The false promise of Open RAN

Why Open RAN does not solve the “5G China challenge”

Digital Power China

A European research consortium

August 2022

Authors: Jan-Peter Kleinhans, Tim Rühlig

About the Digital Power China research consortium

The Digital Power China research (DPC) consortium is a gathering of China experts and engineers based in eight European research institutions, including universities and think tanks. In addition, a European non-resident fellow of a US research institution has joined DPC. The group is devoted to track and analyse China's growing footprint in digital technologies and its implications for the European Union. Based on interdisciplinary research DPC offers concrete policy advise to the EU. Tim Rühlig, Research Fellow at the German Council on Foreign Relations (DGAP), is the convenor of DPC and co-chairs the initiative with Carlo Fischione, who is a Professor at the Royal Institute of Technology in Stockholm.

DPC systematically pairs technological and country expertise. It is based on rigorous academic research that is combined with experience in the provision of policy advice. The informal group brings together a variety of European researchers in order to pair diverging perspectives from across the continent. Responsibility relies solely with the authors of this papers and chapters published by DPC.[1]

At the time of writing the chapters, the participating researchers were affiliated with the following institutions:

• Belgium:	KU Leuven
• France:	French Institute of International Relations (IFRI), Paris
• Germany:	German Council on Foreign Relations (DGAP), Berlin
	Jacobs University Bremen
	Mercator Institute for China Studies (MERICS), Berlin
	Stiftung Neue Verantwortung (SNV), Berlin
• Greece:	Athens University of Economics and Business
• Italy:	University of Insubria, Varese/Como
	University of L'Aquila
• Latvia:	Riga Stradins University
• The Netherlands:	Clingendael Institute, The Hague
	Leiden Asia Centre at Leiden University
• Sweden:	The Royal Institute of Technology (KTH), Stockholm
	The Swedish Institute of International Affairs (UI), Stockholm
	Uppsala University (UU)
• United States	Belfer Center for Science and International Affairs, Harvard University, Cambridge

[1] This publication is based upon work from COST Action CA18215 - China In Europe Research Network (CHERN - www.china-in-europe.net), supported by the European Cooperation in Science and Technology (COST - www.cost.eu).

The false promise of Open RAN

Jan-Peter Kleinhans, Tim Rühlig

Abstract

The question of whether to include Huawei technology in the rollout of Europe's 5G infrastructure has increased awareness of the vulnerabilities that stem from technological dependence on China. The high level of market concentration in the Radio Accession Network (RAN) market has led to Open RAN being presented as a solution, as it disaggregates the components of RAN. However, while Open RAN is a promising technological concept, it does not solve the "China challenge" as it neither reduces reliance on China nor necessarily offers a higher degree of network security.

The fifth generation of wireless infrastructure, widely known as 5G, has become the subject of geopolitical rivalry in recent years.[2] A group of states spearheaded by the United States (US) argues that Chinese technology suppliers, notably Huawei and ZTE, are untrustworthy. Their major concern is that the Chinese party-state ultimately controls technology firms based in the People's Republic of China (PRC), which could allow the authoritarian leaders in Beijing to exploit network insecurities and technological overdependence for political purposes. Several states have therefore either explicitly or de facto excluded Huawei and ZTE from their rollout of 5G infrastructure.

As a result, there is a risk of a further consolidation of the highly concentrated Radio Access Network (RAN) equipment market. Only three companies share around 80 percent of the global RAN market: Sweden's Ericsson, Finland's Nokia and China's Huawei.[3] There may be other RAN vendors, particularly in the transport network, core network and management software, but only four

[2] Jan-Peter Kleinhans. Europe's 5G challenge and why there is no easy way out. TechNode. 25 June 2019. https://technode.com/2019/06/25/europes-5g-challenge-and-why-there-is-no-easy-way-out/; and Tim Nicholas Rühlig, John Seaman and Daniel Voelsen. 5G and the US–China Tech Rivalry: A Test for Europe's Future in the Digital Age. SWP Comment no. 29. Berlin: SWP, 2019.

[3] Gabriel Brown et al. TIP OpenRAN: Toward disaggregated mobile networking. 30 June 2020. https://telecominfraproject.com/event/light-reading-tip-openran-towards-disaggregated-mobile-networking

companies are “full-stack” vendors able to offer tightly integrated solutions for radio, transport, core network and management software: Ericsson, Nokia, Huawei and ZTE.[4] Thus, the exclusion of Huawei (and ZTE) reduces the market options to two dominant players in the west, thereby potentially increasing the cost of RAN. More crucially, vendor diversity strengthens network security.[5] Banning Chinese suppliers for the sake of security could create other network security vulnerabilities as a result of the reduction in market options linked to less vendor diversity.

Some policymakers hope that a new technological concept could help to resolve this dilemma: “Open RAN”.[6] In contrast to currently deployed single-vendor solutions, Open RAN is intended to enable multi-vendor single RAN site implementation.[7] The Open RAN hardware and software components of a Radio Access Network are disaggregated, making it possible for them to be provided by separate suppliers. In a nutshell, mobile operators would not only have a choice between Ericsson, Nokia and Huawei, but also be able to freely pick RAN components from a range of suppliers. In theory, this would increase network diversity because disaggregation multiplies vendor choice. These hopes have led governments to approve major subsidies for Open RAN development (e.g., in the US and Japan).[8] The United Kingdom has increased its funding of Open RAN research and set a goal for “35% of the UK’s mobile network traffic to be carried over Open RAN by 2030”.[9]

Unfortunately, it is not that simple. While there is no denying the long-term potential of Open RAN, there are major pitfalls to this approach. Neither network security vulnerabilities nor overdependence on Chinese suppliers can be automatically resolved with Open RAN technology.

