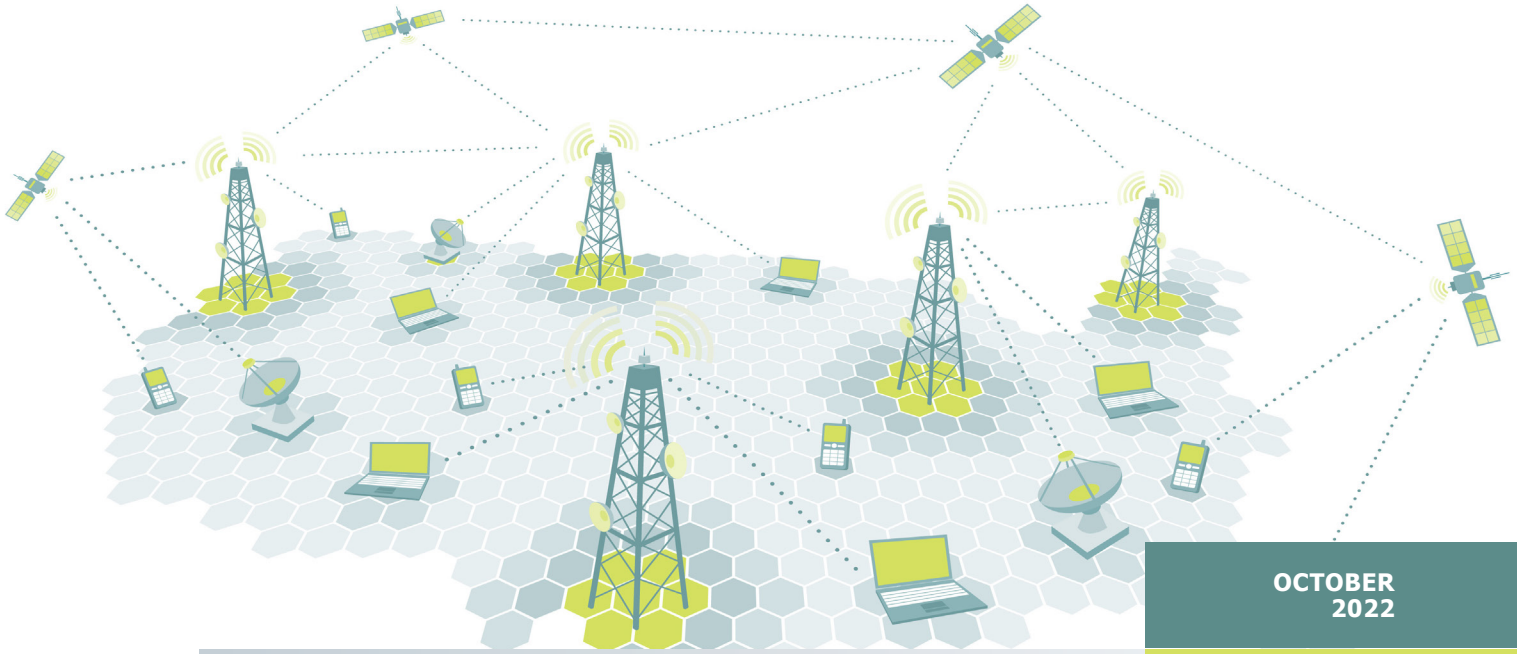
NOTES
DE L'IFRI



OCTOBER
2022

"Open" Telecom Networks (Open RAN)

Towards a Reconfiguration of International Competition in 5G?

Geopolitics of
Technology
Program

Mathilde VELLIET

The French Institute of International Relations (Ifri) is a research center and a forum for debate on major international political and economic issues. Headed by Thierry de Montbrial since its founding in 1979, Ifri is a non-governmental, non-profit organization.

As an independent think tank, Ifri sets its own research agenda, publishing its findings regularly for a global audience. Taking an interdisciplinary approach, Ifri brings together political and economic decision-makers, researchers and internationally renowned experts to animate its debate and research activities.

ISBN: 979-10-373-0602-9

How to quote this publication:
Mathilde Velliet, "'Open' Telecom Networks (Open RAN): Towards a Reconfiguration of International Competition in 5G?", *Notes de l'Ifri*, Ifri, October 2022.

Ifri

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

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

Email: accueil@ifri.org

Website: Ifri.org

Author

Mathilde Velliet is a Research Fellow within the Geopolitics of Technology program at Ifri since September 2021. Her research focuses on international issues related to new technologies, particularly American and Chinese technology policies as well as U.S.-China relations. She is also a PhD student in American civilization at the University of Paris and the University of Aix-Marseille. Her doctoral thesis focuses on U.S. policies on strategic technologies in response to the China threat under the Obama and Biden administration.

She holds a master's degree in English studies from the École Normale Supérieure de Lyon and a master's degree in International Security from Sciences Po Paris. She also conducted research in the United States, at New York University and Boston University.

Her most recent publications include "Convince and Coerce: U.S. Interference in Technology Exchanges Between its Allies and China" (*Études de l'Ifri*, February 2022).

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.

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.

