⁷.

Enfin, certains doutent de la possibilité pour l'Open RAN – dont la place sur le marché mondial des réseaux d'accès radio est estimée à 15 % d'ici 2026 – de transformer celui-ci en profondeur. Les raisons expliquant la consolidation du secteur (en particulier les coûts d'entrée élevés en matière de capital et d'expertise) restent déterminantes et pourraient se traduire dans l'Open RAN par une re-consolidation avec le rachat des petits acteurs par les grands²⁸.

Cybersécurité : plus de risques que d'opportunités

Dans un contexte de menace cyber croissante, les enjeux de sécurité sont au cœur des débats sur la 5G. Les tendances générales à la virtualisation et automatisation présentent déjà en elle-même certaines opportunités en matière de cybersécurité. Par exemple, en réduisant le nombre d'interventions de l'homme, l'automatisation diminue les risques liés à l'erreur humaine²⁹. En plus des avantages en matière de cybersécurité liés à la virtualisation et l'automatisation, l'Open RAN présente certaines opportunités sécuritaires par la désagrégation qu'il propose. Disposer d'un grand nombre de fournisseurs permet de réduire les risques liés à la dépendance à un seul d'entre eux, et crée un cloisonnement contribuant à la résilience du réseau³⁰. La présence d'interfaces ouvertes standardisées, l'accès facilité aux données de performance et l'utilisation de logiciels *open source* peuvent favoriser la visibilité et la transparence sur le fonctionnement du réseau, notamment pour les autorités nationales et auditeurs de sécurité³¹.

Toutefois, plusieurs rapports officiels ont pointé du doigt les risques sécuritaires liés à l'Open RAN sous sa forme actuelle. L'agence européenne de cybersécurité souligne notamment que l'Open RAN accroît les risques

25. H. Lee-Makiyama, « Open RAN: The Technology, its Politics and Europe's Response », *op. cit.* ; R. Loukil, « L'Europe va-t-elle rater le coche de la révolution Open RAN », 30 mars 2022, *op. cit.*

26. Entretien avec un responsable d'un opérateur français, 22 juin 2022.

27. Entretien avec Viktor Arvidsson, 30 mai 2022 ; « Report on the Cybersecurity of OpenRAN », 2022, *op. cit.*

28. P. Cohen. « Open RAN Will Have 15 % Market Share by 2026, Report », *RCR Wireless News*, 24 janvier 2022, disponible sur : www.rcrwireless.com ; S. P. Crawford, *Captive Audience: The Telecom Industry and Monopoly Power in the New Gilded Age*, New Haven, Yale University Press, 2013 ; M. Dinges *et. al.*, « 5G Supply Market Trends: Final Report », European Commission, 2021.

29. « Report on the Cybersecurity of Open RAN », 2022, *op. cit.*, p. 11.

30. « Report on the Cybersecurity of Open RAN », 2022, *op. cit.*

31. *Ibid.*, p. 10 ; *Open RAN Security in 5G*, Open RAN Policy Coalition, avril 2021.

déjà existants de mauvaise configuration des réseaux et de vulnérabilité de composants de faible qualité provenant d'une variété de fournisseurs³².

La multiplication des interfaces ouvertes et des fournisseurs crée également de nouveaux risques sécuritaires. Elle présente davantage d'opportunités pour des cyberattaquants : comme l'écrit une agence gouvernementale américaine, « la surface d'attaque du réseau est considérablement étendue³³ ». Elle s'accompagne en outre de vulnérabilités liées à une chaîne d'approvisionnement complexe, avec de potentiels vendeurs peu fiables dont l'examen devient difficile. Les spécifications de l'O-RAN Alliance ont également été pointées du doigt car le processus de développement ne place pas au centre le principe de « sécurité par design/défaut³⁴ ». En plus des problèmes de performance précédemment évoqués, les équipementiers comme Ericsson ont mis en avant ces vulnérabilités en matière de sécurité de l'Open RAN et en particulier des spécifications de l'O-RAN Alliance, tout en contribuant aux travaux de l'Alliance sur la sécurité pour y remédier³⁵.

D'autres mettent en garde quant à l'utilisation de logiciels *open source* ou développés en commun, comme c'est le cas dans la Communauté logicielle de l'Alliance O-RAN, qui permet à de potentiels acteurs non fiables d'accéder aux informations (et vulnérabilités) du code et de contribuer à son développement³⁶.