To substantiate this claim, this paper explains the concept of Open RAN and distinguishes it from similar terms, such as the O-RAN Alliance or the Open RAN Policy Coalition, that are often equated with it (section I). Next, the paper discusses the concerns raised about the inclusion of Chinese vendors in the rollout of 5G (section

[4] Daryl Schoolar and Jaimie Lenderman. Mobile Operators Have Many 5G Network Vendor Options. Omdia. 15 January 2021. https://omdia.tech.informa.com/-/media/tech/omdia/marketing/commissioned-research/pdfs/mobile-operators-have-many-5g-network-vendor-options.pdf.

[5] Council of the European Union, Council Conclusions on the Significance of 5G to the European Economy and the Need to Mitigate Security Risks Linked to 5G. Council Conclusions, 14519/19, 3 December 2019; and Deutscher Bundestag. “Experten gegen Ausschluss von Anbietern beim Mobilfunkstandard 5G. 22 November 2019”. https://www.bundestag.de/dokumente/textarchiv/2019/kw46-pa-auswaertiges-5g-665414.

[6] Mike Dano, “AT&T, Microsoft and others get behind Trump’s anti Huawei agenda”. 2 April 2020. https://www.lightreading.com/security/atandt-microsoft-others-get-behind-trumps-anti-huawei-agenda-/d/d-id/757286.

[7] While mobile operators use different RAN vendors for different geographic sites, mixing RAN components from different vendors in a single site (base station) is typically not possible today.

[8] Stephan Broszio. “Europe urged to act now to build Open RAN Ecosystem”. T. 18 November 2021. https://www.telekom.com/en/media/media-information/archive/recommendations-for-open-ran-640862

[9] UK Department for Digital, Culture, Media and Sport. 2021. “New measures to boost UK telecoms security”. Press release. 8 December 2021. https://www.gov.uk/government/news/new-measures-to-boost-uk-telecoms-security

II). Open RAN provides no solutions to these risks and two major pitfalls are considered (section III). The paper ends with a short summary and presents six considerations for policymaking in Europe (section IV).

I. What is Open RAN? A primer

The Radio Access Network is becoming more complex, transferring significantly more data each year, using an ever-increasing number of frequency bands, leading to the deployment of more and more cell sites (base stations).[10] In addition, today's mobile networks serve a variety of needs – from consumer-centric mobile broadband to mission-critical communications and massive Internet of Things communications. Naturally, mobile operators strive to keep operational expenditure low, and one trend is for the disaggregation of hardware and software in cell sites to increase flexibility and scalability.

A cell site consists of antennae, radio units that send/receive data, and base-band units that process data and communicate with the operator's core network. Traditionally, an entire cell site (antennae, radio units, base-band units) would have been procured from a single equipment vendor, such as Ericsson, Nokia, Huawei or ZTE, with tightly integrated software and hardware. Virtualized RAN (vRAN) is one trend within the industry for disaggregating software and hardware in the base-band unit. The functionality of a base-band unit is virtualized (a piece of software instead of a box) and can be deployed on standard cloud hardware from any cloud provider.

Open RAN pushes this concept further by virtualizing almost all functions within a cell site to enable it to be deployed on hardware from different vendors, including commercial-off-the-shelf (COTS) hardware. Thus, mobile operators do not purchase RAN equipment from one vendor, but can buy different components from different suppliers and combine them in a fully functioning RAN. The incentive for operators to push disaggregation is to increase competition among equipment vendors: "By separating hardware and software, you can get best of breed on each one. And that allows us, for example, to take a Samsung radio with an Ericsson baseband. And that allows us to play the suppliers against each other. And to their strengths, to be honest".[11]

Importantly, Open RAN technology is not necessarily open source. The "open"

[10] US Defense Innovation Board. "The 5g Ecosystem: Risks & Opportunities for DoD". April 2019. https://media.defense.gov/2019/Apr/04/2002109654/-1/-1/0/DIB_5G_STUDY_04.04.19.PDF

[11] Interview with Nicola Palmer, former Chief Technology Officer at Verizon. Mike Dano. "Editor's corner: This is why the wireless industry is running from cRAN to vRAN to oRAN". Fierce Wireless. 27 February 2018. https://www.fiercewireless.com/tech/editor-s-corner-why-wireless-industry-running-from-cran-to-vran-to-oran.

refers to open interfaces and the openness to combine technology from different suppliers. Open RAN components can be open source, but most of them are proprietary technology.[12] Equally misleading is the equation of Open RAN with the trustworthiness of the technology or its suppliers. Open RAN purely refers to open interfaces and not to any review mechanism for generating trust. In fact, Open RAN was not developed in the context of geopolitical concern over untrustworthy vendors, but in an attempt to reduce costs and increase the flexibility of the wireless infrastructure for mobile operators.

Interoperability relies on standardization: the O-RAN Alliance

A precondition of Open RAN is interoperability. All the different RAN functions need to be based on open interfaces that allow the various suppliers' components to be compatible and interact with each other.

The degree to which interoperability is necessary for Open RAN exceeds existing technical standards established by means of international technical standards organizations. All purpose-built solutions comply with technical standards cooperatively developed in international institutions such as the Third Generation Partnership Project (3GPP) or the International Telecommunications Union (ITU). Open RAN is based on the same technical standards but requires additional technical specifications that generate a higher degree of interoperability and open interfaces for RAN internal components.