Table of Contents

Introduction

The Trump administration's intense diplomatic campaign against Chinese supplier Huawei, which began in 2019 and has been continued by its successor, has highlighted not only the network security risks but also the profoundly geopolitical issues associated with the deployment of 5G around the world. Against a backdrop of a sharp increase in the amount of data transferred by mobile networks, frequency bands used and base stations deployed,[1] three suppliers now account for more than 75% of the global RAN market share: China's Huawei (31%), Sweden's Ericsson (28%) and Finland's Nokia (17%).[2] Presented as a solution to reintroduce more diversity among suppliers while offering alternatives to risky Chinese equipment manufacturers, Open RAN (Open Radio Access Network) is a concept that describes certain network architectures, i.e. ways of organizing hardware and software equipment, protocols, etc., into a whole that allows data transmission within the network and to third-party applications. Because they include open interfaces, these new "open" architectures would allow operators to no longer buy the entire solution from a single supplier, but to freely choose the most suitable solution for each software or hardware component. Open RAN is being promoted by both telecom operators and (mostly American) government actors.

Is Open RAN really the panacea promised to Europe to free itself from dependencies on unreliable suppliers and the risks of duopoly? What risks and opportunities does Open RAN present for European technological sovereignty?

It is first necessary to clarify the definition of Open RAN – as it is both technically complex and often shrouded in a vague rhetoric of "openness" – and to examine the opportunities it promises in terms of cost and innovation, and its apparent weaknesses in terms of maturity and security. Despite these difficulties and the participation of Chinese companies in Open RAN, open networks have been strongly supported politically and financially in the United States, and actively promoted to its allies. For Europe, however, Open RAN presents the risk of creating new dependencies on foreign companies, in a sector where it currently has some of the world's main competitors.

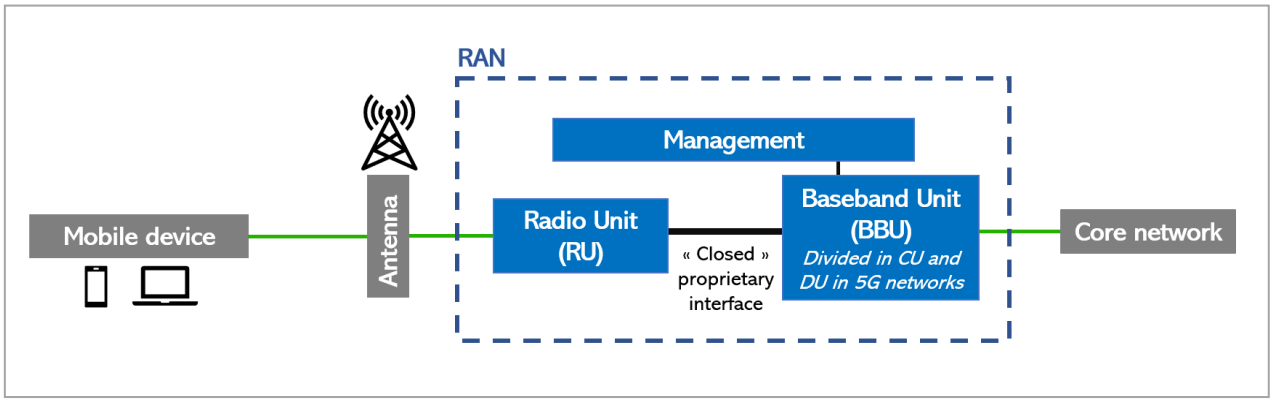
Research for this paper comprised interviews, including with Alix Durand, in charge of strategic analysis at the French National Agency for Information Systems Security (ANSSI), on June 28, 2022.

1. "5G Scoreboard", European 5G Observatory, January 2022, available at: https://5gobservatory.eu.
2. Dell'Oro, "World RAN Market Shares Development", May 19, 2022.

What Open RAN Is (and Isn't)

The Radio Access Network (RAN) is the radio part of a mobile telecommunications system that enables the connection between a terminal (such as a phone or computer) and the core network. To simplify, it consists of an antenna, radio units (RU) receiving and sending data, and in 4G baseband units (BBU)– split into a centralized unit (CU) and a distributed unit (DU) in 5G – processing data and communicating with the operator's core network. Traditionally, the same equipment manufacturer (Huawei, Ericsson, Nokia, etc.) provides a so-called "proprietary" or "closed" solution. In this solution, the hardware and software elements that make up the RU and BBU are intertwined and non-interchangeable, and the two are linked by a proprietary interface. The whole solution, sometimes referred to as a "black box" and represented in blue on the diagram, is provided by a single supplier. However, the interfaces between the antenna and the RU, as well as between the BBU and the core network, are open and standardized by the 3rd Generation Partnership Project (3GPP), a body composed of seven global organizations developing standards for 3G, 4G and 5G telecommunications.[3]

Figure 1: Traditional RAN architecture



Represented in green, the open interfaces standardized by the 3GPP.

As the name suggests, Open RAN reflects the ambition to create new "open" interfaces between different interoperable radio access network building blocks.

3. 3GPP Website, "About 3GPP", available at: www.3gpp.org.

Triple Combination: Virtualization, Automation, Disaggregation

Open RAN can be defined as a network architecture paradigm. It is neither a standard nor a new technology per se, but rather a combination of existing technologies (artificial intelligence [AI], off-the-shelf commercial components, open interfaces, cloud), at the crossroads of three objectives: virtualization, automation, and disaggregation.[4] It is important to differentiate them, because the first two are major trends in telecom networks which go beyond Open RAN[5] and are broadly supported by industrial players, while the third one is the subject of more debate and criticism on the part of equipment manufacturers (in particular Ericsson and Huawei).