L'Open RAN pose donc des problèmes de sécurité à court et moyen termes, auxquels tente de répondre le *Security Focus Group* de l'Alliance O-RAN, devenu un groupe de travail à part entière (le 11^e) en juin 2022³⁷. Pour l'Europe, l'Open RAN crée également un risque de dépendance accrue aux fournisseurs étrangers, en particulier chinois et américains.

32. « Report on the Cybersecurity of Open RAN », 2022, *op. cit.*

33. *Ibid.*, p. 8 ; « Technology Assessment: 5G Wireless, Capabilities and Challenges for an Evolving Network », U.S. Government Accountability Office, novembre 2020 ; voir aussi « Open Radio Access Network Security Considerations », U.S. Cybersecurity and Infrastructure Security Agency (CISA) et National Security Agency (NSA), 15 septembre 2022, disponible sur : www.cisa.gov.

34. S. Köpsell *et. al.*, « Open-RAN Risikoanalyse », Bundesamt für Sicherheit in der Informationstechnik, 21 février 2022.

35. Entretien avec René Summer, directeur des relations avec le gouvernement et l'industrie au sein du groupe Ericsson, 22 juin 2022.

36. J.-P. Kleinans et T. Rühlig, « The False Promise of Open RAN », *Digital Power China*, août 2022 ; H. Lee-Makiyama, « Open RAN: The Technology, its Politics and Europe's Response », *op. cit.*

37. « O-RAN ALLIANCE Introduces 52 New Specifications Released since March 2022 », Alliance O-RAN, 29 août 2022, disponible sur : www.o-ran.org.

La panacée pour remplacer Huawei ? Participation chinoise et intérêts américains dans l'Open RAN

Dans la lignée de la campagne diplomatique des États-Unis visant à dissuader leurs partenaires de recourir aux fournisseurs 5G chinois jugés non fiables tels que Huawei et ZTE, Washington a activement promu l'Open RAN comme alternative. Pourtant, un grand nombre d'entreprises chinoises ont aussi investi l'Open RAN depuis ses débuts. Comment expliquer cette apparente contradiction ?

L'Open RAN : sans Huawei mais pas sans la Chine

Comme ne manquent pas de le souligner certains acteurs américains, Huawei ne fait partie ni de l'Alliance O-RAN ni du Telecom Infra Project³⁸. Toutefois, de nombreux autres fournisseurs et opérateurs chinois sont membres de ces instances, et la participation d'entités chinoises dans les autres organisations internationales de standardisation de l'Open RAN comme le 3GPP s'est accrue ces dernières années³⁹.

L'Alliance O-RAN résulte initialement de la fusion de deux organisations, le forum X-RAN dominé par des Américains et Européens, et l'Alliance C-RAN établie par China Mobile⁴⁰. China Mobile, le plus grand opérateur public chinois, est même l'un des cinq membres fondateurs de l'Alliance O-RAN. Il dispose de sièges permanents au conseil d'administration ainsi que de droits de veto, et co-préside dix de ses quatorze groupes de travail⁴¹. Au total, avec 44 membres en 2021, la Chine est le pays avec le second plus grand nombre de membres dans l'Alliance O-RAN derrière les États-Unis. Au moins deux tiers de ces membres chinois sont partiellement ou totalement détenus par l'État, et 16 ont des liens officiels

38. M. Rasser et A. Riikonen, *Open Future: The Way forward on 5G*, *op. cit.*

39. A. Bondaz, « Promouvoir la “connectivité immatérielle” : réformes et ambitions internationales de la Chine en matière de normalisation », *Recherches & Documents*, n° 14, septembre 2021.