These technical specifications for different RAN functions have mainly been developed within the O-RAN Alliance, which was established by five mobile operators.[13] AT&T, China Mobile, Deutsche Telekom, NTT Docomo and Orange established the O-RAN Alliance as a German entity in 2018. It is important to note that the O-RAN Alliance, as an industry consortium, does not necessarily comply with the World Trade Organization's or the European Union's criteria for technical standardization. In addition, in contrast to 3GPP, the five founding members have veto rights.[14] Furthermore, the O-RAN Alliance only develops technical specifications for 4G and 5G RAN. In developing economies that will have a significant 2G and 3G subscriber base for the foreseeable future, there are no technical specifications currently available. Finally, while 3GPP develops standards for a fully functional mobile

[12] Jean-Christophe Plantin. "The political hijacking of open networking: The case of open radio access network". European Journal of Communication, vol. 36, no. 4 (2021), pp. 404–17.

[13] Parallel Wireless. "Understanding the different OpenRAN groups in the telecoms industry". 3 August 2020. https://www.parallelwireless.com/blog/understanding-the-different-open-ran-groups-in-the-telecoms-industry/.

[14] European Commission. 5G supply market trends. 10 August 2021. https://data.europa.eu/doi/10.2759/833784

system, the O-RAN Alliance – as the name implies – focuses only on RAN.

The O-RAN Alliance has three main work streams: a "specification effort", which develops technical specifications based on existing technical standards for open interfaces; a "software community", which is developing open software for the RAN in close cooperation with the Linux Foundation; and the "testing and integration effort", which supports the community with testing and integrating the Open RAN technology developed by the Alliance.[15]

This distinction is noteworthy because the depth of cooperation across the three work streams is not uniform. The specification effort focuses on open interfaces and provides its participants with little detailed knowledge of other participants' technology. The O-RAN software community, by contrast, jointly develops software code for virtualization and automation specifications. This requires deep collaboration with little supervision in a field that considerably expands the attack surface of RAN technology.[16] Chinese actors are not excluded from any of the three work streams. The Software Community collaborates closely with the Linux Foundation, for instance, and China's technology giants Huawei and Tencent are both represented on the Linux Foundation's board of directors among many others (such as Sony, Oracle or Intel).[17]

O-RAN Alliance: global industry initiatives in times of geopolitical tension

The presence of one US, one Chinese, two European and one Japanese mobile operator is testament to the fact that the O-RAN Alliance is not an expression of geopolitical attempts to exclude Chinese actors from the rollout of mobile infrastructure.

In fact, the O-RAN Alliance united two earlier organizations: the US-based xRAN Foundation and China's C-RAN. According to the Alliance website, this was to create "global synergy [… enabling] rapid progress, accomplishing more in less time than the two earlier organizations could have done separately, while avoiding the risk of fragmentation of specifications".[18] The O-RAN Alliance has since established a formal link with the Telecom Infra Project (TIP), which brings together hundreds of participants from around the globe, including China.[19] China Unicom is particularly prominent in the

[15] O-RAN Alliance. About us. [n.d.]. https://www.o-ran.org/about.
[16] Hosuk Lee-Makiyama. European Centre for International Political Economy. "China's participation in O-RAN". January 2022. https://ecipe.org/blog/chinas-participation-o-ran/.
[17] Linux Foundation. Board of directors. [n.d.]. https://linuxfoundation.org/board-of-directors/.
[18] O-RAN Alliance. "Open and transparent way towards Open RAN by the O-RAN Alliance" [n.d.]. https://www.o-ran.org/blog/2021/10/11/open-and-transparent-way-towards-open-ran-by-the-o-ran-alliance.
[19] Telecom Infra Project. "Our community". [n.d.]. https://telecominfraproject.com/members/.

TIP and leads the Indoor 5G NR Small Cell Subgroup.[20]

This is not to argue that the O-RAN Alliance, TIP or the Linux Foundation are Chinese-led initiatives. Currently, around 20 percent of O-RAN Alliance members are Chinese entities.[21] Nonetheless, the O-RAN Alliance is anything but free from Chinese influence. However, this reflects the fact that the development of mobile networks has long been shaped by economic competition coupled with cooperation, rather than geopolitical cleavages. Not least, this is essential to satisfy the expectations of customers for highly reliable and compatible mobile networks, which requires an exceptionally high degree of technical standards. Such technical standards are developed jointly and cooperatively in international technical standardization organizations, primarily the 3GPP, with participation from across the globe regardless of geopolitical fault lines.

This cooperative approach contrasts with the Open RAN Policy Coalition, which was founded in 2020 and is free of Chinese participants and dominated by US actors.[22] In stark contrast to the O-RAN Alliance, the Open RAN Policy Coalition does not develop technical specifications. It is an advocacy group that promotes policies that support Open RAN solutions, lobbies for government procurement of Open RAN technology and funds Open RAN research and development, among other goals.[23]

In short, while similar in name, Open RAN, the O-RAN Alliance and the Open RAN Policy Coalition need to be distinguished between. Open RAN is a technology concept and trend within the industry. The O-RAN Alliance is an industry association of which only mobile operators can become official members, while equipment vendors, academics and everybody else are categorized as "contributors". The O-RAN Alliance develops technical specifications for open interfaces and software for Open RAN. Only the Open RAN Policy Coalition, a US advocacy group, reflects the geopolitical turn in wireless technology, since it does not have any Chinese members. The latter does not develop open interfaces or software: so why is the question of Chinese participation relevant?

[20] RWR Advisory Group. Chinese Companies Active in the Architecture of Open RAN. Washington, DC. 1 April 2021. https://www.rwradvisory.com/wp-content/uploads/2021/04/RWR_ORAN_Report_4-2021.pdf.

[21] RWR Advisory Group. Chinese Companies Active in the Architecture of Open RAN. Washington, DC. 1 April 2021. https://www.rwradvisory.com/wp-content/uploads/2021/04/RWR_ORAN_Report_4-2021.pdf.

[22] Open RAN Policy Coalition. "Leadership". [n.d.]. https://www.openranpolicy.org/about-us/board-and-executive-committee/.