Virtualization, i.e. the separation of hardware and software elements, is a fundamental trend in 5G in general (and to a lesser extent in previous generations), affecting both the RAN (known as vRAN, for virtual RAN) and the core network. Virtualization allows software to run on generic commercial hardware, or even in the cloud, to perform the functions of traditional telecom equipment.[6]

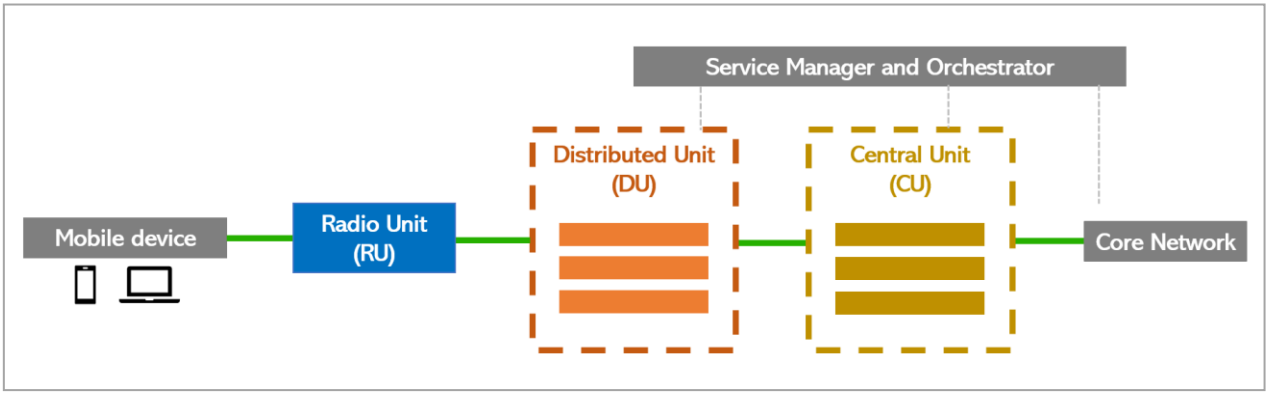
The aim of automation is to make the RAN "intelligent" by replacing manual tasks with automated functionalities (thanks to machine learning in particular), thus reducing operating costs and increasing performance.[7] It is increasingly implemented in 5G by operators (Dish, China Mobile, Vodafone…) as well as by major equipment manufacturers in order to manage an increasing amount of data in an increasingly complex network.[8]

Linked to virtualization and automation, disaggregation is the division of RAN functions into different interoperable bricks. These disaggregated architectures are already functionally and numerically more important in 5G than in previous generations, and some have already been standardized by 3GPP.[9] The Open RAN proposal is to go even further by proposing a

4. H. Lee-Makiyama, "Open RAN: The Technology, its Politics and Europe's Response", *ECIPE Policy Brief*, No. 8, European Centre for International Political Economy, 2020; "Report on the Cybersecurity of Open RAN", NIS Cooperation Group, May 11, 2022, p. 4, available at: 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*, No. 3707, June 2022; R. Loukhil, "Le Royaume-Uni sonne la migration de ses réseaux mobiles vers la technologie Open RAN", *L'Usine Nouvelle*, February 26, 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*, June 17, 2021.
7. S. Pongratz, "The Role of Intelligent RAN and Automation", Dell'oro Group, June 15, 2022, available at: www.delloro.com; "Ericsson Intelligent RAN Automation", Ericsson, August 25, 2022, available at: www.ericsson.com.
8. *Ibid*; Laurent Leboucher quoted in J. Taaffe, "How Orange's CTO Is Driving Network Transformation", Inform, January 2022, available at: https://inform.tmforum.org.
9. Such as the split dividing the Basebad Unit (BBU) in two units, the Distributed Unit (DU) and the Central Unit (CU), which is defined by the 3GPP Release 15. See "Study on CU-DU Lower Layer Split for

dozen new open interfaces between the bricks, for example between the radio unit (RU) and the distributed unit (DU).

Figure 2: "open" architecture



Represented in green, the open interfaces following 3GPP standards or O-RAN specifications.

The goal is to allow the operator to buy these hardware and software bricks from various suppliers, to choose the most efficient option for each brick by freely mixing different solutions. The interoperability between the bricks is ensured by specifications which complement and are dependent on 3GPP standards: the specifications developed by the O-RAN Alliance.[10]

The O-RAN Alliance was founded in 2018 by five major mobile operators (AT&T, China Mobile, Deutsche Telekom, NTT Docomo and Orange) – who retain a prominent place in it – specifically to "re-shape the RAN industry towards more intelligent, open, virtualized and fully interoperable mobile network".[11] The main missions of this alliance are threefold: to propose specifications for Open RAN, to develop software for the RAN (O-RAN Software Community), and to support the testing and integration of Open RAN solutions.[12] The Alliance collaborates with the Telecom Infra Project (TIP), an industry consortium which includes a group dedicated to accelerating the innovation and commercialization of Open RAN solutions.

NR", 3GPP Technical Report 38.816, 2017, available at: https://portal.3gpp.org and O. Andersson, "Functional Splits: The Foundation of an Open 5G RAN", 5G Technology World, May 17, 2021, available at: www.5gtechnologyworld.com.

10. R. Layton, "OpenRAN: American Trade Policy Masquerading As Security", *Forbes*, December 3, 2021.

11. "About Us", O-RAN Alliance, available at: www.o-ran.org.