40. J. Leen, Eric Zhang et R. Creemers, « China Standardisation System – Trends, Implications and Case Studies in Emerging Technologies », Leiden Asia Center, avril 2022 ; H. Lee-Makiyama, « Open RAN: The Technology, its Politics and Europe's Response », *op. cit.*

41. H. Lee-Makiyama, « China's Participation in O-RAN », European Centre for International Political Economy, janvier 2022.

avec des activités militaires ou de sécurité⁴². L'Alliance compte même de nombreuses entreprises chinoises sous sanctions américaines (parfois en raison de leurs liens avec le Parti communiste chinois ou l'armée), telles que Inspur⁴³, SMIC, Kindroid, Phytium, H3C⁴⁴, et les trois opérateurs publics China Mobile, China Telecom et China Unicom⁴⁵. Cela a même conduit Nokia à suspendre temporairement sa participation à l'Alliance O-RAN en août 2021, par peur d'enfreindre les restrictions américaines en échangeant avec ces entreprises. Outre les spécifications, les entreprises chinoises sont également investies dans le développement du code *open source* qui peut être utilisé pour l'Open RAN : Huawei était ainsi le 5^e contributeur et membre du comité directeur (de 2017 à 2019) de la plateforme Kubernetes, et Huawei et Tencent font partie du conseil d'administration de la Fondation Linux, partenaire de l'Alliance O-RAN pour le développement de code⁴⁶.

Or, les reproches adressés à Huawei concernant son traitement préférentiel par les autorités chinoises et ses liens étroits avec celles-ci s'appliquent également (voire davantage) à un très grand nombre d'entreprises chinoises des télécoms⁴⁷. Pékin pourrait ainsi utiliser les mêmes outils (subventions, accès au marché privilégié...) pour soutenir les fournisseurs chinois d'équipements Open RAN critiques, créant une situation de concentration semblable à la situation actuelle du marché RAN propriétaire. De fait, selon Kleinhans et Rühlig, « les considérations stratégiques des *think tanks* chinois dirigés par l'État en Chine suggèrent que le pays voit l'Open RAN comme une opportunité de contourner les sanctions américaines⁴⁸ ».

L'Open RAN ne semble donc pas être une solution automatique pour atténuer les possibles dangers liés aux fournisseurs à risque ou la dépendance excessive aux technologies chinoises. Il a pourtant été vigoureusement promu par les acteurs industriels et politiques américains.

42. *Ibid.*

43. Sur la liste des « entreprises chinoises communistes militaires » du département de la Défense américain. Voir « Timeline of Executive Actions on China », U.S.-China Economic and Security Review Commission, 1^{er} avril 2021, disponible sur : www.uscc.gov.

44. Tous les quatre sur la liste d'Entités du département du Commerce américain. « Supplement No. 4 to Part 744 – Entity List », Bureau of Industry and Security, 24 août 2022, disponible sur : www.bis.doc.gov.

45. Tous les trois sur la liste des « entreprises du complexe militaro-industriel chinois » du département du Trésor américain. « Introduction of Non-SDN Chinese Military-Industrial Complex Companies List », U.S. Department of the Treasury, 3 juin 2021, disponible sur : <https://home.treasury.gov>.

46. R. Layton, « OpenRAN: American Trade Policy Masquerading As Security », *Forbes*, 3 décembre 2021 ; « Board of Directors », The Linux Foundation, disponible sur : www.linuxfoundation.org.

47. R. Layton, « Efforts to Make 5G More 'Open' With Less Huawei Have Attracted Dozens of Chinese Vendors », *Forbes*, 17 décembre 2020.

48. J.-P. Kleinhans et T. Rühlig, « The False Promise of Open RAN », *op. cit.*, p. 12-13. ; voir aussi J. Leen, E. Zhang et R. Creemers, *China Standardisation System*, *op. cit.*, p. 19.

Intérêts et lobbying américains

Outre l'objectif d'exclure Huawei des réseaux, l'Open RAN est également explicitement conçu par les industriels, politiciens, et chercheurs outre-atlantique comme une « opportunité pour le leadership technologique américain⁴⁹ », en l'absence de grand champion américain des équipements 5G. Comme l'écrit John Baker, vice-président du développement commercial chez Mavenir, « [v]oilà la réalité : le meilleur moyen de prioriser le leadership américain dans la 5G est de créer des politiques qui priorisent l'Open RAN⁵⁰ ». L'Open RAN fait en effet évoluer la chaîne de valeur de la 5G autour des points forts des entreprises américaines, tant dans le *software* que le *hardware*⁵¹.