[23] Open RAN Policy Coalition. "About us". [n.d.]. https://www.openranpolicy.org/about-us/.

II. Are Chinese vendors a risk to European 5G networks?

The inclusion of Huawei as a wireless technology vendor has triggered controversy in the west and some parts of Asia. Critics raise two primary concerns. First, that technological overdependence on Chinese suppliers could result from the limited number of vendors and Huawei's cost-effective solutions. Currently an oligopoly, the RAN market could become dominated by Huawei. If this were to happen, the west would not only give up its ability to construct its critical infrastructure, but also be reliant on a Chinese vendor to maintain it. Current wireless infrastructure already requires constant maintenance work; 5G and future generations of mobile infrastructure will be even more software-defined and the need for maintenance work will only increase. Critics argue that the EU would be entrusting the maintenance of its critical infrastructure to a technology company from an authoritarian state that is not a security ally of Europe.[24]

Second, 5G networks are highly complex, which increases the attack surface considerably. Critics fear that use of Huawei equipment would provide privileged knowledge and access for the vendor to the 5G network. Chinese party-state agencies could gain better opportunities for espionage and to sabotage wireless networks in Europe.[25] This would have much more grave consequences than today because 5G and 6G will be the backbone of a broad digitization of society and the economy. Shutting down 5G networks would disable not only mobile telephony, but also autonomous driving, machine-to-machine communication essential to industrial production, and smart home and smart health appliances, to name just a few examples.[26]

Concerns over technological dependence and network insecurity each assume that Huawei (and its Chinese competitor ZTE) are not private companies like any other, but instead could be subject to intervention by the Chinese party-state. Loopholes in Huawei's governance structure reinforce concerns that the company is ultimately controlled by the Chinese Communist Party.[27] Hence, both network insecurities

[24] Mathieu Duchâtel and Francois Godement. Europe and 5G: The Huawei Case. Paris: Institut Montaigne, 2019.

[25] Dan Sabbagh and Jon Henley. "Huawei poses security threat to UK, says former MI6 chief". The Guardian, 16 May 2019. https://www.theguardian.com/technology/2019/may/16/huawei-poses-security-threat-to-uk-says-former-mi6-chief; Tom Uren, "The technical reasons why Huawei is too great a 5G risk". ASPI. 14 June 2018. https://www.aspi.org.au/opinion/technical-reasons-why-huawei-too-great-5g-risk and Cassell Bryan-Low et al. "Special report: Hobbling Huawei, Inside the US war on China's tech giant". Reuters, 21 May 2019. https://www.reuters.com/article/us-huawei-usa-5g-specialreport/special-report-hobbling-huawei-inside-the-u-s-war-on-chinas-tech-giant-idUSKCN1SR1EU .

[26] James A. Lewis. How 5G Will Shape Innovation and Security: A Primer. Washington, DC: CSIS, 2018.

[27] Tim Rühlig. Who Controls Huawei? Implications for Europe. Stockholm: Swedish Institute of International Affairs, 2020.

and technological dependencies could become political tools in the hands of the authoritarian leaders in Beijing.[28] Huawei denies these accusations and argues that ownership of the company lies not with the Chinese state, but almost exclusively with its employees.[29] Huawei's claims are correct but the problem is not the ownership structure, but that ownership in Huawei's case does not come with control over the firm. That the PRC is using Huawei equipment for surveillance purposes and human rights infringements of Muslim minorities in China's north-western Xinjiang province has fuelled the concerns of the company's critics.[30]

Citing these concerns, countries such as Australia, Belgium, Estonia, India, Japan, the US, the UK, Lithuania, Sweden and Vietnam have either explicitly or de facto banned Chinese firms from their domestic mobile network rollout. Other states, such as Italy and France, have tightened regulations to make it more complicated for domestic mobile operators to develop their 5G networks with Huawei.[31] While Huawei has lost significant market share, it remains present not only in China, but also in a few European countries, such as Hungary and Cyprus,[32] and in large parts of the developing world, not least in Africa.[33]

Operators in states that have excluded Huawei technology are essentially left with the choice between RAN technology provided by Ericsson, Nokia and Samsung.[34] This lack of choice could increase prices and comes with potential network insecurities linked to a lack of vendor diversification. Diversification increases the costs of espionage and sabotage. To some observers, Open RAN is the solution to this dilemma: but does Open RAN reduce the risk of technological overdependence on China and provide improvements in network security?

[28] Jan-Peter Kleinhans. "Whom to trust in a 5G world? Policy recommendations for Europe's 5G challenge". Stiftung Neue Verantwortung. 5 December 2019. https://www.stiftung-nv.de/en/node/2717.

[29] Raymond Zhong. "Who owns Huawei? The company tried to explain: It got complicated". New York Times. 25 April 2019. https://www.nytimes.com/2019/04/25/technology/who-owns-huawei.html.

[30] Danielle Cave, Fergus Ryan and Vicky Xiuzhong Xu. Mapping More of China's Tech Giants: AI and Surveillance (Barton: ASPI, 2019). https://www.aspi.org.au/report/mapping-more-chinas-tech-giants.

[31] For an overview of sources to the relevant regulations, see Tim Rühlig and Richard Q. Turcsanyi. 5G and the political turn of technology in Europe. UI Policy Brief. (Stockholm: UI, forthcoming).

[32] Andreas Vou. "Data dominance: In Cyprus, a Chinese outpost inside the EU". BIRN. Nicosia. 7 December 2021. https://balkaninsight.com/2021/12/07/data-dominance-in-cyprus-a-chinese-outpost-inside-the-eu/.