12. *Ibid.*

Openness as a "Discursive Device": Open Source, Open Standards, Open RAN

One of the difficulties in understanding Open RAN relates to the use of the concept of openness as a "discursive tool" by the industry and governmental actors promoting it.[13] Indeed, this concept embed Open RAN in a social imaginary of transparency, trust and freedom – as opposed to the "black boxes" that proprietary solutions represent. It often conflates three different realities:

- open (i.e. non-proprietary) interfaces between network bricks
- open source,
- "open standards".[14]

As explained earlier, Open RAN does indeed imply the creation of more open interfaces, i.e interfaces which allow interoperability between network bricks, as opposed to a so-called "closed" proprietary interface. In Open RAN, but also more widely in virtualized networks and/or in the cloud, some of these bricks can be composed of open source software developed collectively. For instance the O-RAN Alliance is working in cooperation with the Linux Foundation to develop open source software for the RAN.[15] Yet most of Open RAN components remain proprietary technologies.[16]

Last, the argument around the "open standards" of Open RAN is ambiguous. This term is used to designate technical decisions standardizing open *interfaces*. However, in the case of the O-RAN Alliance, the process itself by which these specifications are developed is not very open. Its lack of transparency has been criticized in a report by the European Cybersecurity Agency[17] for two main reasons. First, not all O-RAN specifications are publicly available. Secondly, the process of developing the specifications does not abide by the founding principles of the World Trade Organization (WTO) on the development of international standards.[18]

13. J.-C. Plantin, "The Geopolitical Hijacking of Open Networking", *European Journal of Communication*, Vol. 36, No. 4, 2021.
14. Terms used for instance in: "O-RAN Alliance Conducts First Global Plugfest to Foster Adoption of Open and Interoperable 5G Radio Access Networks", O-RAN Alliance, December 19, 2019, available at: www.o-ran.org; Open RAN Policy Coalition, "Open RAN Policy Coalition Releases New Policy Roadmap", December 1, 2020, available at: www.openranpolicy.org; M. Rasser and A. Riikonen, "Open Future: The Way forward on 5G", Center for a New American Security, July 28, 2020.
15. "About Us", O-RAN Alliance, available at: 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. These principles were agreed upon in 2000 by the Technical Barriers to Trade (TBT) Committee of the World Trade organization: "Principles for the Development of International Standards, Guides and Recommendations", World Trade Organization, available at: www.wto.org.

Promises and Weaknesses of Open RAN

Increasing Diversity to Spur Innovation and Lower Costs?

In the highly-concentrated 5G market, dominated by three major equipment manufacturers and fraught with the risk of an Ericsson-Nokia duopoly following the exclusion of Huawei from many countries, telecom operators are emphasizing the flexibility and supplier diversification enabled by Open RAN.[19] Open interfaces allow new players to enter the market with solutions for certain components, and allow operators to highten competition among vendors while freeing themselves from the constraints of proprietary technology sets from large equipment manufacturers. This more competitive 5G environment could provide more innovative and less expensive solutions, whereas market domination by a small number of companies is blamed for high prices and slow innovation.[20] These benefits are combined with those of virtualization and automation: use of less expensive generic hardware, pooling of resources, easier and simpler maintenance, faster adaptation and improved resilience of the network, etc.[21]

However, Open RAN is not a mature solution in the short term.[22] The integration of all these disaggregated building blocks is both technically complex and costly.[23] As some operators and vendors point out, it is not certain that operators will choose to multiply the number of suppliers per site, nor that this system will result in significant savings.[24]

Many players are also questioning the performance improvements promised by the opening of new interfaces. Commercial off-the-shelf hardware is not yet able to compete in terms of performance (including energy performance) with the electronic components of proprietary

19. See for instance: Deutsche Telekom, Orange, Telefónica and Vodafone, "Memorandum of Understanding on the Implementation of Open RAN Based Networks in Europe", January 2021.
20. *Ibid*; D. Rinaldo, "Leading the Wireless Future: Securing American Network Technology", Hearing before the House of Representatives, April 21, 2021.
21. J. Taaffe, "How Orange's CTO Is Driving Network Transformation", *Inform*, January 2022; R. Loukhil, "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,* May 27, 2022, available at: www.rcrwireless.com; R. Loukil, "L'Europe va-t-elle rater le coche de la révolution Open RAN des réseaux mobiles", *L'Usine Nouvelle*, March 30, 2022.
23. Interview with Viktor Arvidsson, Head of Public Affairs, Innovation and Strategy, France, Belgium, Luxembourg, Algeria and Tunisia at Ericsson, Paris, May 30, 2022; R. Loukil, "L'Europe va-t-elle rater le coche de la révolution Open RAN des réseaux mobiles", *op. cit.*; H. Lee-Makiyama and R. Baker, "TTC and Pre-Empting the Next Transatlantic Tech War", May 2022, available at: https://ecipe.org.
24. *Ibid.*; "Nokia's Mobile Chief: Open RAN Progress Is Too Slow, Implementation Complex and Costly", *Communications Day*, No. 6397, May 2022; I. Morris, "BT Takes Aim at Open RAN Myths", *LightReading*, November 12, 2021, available at: www.lightreading.com.

solutions, optimized for their specific tasks.[25] This issue of energy efficiency will be crucial for Open RAN.[26] More broadly, in their current form, open interface specifications constrain the functions that can be run on each side of the interface (at the RU and DU level, for example), which may have an impact on network performance.[27]

Last, there are doubts about whether Open RAN – which is estimated to gain a 15% share of the global radio access network market by 2026 – can fundamentally transform the market. The reasons for industry consolidation (in particular the high cost of entry in terms of capital and expertise) remain key and could result in re-consolidation in Open RAN, with the big players buying out the small players[28].