L'importance du logiciel et de la virtualisation, au cœur de l'Open RAN, joue sur les forces américaines. Le marché du *cloud*, indispensable dans la virtualisation et *cloudification* des réseaux, est en effet dominé par les grandes entreprises américaines comme Amazon Web Services, Google, Microsoft Azure ou Oracle, dont l'importance dans les télécoms au sens large et dans les projets Open RAN en particulier semble devoir croître. Ces entreprises promeuvent d'ailleurs l'Open RAN, notamment à travers leur participation dans l'Alliance O-RAN et l'Open RAN Policy Coalition⁵². De même, les nouveaux fournisseurs leaders dans les solutions logicielles clé pour l'Open RAN, comme Mavenir, Parallel Wireless, ou Altostar⁵³, sont américains. L'utilisation d'équipements matériels génériques (et non plus dédiés) représente également une opportunité pour les fabricants américains de ces composants, comme Dell, Intel ou Qualcomm⁵⁴.

Ces opportunités expliquent le fort soutien politique et financier des acteurs gouvernementaux américains en faveur de l'Open RAN. Le rapport publié en 2021 par la National Telecommunications and Information Administration (NTIA) au nom de tout le gouvernement américain annonce ainsi explicitement que « la branche exécutive soutient pleinement le développement de l'Open RAN par l'industrie⁵⁵ » et incite la Commission fédérale pour les communications (FCC) à prendre des mesures facilitatrices. Ce soutien a d'ailleurs été exprimé séparément à la fois par le département

49. M. Rasser et A. Riikonen, *Open Future: The Way forward on 5G*, op. cit.

50. J. Baker, « It's Time to Prioritize American Mobile Technology », Mavenir, 24 mars 2021, disponible sur : <https://medium.com>.

51. B. Clark et D. Patt, « Weaponizing the 5G Value Chain: A Two-Pronged Strategy to Establish America's Lead in Next-Generation Telecommunications », Hudson Institute, septembre 2020.

52. Amazon, Google, Microsoft et Oracle font toutes les quatre parties de ces organisations. Voir « Members », Open RAN Policy Coalition, disponible sur : www.openranpolicy.org et « O-RAN Companies », Alliance O-RAN, disponible sur : www.o-ran.org.

53. Racheté par le japonais Rakuten en 2021.

54. R. Loukil, « Pourquoi Qualcomm rachète Cellwize, une pépite des réseaux mobiles Open RAN », *L'Usine Nouvelle*, 13 juin 2022.

55. « NTIA Comments on Promoting the Deployment of 5G Open Radio Access Networks », National Telecommunications and Information Administration, 16 juillet 2021, disponible sur : www.ntia.gov.

du Commerce (dont fait partie la NTIA), le département d'État⁵⁶, le département de la Défense⁵⁷, et même la Central Intelligence Agency (CIA), qui a investi dans Parallel Wireless *via* son fonds de capital-risque In-Q-Tel⁵⁸.

La proximité avec l'administration de l'Open RAN Policy Coalition, créée en mai 2020 pour « éduquer les politiciens » et faire du lobbying en faveur de l'Open RAN (principalement aux États-Unis), est également évidente : la directrice exécutive est Diane Rinaldo, ancienne administratrice de la NTIA et Secrétaire adjointe pour les Communications et l'Information au département du Commerce (2018-2020). Contrairement à l'O-RAN Alliance, cette coalition inclut principalement des acteurs américains (y compris les géants susmentionnés AWS, Google, Meta, Microsoft...) mais aucune entreprise chinoise⁵⁹.

Ce lobbying semble avoir porté ses fruits : le Congrès américain a manifesté un soutien bipartisan à l'Open RAN en votant plusieurs lois en ce sens. Le *Secure and Trusted Communications Networks Act* de 2019 alloue 1,9 milliard de dollars à un programme permettant aux opérateurs de remplacer les équipements à risque dans les réseaux télécoms, ouvrant la porte à l'utilisation de l'Open RAN à la place⁶⁰. D'autres législations attribuent plus directement des subventions à l'Open RAN, comme la loi *Utilizing Strategic Allied (USA) Telecommunications Act*⁶¹ qui crée un fonds de 750 millions de dollars (de 2021 à 2031) pour soutenir le déploiement de l'Open RAN aux États-Unis, et le *CHIPS and Science Act* d'août 2022 qui alloue 1,5 milliard de dollars à ce fond⁶².