[33] "Hungarian minister opens door to Huawei for 5G network rollout." Reuters. 5 November 2019. https://www.reuters.com/article/us-hungary-telecoms-huawei-idUSKBN1XF12U; and David Ehl. "Africa embraces Huawei technology despite security concerns." DW, 8 February 2022. https://www.dw.com/en/africa-embraces-huawei-technology-despite-security-concerns/a-60665700 .

[34] Bevin Fletcher. "Samsung scores $6B network deal with Verizon" Fierce Wireless. 8 September 2020.

III. Is Open RAN the solution to the geopolitics of 5G?

Open RAN as a concept and technology trend within the industry, and sometimes even the O-RAN Alliance, are cited as potential solutions to the strength of Huawei in 5G infrastructure and the related security concerns. A closer look, however, reveals similar technological dependencies and network security risks in Open RAN to those in single-vendor solutions. That is not to say that these cannot be resolved, but the same holds true for proprietary technology, as is demonstrated below.

A. Does Open RAN reduce technological dependencies on China?

The expectation that a disaggregation of RAN technology will minimize western dependence on Chinese technology is optimistic at best. Whether we consider single-vendor or Open RAN technology, China remains best positioned in the global market. The barriers to market entry for Radio Access Network technology, as well as its components, are high. Entry requires expertise and is highly capital intensive. High upfront costs mean that telecommunications tends to be a natural monopoly.[35] The global RAN market has consolidated for a good reason that will not automatically disappear with Open RAN.[36]

The global market share of Open RAN is still small.[37] It is estimated that 15 percent of global RAN could be Open RAN by 2026.[38] Others predict that Open RAN will only become a significant trend in the sixth generation of mobile infrastructure (6G). Either way, China's party-state will be able to sustain an uneven playing field by the very same means it has used to support Huawei.

According to the *Wall Street Journal*, Huawei has received at least US$75 billion in tax breaks, financing and soft loans in the past 25 years. The company has benefited from US$36 billion in cheap loans, credit lines and other support from state lenders alone. Between 2008 and 2018, Huawei saved US$25 billion in taxes due to state incentives to promote the tech sector. The company has also profited from cheap loans for its customers provided by Chinese state-owned banks. The China Development Bank and the Export-Import Bank of China are reported to have lent at least US$30

[35] Susan P. Crawford. Captive Audience: The Telecom Industry and Monopoly Power in the New Gilded Age. Yale University Press, 2013.

[36] Elsa B. Kania, "Why doesn't the US have its own Huawei?". Politico. https://www.politico.com/news/agenda/2020/02/25/five-g-failures-future-american-innovation-strategy-106378.

[37] StrandConsult. 2021. "Debunking 25 Myths of OpenRAN". [n.d.]. https://strandconsult.dk/debunking-25-myths-of-openran/

[38] Peter Cohen. "Open RAN will have 15% market share by 2026, report". RCR Wireless News. 24 January 2022. https://www.rcrwireless.com/20220124/open_ran/open-ran-revenues-forecast-to-15-of-ran-market-report.

billion to Huawei customers.[39] Huawei has refuted these numbers, but there can be little doubt that the company has profited from preferential treatment in a largely shielded domestic market,[40] public procurement policies, tax breaks, soft loans, subsidies and export credits.[41]

Since the Chinese party-state has an obvious interest in the promotion of Chinese wireless infrastructure vendors, it requires little imagination to see the authorities using the same means to support domestic suppliers of Open RAN equipment. This could create a situation in which the very same market concentration emerges for critical Open RAN components that we are currently witnessing in the market for proprietary RAN.

Huawei is by no means the most party-state controlled Chinese technology vendor. In China, it is not ownership but the degree of "state capture" that is pivotal. Through significant support from the party-state, state-owned and privately owned firms enjoy the same treatment in terms of access to markets, state subsidies, procurement and the exercise of political guidance. The economic and the political overlap in China. Based on publicly available information, 95 of the top 100 private sector firms in China and eight of the top ten internet companies have a founder or de facto controller who is currently or was formerly a member of a central or local party or party-controlled state organ.[42] These figures are based on publicly available data and are therefore likely to be a conservative estimate. This is not to deny that firms in China have agency. However, strategically important companies are best thought of as an integral part of the PRC's political economy: they are agents within the party-state complex and not separate from it.

The party-state's control over interest rates and the state-dominated banking sector allows it to grant loans at below market rates, while preferential treatment in procurement and public listings as well as the protection of regional or even national monopolies, in combination with corruption and coterie, preserve a high level of state control over the entire economy, including privately owned firms.[43] This may not apply to all firms across all sectors, but the risk of party-state control in strategic sectors such as RAN technology vendors is high. It would be irrational to believe that this holds true only for single-vendor and not for Open RAN solutions. In fact, strategic considerations of state-run think tanks in

[39] Chuin-wei Yap. "State Support Helped Fuel Huawei's Global Rise". Wall Street Journal. https://www.wsj.com/articles/statesupport-helped-fuel-huaweis-global-rise11577280736.

[40] Gareth Owen. "Mixed fortunes for Ericsson and Nokia in China 5G RAN tender". Counterpoint. 23 July 2021. https://www.counterpoint-research.com/ericsson-nokia-china/

[41] US Congressional Research Service. China's Recent Trade Measures and Countermeasures: Issues for Congress. Updated 10 December 2021. https://sgp.fas.org/crs/row/R46915.pdf.

[42] Curtis J. Milhaupt and Wentong Zheng. "Beyond ownership: State capitalism and the Chinese firm". Georgetown Law Journal, vol. 103, no. 3 (2015).

[43] Tim Rühlig. China Foreign Policy Contradictions. New York: Oxford University Press, 2022. Chapters 2 and 5.

China suggest that the country sees Open RAN as an opportunity to circumvent US sanctions.