Cybersecurity: More Risks Than Opportunities

In a context of increasing cyber threat, security issues are at the heart of 5G discussions. General trends toward virtualization and automation already present certain cybersecurity opportunities. For example, by reducing the amount of human intervention, automation decreases the risks associated with human error.[29] In addition to the cybersecurity benefits of virtualization and automation, Open RAN presents some security opportunities through the disaggregation it offers. Having a large number of vendors reduces the risks associated with dependency on a single vendor, and implies a form of compartmentalization that contributes to network resiliency.[30] The presence of standardized open interfaces, easier access to performance data, and the use of open source software can foster visibility and transparency on network operations, especially for national authorities and security testers.[31]

However, several official reports have pointed out the security risks associated with Open RAN in its current form. In particular, the European Cybersecurity Agency points out that Open RAN increases the already existing risks of network misconfiguration and of security vulnerability inherent to low-quality components provided by a multiplicity of vendors.[32]

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", March 20, 2022, *op. cit.*
26. Interview with a French mobile operator, 22 June 2022.
27. Interview with Viktor Arvidsson, May 30, 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,* January 24, 2022, available at: 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. *Ibid.*.
31. *Ibid.*, p. 10; *Open RAN Security in 5G*, Open RAN Policy Coalition, April 2021.
32. "Report on the Cybersecurity of Open RAN", 2022, *op. cit.*

The proliferation of open interfaces and vendors also creates new security risks. It presents more opportunities for cyber attackers: as one U.S. government agency writes, "the attack surface of the network expands considerably".[33] It is also fraught with the vulnerabilities inherent to a more complex supply chain, with the presence of potentially unreliable vendors that are difficult to vet. The O-RAN Alliance's specifications have also been singled out for criticism because their development process does not place the principle of "security by design/default"[34] at its core. In addition to the performance issues previously discussed, suppliers like Ericsson pointed out these security vulnerabilities associated with Open RAN and O-RAN specifications in particular, while contributing to the Alliance's work on security to remedy them.[35]

Others warn about the use of open source or jointly developed software, as is the case in the O-RAN Alliance Software Community, because it allows potential untrusted actors to access information (and vulnerabilities) in the code and contribute to its development.[36]

Open RAN therefore poses short and medium term security problems, that the O-RAN Alliance's Security Focus Group, which became a full-fledged working group (the 11th) in June 2022, has been trying to address.[37] For Europe, the Open RAN also creates a risk of increased dependence on foreign suppliers, particularly Chinese and American.

33. *Ibid.*, p. 8; "Technology Assessment: 5G Wireless, Capabilities and Challenges for an Evolving Network", U.S. Government Accountability Office, November 2020, p. 33; see also "Open Radio Access Network Security Considerations", U.S. Cybersecurity and Infrastructure Security Agency (CISA) and National Security Agency (NSA), September 15, 2022, available at: www.cisa.gov.
34. S. Köpsell *et. al.*, "Open-RAN Risikoanalyse", Bundesamt für Sicherheit in der Informationstechnik, February 21, 2022.
35. Interview with René Summer, Director of Government and Industry Relations at Ericsson Group, June 22, 2022.
36. J.-P. Kleinhans and T. Rühlig, "The False Promise of Open RAN", *Digital Power China*, August 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, August 29, 2022, available at: www.o-ran.org.

A Panacea to Replace Huawei? Chinese Participation and American Interests in Open RAN

In line with the U.S. diplomatic campaign to dissuade its partners from using Chinese 5G vendors deemed unreliable such as Huawei and ZTE, Washington has actively promoted Open RAN as an alternative. Yet a large number of Chinese companies have invested in Open RAN since its inception. How can this apparent contradiction be explained?

Open RAN: Without Huawei but not Without China

As some American actors emphasize, Huawei is not part of either the O-RAN Alliance or the Telecom Infra Project.[38] However, many other Chinese vendors and operators are members of these bodies, and the participation of Chinese entities in other international Open RAN standardization organizations such as 3GPP has increased in recent years.[39]

The O-RAN Alliance initially resulted from the merger of two organizations, the American- and European-dominated XRAN Forum, and the C-RAN Alliance established by China Mobile.[40] China Mobile, China's largest state-owned operator, is even one of the five founding members of the O-RAN Alliance. It has permanent seats on the board of directors as well as veto rights, and it co-chairs ten of its fourteen working groups.[41] In total, with 44 members in 2021, China is the country with the second largest number of members in the O-RAN Alliance after the United States. At least two-thirds of these Chinese members are partially or wholly state-owned, and 16 have official ties to military or security activities.[42] The Alliance even includes many Chinese companies under U.S. sanctions

38. M. Rasser and 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,* No. 14, September 2021.
40. J. Leen, Eric Zhang and R. Creemers, "China Standardisation System – Trends, Implications and Cas Studies in Emerging Technologies", Leiden Asia Center, April 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, January 2022.
42. *Ibid.*

(sometimes because of their ties to the Chinese Communist Party or the Chinese army), such as Inspur,[43] SMIC, Kindroid, Phytium, H3C,[44] and the three state-owned operators China Mobile, China Telecom and China Unicom.[45] This even led Nokia to temporarily suspend its participation in the O-RAN Alliance in August 2021, for fear of violating U.S. restrictions by trading with these companies. In addition to specifications, Chinese companies are also invested in the development of open source code that can be used for Open RAN. For instance, Huawei was the 5th contributor and steering committee member (from 2017 to 2019) of the Kubernetes platform, and both Huawei and Tencent are on the board of the Linux Foundation, a partner of the O-RAN Alliance for code development.[46]

The criticisms levelled at Huawei regarding its preferential treatment by and close ties to the Chinese authorities apply equally (or even more so) to a large number of Chinese telecom companies.[47] Beijing could thus use the same tools (subsidies, privileged market access…) to support Chinese suppliers of critical Open RAN equipment, creating a concentration situation similar to the current situation in the proprietary RAN market. Indeed, according to Kleinhans and Ruhlig, "strategic considerations by state-run Chinese think tanks in China suggest that the country sees Open RAN as an opportunity to circumvent US sanctions".[48]

Open RAN thus does not appear to be an automatic solution to mitigate possible dangers associated with risky suppliers or over-reliance on Chinese technologies. Yet it has been vigorously promoted by U.S. industry and political actors.