Outre ces encouragements au déploiement de l'Open RAN sur le sol américain, les administrations Trump et Biden ont également mené une campagne diplomatique soutenue en ce sens auprès de leurs alliés. Celle-ci s'est déployée à la fois en bilatéral et dans des instances plurilatérales, comme la Conférence de Prague sur la Sécurité 5G⁶³, le G7⁶⁴, ou le Conseil UE-US pour le Commerce et les Technologies (TTC)⁶⁵. Washington bénéficie

56. Voir par exemple le discours du Secrétaire d'État Mike Pompeo au Forum on 5G Open Radio Access Network, le 14 septembre 2020, disponible sur : www.fcc.gov ; ou plus récemment : « Joint Statement of the U.S.-Japan Economic Policy Consultative Committee: Strengthening Economic Security and the Rules-Based Order », Office of the Spokesperson, 29 juillet 2022, disponible sur : www.state.gov.

57. K. Stacey, « Pentagon Wants Open-Source 5G Plan in Campaign against Huawei », *Financial Times*, 22 décembre 2019.

58. M. Rasser et A. Riikonen, *Open Future: The Way forward on 5G*, *op. cit.*

59. « Open RAN: A Year in Review », Open RAN Policy Coalition, 3 mai 2021, disponible sur : www.openranpolicy.org.

60. T. Maupile, « The Role of Legislative Policy Initiatives in Open RAN », Altiostar, 30 mars 2021, disponible sur : www.altiostar.com.

61. Adopté au sein du *National Defense Authorization Act* adopté le 1^{er} janvier 2021, section 9202.

62. *CHIPS and Science Act of 2022*, division A, 9 août 2022.

63. Voir par exemple le discours du président de la FCC Ajit Pai : A. Pai, « Remarks to the Prague 5G Security Conference », 24 septembre 2020, disponible sur : <https://docs.fcc.gov>.

64. Entretien avec un acteur privé du numérique européen, mai 2022.

65. Propos tenus sous la règle de Chatham House, 2022.

dans cette démarche du soutien de Londres, qui voit en l'Open RAN une opportunité pour ses entreprises (et pour sa « relation spéciale » avec les États-Unis), ainsi qu'une possibilité de s'affranchir de sa forte dépendance envers les équipements Huawei sans devenir trop dépendant d'Ericsson et Nokia.

Assez intense pour être qualifiée de « détournement géopolitique des réseaux ouverts⁶⁶ », de « politique commerciale américaine déguisée en [politique de] sécurité⁶⁷ », voire de « forçing⁶⁸ », celle-ci a été reçue de façon mitigée en Europe.

Dépendances et réactions européennes

Face à l'enthousiasme américain, japonais, britannique, et des opérateurs européens⁶⁹, l'Union européenne (UE) a adopté une position prudente sur l'Open RAN, tout en promouvant plus de diversité et de sécurité dans les télécoms. Outre les questions précédemment évoquées concernant la maturité, la performance et la sécurité de la 5G ouverte, cette position s'explique par les risques, inhérents à l'Open RAN, d'exacerbation des dépendances européennes.

En effet, si pour l'Europe l'Open RAN présente certaines opportunités (notamment pour les opérateurs, et pour certains nouveaux acteurs fournissant des solutions matérielles ou logicielles), le risque est double⁷⁰. D'une part, bien qu'engagés dans les discussions sur l'Open RAN, les champions européens Nokia et Ericsson, fournisseurs de solutions propriétaires, pourraient perdre des parts de marché significatives avec cette nouvelle architecture et l'entrée de nouveaux acteurs. D'autre part, il est fort probable que ces acteurs soient en majorité non européens : si l'Open RAN joue sur les points forts américains, il attire l'attention sur les faiblesses européennes, notamment dans les marchés de services et de logiciels.

La tendance à la virtualisation, qui dépasse l'Open RAN, soulève déjà des questions quant au rôle croissant dans les télécoms des géants de l'internet américains, qui peuvent tirer parti de leurs capacités en matière de *cloud* et *edge computing* et de logiciels⁷¹. Si les partisans de l'Open RAN soulignent la possibilité de faire entrer de nouveaux petits acteurs sur le marché, le risque est que ce soit surtout les *hyperscalers* non européens, présents dans l'Alliance O-RAN et l'Open RAN Policy Coalition, qui

66. J.-C. Plantin, « The Geopolitical Hijacking of Open Networking: The Cas of Open RAN », *op. cit.*

67. R. Layton, « OpenRAN: American Trade Policy Masquerading As Security », *Forbes*, 3 décembre 2021.

68. R. Loukhal, « L'Europe face à la révolution Open RAN », juin 2022, *op. cit.*

69. « Europe Urged to Act Now to Build Open Ran Ecosystem », Memorandum of Understanding, Deutsche Telekom, Orange, Telecom Italia, Telefónica et Vodafone, novembre 2021, disponible sur : <https://media.orange.com>.