Such probabilities are mirrored in the realities of the most influential existing Open RAN community: the O-RAN Alliance. Not only are 36 company participants in the O-RAN Alliance headquartered in China, but some of its most active members are subject to US sanctions. Inspur,[44] Kindroid,[45] Phytium[46] and H3C are on the US BIS Entity List for their involvement in military technology upgrading.[47] China Mobile, China Telecom and China Unicom are under US Treasury OFAC sanctions.[48]

Assessed against the backdrop of some Chinese O-RAN Alliance participants, Huawei appears to be a role model of transparency and independence from party-state influence. A recently published analysis of Chinese participants finds that at least two-thirds of the Chinese O-RAN Alliance members have elements of state-ownership, and six are outright public institutions or agencies. At least 16 O-RAN Alliance members have public links to the Chinese security apparatus, including ZTE, Sichuan Huihou, Grentech, HGTech, Nanjing Haojun, SageRAN, Spider Radio, Sunwave, Tsinghua University and H3C.[49]

Strikingly, all three of China's main mobile operators, China Mobile, China Telecom and China Unicom, participate in the O-RAN Alliance. All are state-owned and supervised by the Ministry of Industry and Information Technology (MIIT). All the companies have participated in the provision of telecoms infrastructure linking islands in the South China Sea that China claims in breach of international law. In the East China Sea, the three companies have reportedly provided an upgrade of signals intelligence and location services to the People's Liberation Army (PLA).[50]

[44] Timeline of Executive Actions on China. Updated 1 April 2021. https://www.uscc.gov/sites/default/files/2021-04/Timeline_of_Executive_Actions_on_China-2017_to_2021.pdf.

[45] Federal Register. Addition of Certain Entities to the Entity List; Revision of Existing Entry on the Entity List; Removal of Entity From the Unverified List; and Addition of Entity to the Military End-User (MEU) List. 12 July 2021. https://www.federalregister.gov/documents/2021/07/12/2021-14656/addition-of-certain-entities-to-the-entity-list-revision-of-existing-entry-on-the-entity-list.

[46] US Department of Commerce. "Commerce Adds Seven Chinese Supercomputing Entities to Entity List for their Support to China's Military Modernization, and Other Destabilizing Efforts". Press release. 8 April 2021. https://www.commerce.gov/news/press-releases/2021/04/commerce-adds-seven-chinese-supercomputing-entities-entity-list-their.

[47] Federal Register. Addition of Entities and Revision of Entries on the Entity List; and Addition of Entity to the Military End-User (MEU) List. 26 November 2021. https://www.federalregister.gov/documents/2021/11/26/2021-25808/addition-of-entities-and-revision-of-entries-on-the-entity-list-and-addition-of-entity-to-the.

[48] US Department of the Treasury. Issuance of Executive Order Addressing the Threat from Securities Investments that Finance Certain Companies of the People's Republic of China & related FAQs; Introduction of Non-SDN Chinese Military-Industrial Complex Companies List. 3 June 2021. https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20210603.

[49] Hosuk Lee-Makiyama. European Centre for International Political Economy. "China's participation in O-RAN". January 2022. https://ecipe.org/blog/chinas-participation-o-ran/.

[50] RWR Advisory Group. Chinese Companies Active in the Architecture of Open RAN. Washington, DC. 1

The case of China Mobile is particularly problematic. China's largest mobile operator is a founding member of the O-RAN Alliance with permanent membership of its Board of Directors and Executive Committee. The company also co-chairs ten of the 14 O-RAN Alliance working groups,[51] and is a member of the Alliance's influential Technical Steering Committee. The latter "decides or gives guidance on O-RAN technical topics and approves O-RAN specifications prior to the Board's approval and publication".[52] In 2016, China Mobile signed an agreement on civil-military fusion with the PLA.[53] In 2021, it was forced to delist from the New York Stock Exchange following US sanctions as a company that is part of the Chinese Military-Industrial complex.[54] Whatever one might think of Huawei, there is less evidence of party-state influence in the widely criticized company compared to O-RAN Alliance members.

In short, Open RAN solutions could help to circumvent the market power of Huawei, but the challenge is western overdependence not on Huawei, but on China. Nor does the concept of Open RAN prevent a dominant Chinese market presence in strategic segments of Open RAN equipment or the development of an unlevel playing field. There are clear indications that China has an active interest in Open RAN in order to circumvent US sanctions. It also has a strong presence in the O-RAN Alliance. In a nutshell, Open RAN provides no guarantee of less reliance on Chinese vendors. The only foreseeable shift that will come with Open RAN is the strengthening of cloud providers. As these are not European but mostly US or Chinese firms,[55] this is not necessarily in Europe's best interests.

B. Is Open RAN providing better network security?

Critics of Huawei are concerned that the Chinese equipment manufacturer or other Chinese actors could use advanced knowledge of the deployed RAN technology for espionage or to sabotage the wireless network and the critical infrastructure it connects. At worst, Chinese security services could use vulnerabilities or intentional backdoors to shut down the entire 5G network of an adversary, often referred to as a "kill switch".[56]

April 2021. https://www.rwradvisory.com/wp-content/uploads/2021/04/RWR_ORAN_Report_4-2021.pdf.

[51] Hosuk Lee-Makiyama. European Centre for International Political Economy. "China's participation in O-RAN". January 2022. https://ecipe.org/blog/chinas-participation-o-ran/.

[52] O-RAN Alliance. "About us". [n.d.]. https://www.o-ran.org/about.

[53] RWR Advisory Group. Military Ties of Major Chinese State-owned Telcom Companies: China Mobile, China Unicom, China Telecom. Washington, DC. 2 February 2021. https://www.rwradvisory.com/wp-content/uploads/2021/02/RWR_China_Telco_CCMCs.pdf.

[54] US Department of the Treasury. (note 47).