American Interests and Lobbying

In addition to the goal of excluding Huawei from networks, Open RAN is explicitly conceived by industry, politicians, and researchers across the pond as an "opportunity for American technology leadership",[49] in the absence of a major U.S. 5G champion. As John Baker, vice president of business development at Mavenir, writes, "[t]he best way to prioritize

43. On the Department of Defense's listing of "Communist Chinese Military Companies", see "Timeline of Executive Actions on China", U.S.-China Economic and Security Review Commission, April 1, 2021, available at: www.uscc.gov.
44. All 4 are on the Department of Commerce's Entity List. "Supplement No. 4 to Part 744 – Entity List", Bureau of Industry and Security, August 24, 2022, available at: www.bis.doc.gov.
45. All 3 are on the Department of the Treasury's List of "Chinese Military-Industrial Companies". "Introduction of Non-SDN Chinese Military-Industrial Complex Companies List", U.S. Department of the Treasury, June 3, 2021, available at: https://home.treasury.gov.
46. R. Layton, "OpenRAN: American Trade Policy Masquerading As Security", *Forbes*, December 3, 2021; "Board of Directors", The Linux Foundation, available at: www.linuxfoundation.org.
47. R. Layton, "Efforts to Make 5G More 'Open' with Less Huawei Have Attracted Dozens of Chinese Vendors", *Forbes*, December 17, 2020.
48. J.-P. Kleinhans and T. Rühlig, "The False Promise of Open RAN", *op. cit.*, pp. 12-13.; see also J. Leen, E. Zhang and R. Creemers, *China Standardisation System, op. cit.*, p. 19.
49. M. Rasser and A. Riikonen, *Open Future: The Way forward on 5G*, *op. cit.*

American leadership in 5G is to create policies that prioritize OpenRAN."[50] Open RAN does indeed drive the evolution of the 5G value chain towards areas where U.S. companies have an advantage, both in software and hardware.[51]

The importance of software and virtualization, at the heart of the Open RAN, plays to U.S. strengths. The cloud market, which is essential for network virtualization and cloudification, is dominated by large American companies such as Amazon Web Services, Google, Microsoft Azure and Oracle, whose importance in telecoms in the broadest sense and in Open RAN projects in particular seems set to grow. These companies are engaged in promoting Open RAN, notably through their participation in the O-RAN Alliance and the Open RAN Policy Coalition.[52] Similarly, the new leading vendors of key software solutions for Open RAN, such as Mavenir, Parallel Wireless, and Altiostar,[53] are American. The use of generic (rather than dedicated) hardware also represents an opportunity for the U.S. companies which manufacture these components, such as Dell, Intel, or Qualcomm.[54]

These opportunities explain the strong political and financial support of American governmental actors for Open RAN. The report published in 2021 by the National Telecommunications and Information Administration (NTIA) on behalf of the entire U.S. government explicitly states that "the executive branch fully supports the development of Open RAN by industry"[55] and urges the Federal Communications Commission (FCC) to take facilitating measures. This support has been expressed separately by the Department of Commerce (which includes the NTIA), the Department of State,[56] the Department of Defense,[57] and even the Central Intelligence Agency (CIA), which has invested in Parallel Wireless through its venture capital fund In-Q-Tel.[58]

50. J. Baker, "It's Time to Prioritize American Mobile Technology", Mavenir, March 24, 2021, available at: https://medium.com.
51. B. Clark and D. Patt, "Weaponizing the 5G Value Chain: A Two-Pronged Strategy to Establish America's Lead in Next-Generation Telecommunications", Hudson Institute, September 2020.
52. Amazon, Google, Microsoft and Oracle are all members of these organizations. See "Members", Open RAN Policy Coalition, available at: www.openranpolicy.org and "O-RAN Companies", Alliance O-RAN, available at: www.o-ran.org.
53. Acquired by the Japanese Rakuten in 2021.
54. R. Loukil, "Pourquoi Qualcomm rachète Cellwize, une pépite des réseaux mobiles Open RAN", *L'Usine Nouvelle*, June 13, 2022.
55. "NTIA Comments on Promoting the Deployment of 5G Open Radio Access Networks", National Telecommunications and Information Administration, July 16, 2021, available at: www.ntia.gov.
56. See for instance Secretary of State Mike Pompeo's speech at the Forum on 5G Open Radio Access Network, on September 14, 2020, available at: www.fcc.gov; or more recently: "Joint Statement of the U.S.-Japan Economic Policy Consultative Committee: Strengthening Economic Security and the Rules-Based Order", Office of the Spokesperson, July 29 2022, available at: www.state.gov.
57. K. Stacey, "Pentagon Wants Open-Source 5G Plan in Campaign against Huawei", *Financial Times*, December 22, 2019.
58. M. Rasser and A. Riikonen, *Open Future: The Way forward on 5G*, *op. cit.*