70. M. Dinges *et. al.*, « 5G Supply Market Trends: Final Report », 2021, *op. cit.*

71. Leur rôle pourrait toutefois être contraint par les exigences européennes et surtout les réglementations nationales en matière de sécurité des réseaux de télécommunications (comme, en France, l'article R226 du Code pénal).

bénéficient de cette ouverture grâce à leurs capacités d'innovation... et de consolidation⁷². Pour proposer des alternatives aux *hyperscalers*, les opérateurs comme Orange réclament des solutions « *telco cloud* » européennes⁷³, avec des composants *open source*, dont la concrétisation semble encore assez incertaine.

Outre les géants du *cloud*, l'Open RAN risque d'accroître les dépendances européennes dans le *hardware* comme dans le *software*. Comme le résume *L'Usine Nouvelle*, « contrairement aux États-Unis, qui disposent d'un écosystème complet, des puces jusqu'aux services d'intégration, avec une pléthore d'acteurs émergents, l'Europe souffre d'une présence partielle, concentrée sur les matériels radios, et du manque de nouveaux acteurs dans le logiciel Open RAN⁷⁴ ». Ces nouveaux acteurs – qui incluent par exemple l'entreprise belge AccelleRAN – sont beaucoup moins nombreux que leurs concurrents (13 contre 57 ailleurs dans le monde) et encore en phase d'expérimentation. En conséquence, même les opérateurs européens ont commencé le déploiement de l'Open RAN dans leurs réseaux principalement avec des fournisseurs étrangers : l'espagnol Telefonica a ainsi fait appel au japonais NEC et aux américains Altostar, Mavenir et Airspan, Deutsche Telekom à Fujitsu, NEC et Mavenir, et Telecom Italia Mobile à JMA Wireless et Mavenir⁷⁵. Les opérateurs comme Orange et Vodafone soulignent leur objectif de « faire émerger en Europe un écosystème Open RAN comparable à ceux qui existent aux États-Unis, au Japon et en Corée du Sud » – et demandent pour cela plus de soutien politique et industriel de la part de la Commission européenne et des États membres⁷⁶. Certains opérateurs ont même encouragé, sans succès à ce jour, les autorités américaines à travailler avec leurs homologues européens pour développer des opportunités de financement pour le développement d'un écosystème européen, notamment *via* le TTC, pour tenter de convaincre Bruxelles d'adhérer à l'Open RAN⁷⁷. Au vu de son retard, développer cet écosystème européen paraît toutefois long et coûteux, et les acteurs non européens seront probablement les premiers bénéficiaires d'une ouverture des réseaux⁷⁸.

Couplés aux préoccupations techniques, ces éléments expliquent la position mesurée de la Commission européenne sur l'Open RAN. Comme elle l'avait fait en publiant la « Boîte à outils pour la sécurité des réseaux 5G », la Commission se dote de ses propres outils d'analyse pour construire une

72. Voir par exemple le rachat de la *start-up* allemande MobicEdgeX par Google : R. Karayan, « Edge Computing : Google Cloud rachète MobicEdgeX », *L'Usine Digitale*, 3 mai 2022, disponible sur : www.usine-digitale.fr ; ou I. Morris, « Prickly Deutsche Telekom Boss Wants Hyperscaler Deals Curbed », *LightReading*, 16 novembre 2021, disponible sur : www.lightreading.com.

73. J. Taaffe, « How Orange's CTO Is Driving Network Transformation », *Inform*, janvier 2022.

74. R. Loukil, « L'Europe va-t-elle rater le coche de la révolution Open RAN des réseaux mobiles », *op. cit.*

75. *Ibid.*

76. Michaël Trabbia, directeur de l'innovation chez Orange, cité dans R. Loukil, « Comment Orange se prépare à la révolution Open RAN des réseaux mobiles », *L'Usine Nouvelle*, 14 mars 2022 ; N. Fildes, « Vodafone Taps Japan and US to Fill Huawei Gap », *Financial Times*, 15 juin 2021.