[55] Jean-Christophe Plantin. "The political hijacking of open networking: The case of open radio access network". European Journal of Communication, vol. 36, no. 4 (2021), pp. 404–17.

[56] Jan-Peter Kleinhans. "Whom to trust in a 5G world? Policy recommendations for Europe's 5G challenge". Stiftung Neue Verantwortung. 5

As argued elsewhere, however, the Chinese security services are advanced enough to conduct espionage or sabotage operations with or without the deployment of Huawei equipment.[57] This applies to Open RAN equipment too. Hence, the exclusion of Chinese vendors when deploying mobile networks provides only a limited increase in network security.

Encryption is a more effective tool for combating espionage and increasing the confidentiality of data than the exclusion of Chinese suppliers. Furthermore, while Chinese cyber-espionage is a crucial challenge, the overwhelming proportion of cyber espionage is carried out through phishing rather than mobile infrastructure.[58] The most effective means for reducing the risk of a kill switch is to increase the costs for a malign actor through vendor diversification. In a diverse network, an attacker needs to identify and exploit vulnerabilities in the equipment of not one, but several vendors.[59] At least in theory, the disaggregation of equipment in an Open RAN scenario eases network diversity and improves network security. Importantly, however, while Open RAN facilitates network diversification, it also presents two risks: (a) increased access to information among the Open RAN community while developing open interfaces and code; and (b) increased network insecurities when deploying Open RAN equipment linked to increased complexity and the potential involvement of untrustworthy vendors.

First, Open RAN requires a community of operators, vendors and researchers to develop open interfaces and software. This is not necessarily problematic. Cooperative technical standard-setting has not substantially compromised IT, cyber and network security. Instead, transparency and security standards have improved it. Similarly, the development of open interfaces for Open RAN appears fairly harmless since it provides little information on the actual equipment but focuses instead on the interfaces that are necessary for interoperability.

This appears to be riskier when code is jointly developed, as is the case in the O-RAN Alliance’s Software Community, as the complexity of RAN code provides multiple options for backdoors not only in a single piece of code, but also in the combination of them. It is unrealistic to expect constant review of all the code provided by all participants in an Open RAN software community. Olav Lysne, a

December 2019. https://www.stiftung-nv.de/en/node/2717.

[57] Tim Rühlig. Who Controls Huawei? Implications for Europe. Stockholm: Swedish Institute of International Affairs, 2020. https://www.ui.se/globalassets/butiken/ui-paper/2020/ui-paper-no.-5-2020.pdf.

[58] Thomas Brewster. “Chinese trio linked to dangerous APT3 hackers charged with stealing 407GB of data from Siemens”. Forbes. 27 November 2017. https://www.forbes.com/sites/thomasbrewster/2017/1 1/27/chinese-hackers-accused-of-siemens-moodystrimble-hacks/.

[59] UK Department for Digital, Culture, Media and Sport. UK Telecoms Supply Chain Review Report. July 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819469/CCS001_CCS0719559014-001_Telecoms_Security_and_Resilience_Accessible.pdf.

Norwegian professor of engineering, estimates that an expert in code analysis could review no more than 1000 lines of code per day, probably less. RAN software consists of thousands of components with millions of lines of code.[60] Hence, a proper security review of RAN code is not possible and absolute security of RAN code is unachievable. The trustworthiness of software suppliers is essential. As a consequence, Open RAN software is only as secure as the participants in any given Open RAN software community are trustworthy. Strikingly, some of the members of the O-RAN Alliance are more obscure and probably less trustworthy than Huawei.[61]

Second, while providing more options for vendor diversification, the deployment of Open RAN comes with additional network security challenges. These largely stem from the higher level of complexity of the various Open RAN network functions and from different suppliers interacting with each other.[62] Such increased complexity enlarges the attack surface of the RAN.[63] At the same time, the high level of virtualization theoretically has considerable potential to increase security. In short, Open RAN helps to resolve concerns over the lack of network diversification, but it comes with a variety of security challenges that stem from increased network complexity. Thus, Open RAN is by no means a silver bullet to increase mobile network security in the long term and poses very real security challenges in the short to medium term.[64] While the high level of virtualization and encapsulation of Open RAN solutions could increase network security, Open RAN development is not exclusively focused on security considerations. Interoperability, openness and time-to-market, to name just a few, are also important. The case that the network security of Open RAN is higher than that of single-vendor solutions is as yet unproven.

In summary, the characteristics of the O-RAN Alliance members outlined above provide some indication that trustworthiness cannot be assumed in Open RAN communities. Under Article 7 of the Intelligence Law, all Chinese actors are legally obliged to cooperate

[60] Thomas Lafarge and Rémi Labed. Chinese Cyberwarfare. ARTE Documentary, 2021, accessed: 2022-02-20, https://www.arte.tv/en/videos/092189-000-A/chinese-cyberwarfare/

[61] US Congressional Research Service. “China’s Recent Trade Measures and Countermeasures: Issues for Congress”. Updated 10 December 2021. https://sgp.fas.org/crs/row/R46915.pdf.

[62] Bundesamt für Sicherheit in der Informationstechnik.“Open-RAN Risikoanalyse”. 22 November 2022. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/5G/5GRAN-Risikoanalyse.html?nn=520690.

[63] "Security Considerations of Open Ran. Ensuring Network Radio Systems Are Open, Interoperable, and Secure by Design." Ericsson, 2021, accessed 2021-12-15, http://www.ercisson.com/en/security/security-considerations-of-open-ran .