The close links between the administration and the Open RAN Policy Coalition, created in May 2020 to "educate politicians" and lobby for Open RAN (primarily in the United States), are also evident: the executive director is Diane Rinaldo, former administrator of the NTIA and Assistant Secretary for Communications and Information at the Department of Commerce (2018-2020). Unlike the O-RAN Alliance, this coalition includes mostly U.S. players (including the aforementioned giants AWS, Google, Meta, Microsoft…) and no Chinese companies.[59]

This lobbying seems to have paid off: the U.S. Congress has shown bipartisan support for Open RAN by passing several pieces of legislation in this direction. The Secure and Trusted Communications Networks Act of 2019 allocates $1.9 billion to a program allowing operators to replace risky equipment in telecom networks, opening the door to using Open RAN components instead.[60] Other legislation more directly grant subsidies to Open RAN, such as the Utilizing Strategic Allied (USA) Telecommunications Act[61], which creates a $750 million fund (from 2021 to 2031) to support Open RAN deployment in the United States, and the CHIPS and Science Act of August 2022, which allocates $1.5 billion to this same fund.[62]

In addition to encouraging the deployment of Open RAN on American soil, the Trump and Biden administrations have also conducted a sustained diplomatic campaign in its favor towards their allies. These diplomatic efforts have been pursued both bilaterally and in plurilateral fora, such as the Prague Conference on 5G Security,[63] the G7,[64] or the EU-US Trade and Technology Council (TTC).[65] In this, Washington has the support of London, which sees the Open RAN as an opportunity for its companies (and for its "special relationship" with the United States), as well as a possibility to free itself from its heavy dependence on Huawei equipment without becoming too dependent on Ericsson and Nokia.

Intense enough to be called a "geopolitical hijacking of open networks",[66] "American trade policy masquerading as security",[67] or even "pressure" ("*forcing*"),[68] it has been received with mixed feelings in Europe.

59. "Open RAN: A Year in Review", Open RAN Policy Coalition, May 3, 2021, available at: www.openranpolicy.org.
60. T. Maupile, "The Role of Legislative Policy Initiatives in Open RAN", Altiostar, March 30, 2021, available at: www.altiostar.com.
61. Adopted within the *National Defense Authorization Act* (section 9202) passed on January 1st, 2021.
62. *CHIPS and Science Act of 2022*, division A, August 9, 2022.
63. See for instance the speech of FCC President Ajit Pai: A. Pai, "Remarks to the Prague 5G Security Conference", September 24, 2020, available at: https://docs.fcc.gov.
64. Interview with a private actor of the European digital ecosystem, May 2022.
65. Remarks under Chatham House rule, 2022.
66. J.-C. Plantin, "The Geopolitical Hijacking of Open Networking: The Case of Open RAN", *op. cit.*
67. R. Layton, "OpenRAN: American Trade Policy Masquerading As Security", *Forbes*, December 3, 2021.
68. R. Loukhil, "L'Europe face à la révolution Open RAN", June 2022, *op. cit.*

European Dependencies and Reactions

In the face of such enthusiasm from the US, Japan, the UK and European operators,[69] the European Union (EU) has adopted a cautious stance on Open RAN, while continuing to promote diversity and security in telecoms. In addition to the issues previously mentioned regarding the maturity, performance and security of an "open 5G", this position is explained by the risks, inherent to Open RAN, of exacerbating European dependencies.

Indeed, while for Europe Open RAN presents certain opportunities (notably for operators, and for certain new players providing hardware or software solutions), the risk is twofold.[70] First, although they are involved in discussions on Open RAN, the European champions Nokia and Ericsson, suppliers of proprietary solutions, could lose significant market share with this new architecture and the entry of new players. Secondly, it is very likely that most of these players will be non-European: while Open RAN plays to American strengths, it draws attention to European weaknesses, especially in the services and software markets.

The trend towards virtualization, which goes beyond Open RAN, already raises questions about the growing role in telecoms of US internet giants, who can leverage their cloud, edge computing and software capabilities.[71] While supporters of Open RAN point to the possibility of bringing new, smaller players into the market, the risk is that it is mainly the non-European hyperscalers, present in the O-RAN Alliance and the Open RAN Policy Coalition, that will benefit from this opening up thanks to their capacity for innovation… and consolidation.[72] To offer alternatives to hyperscalers, operators such as Orange are calling for European "telco cloud" solutions,[73] with open source components, but their realization still seems rather uncertain.

In addition to the cloud giants, Open RAN risks increasing European dependencies in hardware and software. As *L'Usine Nouvelle* summarizes, "unlike the United States, which has a complete ecosystem, from chips to integration services, with a plethora of emerging players, Europe suffers from a partial presence, concentrated on radio hardware, and a lack of new

69. "Europe Urged to Act Now to Build Open Ran Ecosystem", Memorandum of Understanding, Deutsche Telekom, Orange, Telecom Italia, Telefónica et Vodafone, November 2021, available at: https://media.orange.com.

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

71. However, their role could be constrained by European and national regulations on the security of telecom networks (such as the article R226 in France).

72. See for instance the acquisition of the German start-up MobiledgeX by Google: R. Karayan, "Edge Computing: Google Cloud rachète MobiledgeX", *L'Usine Digitale*, May 3, 2022, available at: www.usine-digitale.fr; or I. Morris, "Prickly Deutsche Telekom Boss Wants Hyperscaler Deals Curbed", *LightReading*, November 16, 2021, available at: www.lightreading.com.