77. Conversation avec un acteur privé européen de l'industrie télécom, 7 septembre 2022.

78. M. Dinges *et. al.*, « 5G Supply Market Trends: Final Report », 2021, *op. cit.*

approche concertée et répondre aux incitations et inquiétudes soulevées par Washington : les rapports précédemment cités (sur les tendances du marché dans la 5G en 2021 ou sur la cybersécurité de l'Open RAN, en mai 2022)⁷⁹ en sont l'illustration. En outre, au vu de priorités et de considérations divergentes en matière de sécurité et d'efficacité entre l'Europe et les États-Unis, des représentants européens ont indiqué qu'ils ne céderaient pas au lobbying américain sur l'Open RAN, sans toutefois que cela ne bloque les autres discussions sur la 5G au sein du Conseil pour le commerce et les technologies⁸⁰.

Derrière cette position commune affichée par la Commission européenne, les approches des États membres sur l'Open RAN varient, en fonction de divers facteurs : influence des principaux opérateurs mobiles du pays, dépendance aux équipements Huawei, relations avec la Chine et les États-Unis... Un exemple intéressant est l'Allemagne, sans doute l'un des pays européens les plus favorables à l'Open RAN : le gouvernement allemand a annoncé un investissement de 300 millions d'euros dans l'Open RAN en juin 2021, et soutient plusieurs centres d'excellence et projets de déploiement (dont une « ville Open RAN⁸¹ »). Si l'influence de Deutsche Telecom à Berlin n'y est sans doute pas pour rien, cette position s'explique surtout par la dépendance importante de l'Allemagne aux équipementiers chinois, et ses difficultés à appliquer la Boîte à outils 5G. Peu désireuse de froisser le partenaire commercial chinois par une exclusion directe et immédiate de ses fournisseurs, l'Allemagne utilise ainsi l'Open RAN comme un argument pour retarder le coûteux retrait des équipements Huawei jusqu'à ce que cette solution multifournisseur arrive à maturité... tout en satisfaisant l'allié américain⁸².

79. *Ibid.* ; « Report on the Cybersecurity of Open RAN », *op. cit.*

80. Propos tenus sous la règle de Chatham House, 2022.

81. B. Thomas, « Why Germany's Investment in Open RAN Will Not Solve its 5G Problem », Conseil européen des relations internationales, 6 avril 2021, disponible sur : <https://ecfr.eu> ; K. Wieland, « Mavenir Puts Down Open RAN R&D Roots in Germany », *LightReading*, 25 avril 2022, disponible sur : www.lightreading.com.

82. Entretien avec un acteur privé du numérique européen, mai 2022 ; Entretien avec un responsable d'un opérateur français, 22 juin 2022 ; P. Hunter, « G7 Countries Grope towards Coordinated Approach to Open RAN Ecosystem », *Rethink Research*, 25 mai 2021, disponible sur : <https://rethinkresearch.biz>.

Conclusion

Au croisement de la géopolitique de la 5G et des standards, l'Open RAN est au cœur de débats dépassant les seules considérations techniques (maturité, cybersécurité, performance...) ou économiques (coûts, risque de duopole...). Au vu de la participation dans l'Alliance O-RAN de nombreuses entreprises chinoises étroitement liées aux autorités politiques et militaires de la République populaire de Chine, l'Open RAN peut difficilement être considéré comme la panacée pour réduire la présence dans les réseaux européens de fournisseurs étrangers à risque. Il pourrait au contraire accroître les dépendances de l'UE envers des acteurs non européens (principalement américain, chinois, japonais et sud-coréen), d'où son intense promotion par Washington ces dernières années.

Toutefois, quelle que soit la part de marché gagnée par l'Open RAN tel que conçu aujourd'hui, beaucoup des défis qu'il suscite sont liés aux tendances à la virtualisation, à l'automatisation, et plus largement à la complexification des réseaux télécoms. L'Europe devra donc nécessairement y faire face. Tant au niveau des États membres que de l'UE, le développement de meilleures capacités d'analyse et de régulation du RAN et de sa chaîne de valeur semble nécessaire pour identifier les vulnérabilités et cibler les politiques de soutien au secteur.



27 rue de la Procession 75740 Paris cedex 15 – France

Ifri.org