73. J. Taaffe, "How Orange's CTO Is Driving Network Transformation", *Inform*, January 2022.

players in Open RAN software".[74] These new players – which include, for example, Belgium's AccelleRAN – are far fewer in number than their competitors (13 compared to 57 elsewhere in the world) and are still in the experimentation phase. As a result, even European operators have started the deployment of Open RAN in their networks primarily with foreign vendors: Spain's Telefonica, for example, has enlisted the help of Japan's NEC and the U.S.'s Altiostar, Mavenir, and Airspan; Deutsche Telekom has partnered with Fujitsu, NEC, and Mavenir; and Telecom Italia Mobile has teamed up with JMA Wireless and Mavenir.[75] Operators such as Orange and Vodafone emphasize their goal of "building an Open RAN ecosystem in Europe comparable to those in the United States, Japan and South Korea" – and call for more political and industrial support from the European Commission and Member States.[76] Some operators have encouraged (unsuccessfully to date) the American authorities to work with European counterparts to build financing opportunities for the development of a European ecosystem, including via the TTC, in an attempt to convince Brussels to embrace Open RAN.[77] However, given the delay, developing this European ecosystem seems long and costly, and non-European players are likely to be the first to benefit from disaggregation.[78]

Coupled with technical concerns, these elements explain the European Commission's measured position on Open RAN. As it did when it published the "EU Toolbox for 5G security", the Commission is developing its own analytical tools to build a concerted approach and respond to the incentives and concerns raised by Washington. The previously mentioned reports (on 5G market trends 5G in 2021 or on Open RAN cybersecurity, in May 2022) illustrate this.[79] In addition, because of diverging priorities and considerations on security and efficiency between Europe and the United States, European representatives have indicated that they will not give in to US lobbying on Open RAN, although this does not obstruct other discussions on 5G within the Trade and Technology Council.[80]

Behind this common position displayed by the European Commission, member states' approaches on Open RAN vary, depending on various factors: influence of the country's main mobile operators, dependence on Huawei equipment, relations with China and with the United States… An interesting example is Germany, arguably one of the most pro-Open RAN countries in Europe. The German government announced a €300 million

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, Head of Innovation at Orange, quoted in R. Loukhil, "Comment Orange se prépare à la révolution Open RAN des réseaux mobiles", *L'Usine Nouvelle*, March 14, 2022; N. Fildes, "Vodafone Taps Japan and US to Fill Huawei Gap", *Financial Times*, June 15, 2021.
77. Interview with a private European actor of the telecom industry, September 7, 2022.
78. M. Dinges *et. al.*, "5G Supply Market Trends: Final Report", 2021, *op. cit.*
79. *Ibid.*; "Report on the Cybersecurity of Open RAN", *op. cit.*
80. Remarks under Chatham House rule, 2022.

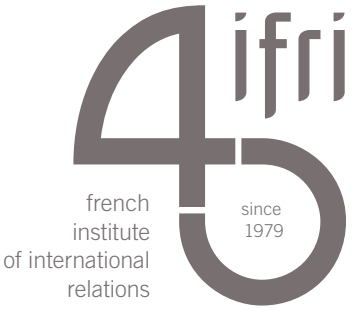
investment in Open RAN in June 2021, and is supporting several centers of excellence and deployment projects (including an "Open RAN City"[81]). While Deutsche Telecom's influence in Berlin is likely to have something to do with it, this stance is linked to Germany's heavy reliance on Chinese suppliers, and its difficulties in implementing the 5G Toolbox. Unwilling to offend the Chinese business partner by a direct and immediate exclusion of Chinese suppliers, Germany uses Open RAN as an argument to delay the costly withdrawal of Huawei equipment until this multi-vendor solution matures… while satisfying the American ally.[82]

81. B. Thomas, "Why Germany's Investment in Open RAN Will Not Solve its 5G Problem", European Council of International Relations, April 6, 2021, available at: https://ecfr.eu; K. Wieland, "Mavenir Puts Down Open RAN R&D Roots in Germany", *LightReading*, April 25, 2022, available at: www.lightreading.com.
82. Interview with a private European digital player, May 2022; Interview with a French mobile operator, 22 juin 2022; P. Hunter, "G7 Countries Grope towards Coordinated Approach to Open RAN Ecosystem", *Rethink Research*, May 25, 2021, available at: https://rethinkresearch.biz.

Conclusion

At the crossroads of the geopolitics of 5G and of standards, Open RAN is at the heart of debates that go beyond technical considerations (maturity, cybersecurity, performance…) or economic concerns (costs, risk of duopoly…). Given the participation in the O-RAN Alliance of many Chinese companies closely linked to the political and military authorities of the People's Republic of China, Open RAN can hardly be considered a panacea for reducing the presence of risky foreign suppliers in European networks. On the contrary, it could increase the EU's dependence on non-European actors (mainly American, Chinese, Japanese and South Korean), hence its intense promotion by Washington in recent years.

However, regardless of the market share gained by Open RAN as conceived today, many of the challenges it raises are linked to broader trends like virtualization, automation, and more generally the increasing complexity of telecom networks. Europe will therefore have to face these challenges. At both the Member States and EU levels, the development of better analytical and regulatory capabilities for the RAN and its value chain seems necessary to better identify vulnerabilities and target policies supporting the sector.



27 rue de la Procession 75740 Paris Cedex 15 – France

Ifri.org