[64] European Telecommunications Network Operators’ Association. State of Digital Communications, 2022. February 2022. https://www.etno.eu/downloads/reports/state_of_digi_2022.pdf.

with the Chinese security services.[65] Chinese intelligence has little interest in the cooperation of most companies, but it seems likely that they would be tempted to gain information from suppliers of critical infrastructure in third countries. All this leads us to the conclusion that Open RAN is not necessarily preferable to single-vendor solutions in the geopolitics of mobile networks.[66] The O-RAN Alliance, more specifically, is anything but a trustworthy partner and it is highly questionable whether cooperation in and the deployment of O-RAN Alliance compliant equipment can effectively address the vulnerabilities that have been identified in the discussions on the role of Huawei in the rollout of 5G.

IV. Conclusions and recommendations

Open RAN is a new concept mainly driven by mobile operators that some perceive as a potential solution to the geopolitics of wireless network infrastructure. This paper demonstrates that these are false hopes. Open RAN is a concept for disaggregating the software and hardware in RAN technology by means of open interfaces and virtualization. This is an innovative approach that could become an integral part of 5G and 6G RAN markets in the future. Open RAN should not be conflated with the O-RAN Alliance – an operator-led industry consortium driving the development of Open Ran specifications.

Open RAN is said to carry the promise of network diversification. Some observers hope that this will reduce dependence on Chinese vendors and improve network security. Both aspirations are open to question. Just as in the market for proprietary RAN equipment, Chinese suppliers are well positioned in the Open RAN ecosystem. It seems likely that Open RAN will come with chokepoints. The O-RAN Alliance is indicative of the profound interest of Chinese actors in Open RAN, not least in order to circumvent US sanctions against technology firms headquartered in China.[67] In fact, many members of the O-RAN Alliance are less transparent than Huawei, and have clear links to the Chinese Communist Party and the PLA. Some O-RAN Alliance members deliver surveillance technologies to Chinese state institutions in Xinjiang in support of breaching the human rights of Muslim minorities.

Nor does Open RAN necessarily increase network security. The collective development of code, as is the case with O-RAN

[65] Peking University Law Database, National Intelligence Law of the People's Republic of China (2018 Amendment) [Effective]. PKULaw. https://en.pkulaw.cn/display.aspx?cgid=313975&lib=law .

[66] Roslyn Layton. "OpenRAN: American Trade Policy Masquerading as Security". Forbes. 3 December 2021. https://www.forbes.com/sites/roslynlayton/2021/12/03/openran-americas-trade-policy-masquerading-as-security/.

[67] StrandConsult. "Debunking 25 Myths of Open RAN". [n.d.], https://strandconsult.dk/debunking-25-myths-of-openran/.

Alliance Software Community, requires a high degree of trust. Given that several Chinese O-RAN Alliance members are less trustworthy than Huawei, this initiative carries obvious risks to network security. The deployment of more diverse RAN technology to increase network security comes with new vulnerabilities that stem from increased technological complexity.

All this is not to deny the potential of Open RAN. For good reason, Open RAN is likely to gain market share in the coming years, albeit more slowly than many believe.[68] Open RAN may also be a significant factor in 6G. However, Open RAN is not a solution to the geopolitical concerns that have been raised with regard to Huawei.

Depending on how Open RAN is developed and deployed, geopolitical concerns can be mitigated to some extent. However, the same holds true for purpose-built solutions. Hence, the EU and its member states should neither dismiss Open RAN nor place too high hopes on the concept. We make the following four suggestions for consideration:

1. **Consider whether and when to support Open RAN.** Western governments, including from the United States, Japan, the United Kingdom and Germany, have promised financial support for the development of Open RAN. Before such support is provided, governments should carefully consider the structure and activities of the Open RAN community that they are supporting. This is essential to avoid unintended geopolitical outcomes. Support for Open RAN might be useful, but it does not mitigate geopolitical concerns. Hence, support for Open RAN should be justified by reasons other than geopolitical rivalry.[69]

2. **Get fit to assess more complex RAN.** Open RAN is technologically more complex. This heightens the need for proper regulation, assessment, testing and certification. The European Union and its members states should provide additional resources to regulators to enable them to identify critical network components and their functionalities.

3. **Invest in an analysis of the RAN ecosystem.** When relying on single-vendor solutions, RAN

[68] Dell'Oro. "Open RAN on track comprise 15 Percent of RAN by 2026, according to Dell'Oro Group". Press release. 21 January 2022. https://www.delloro.com/news/open-ran-on-track-comprise-15-percent-of-ran-by-2026/

[69] Iain Morris. "European telco VC arms have shown minimal interest in open RAN". Light reading. 1 June 2022. https://www.lightreading.com/open-ran/european-telco-vc-arms-have-shown-minimal-interest-in-open-ran/d/d-id/774416

vendors need to take action to protect their supply chain security, and monitor the quality, reliability and trustworthiness of their suppliers and equipment. Open RAN shifts such responsibilities to a great extent from vendors to service providers, integrators and a global community of developers,[70] and ultimately to public agencies. This will require a deep knowledge of supply chains, vendors and potential chokepoints. The development and maintenance of such expertise will require public investment by EU member states.

4. **Pool European resources for an EU regulator.** As indicated above, Open RAN shifts the burden from RAN vendors such as Ericsson and Nokia to operators and public regulators. Some EU member states might be able to live up to the requirements, but will need to devote substantial financial resources. Smaller EU member states will find it increasingly difficult to oversee their wireless networks as Open RAN gains significant market share. However, challenges to network security and the dependencies of single EU member states are no longer a national issue. The EU is highly interconnected and challenges to one EU member state are problematic for the entire EU. We therefore suggest a pooling of resources across the EU for a European regulator.

Authors:
Jan-Peter Kleinhans is the Director of Technology and Geopolitics at Stiftung Neue Verantwortung in Germany. Contact: jkleinhans@stiftung-nv.de
Tim Rühlig is a Research Fellow at the German Council on Foreign Relation and an Associate Research Fellow of the Swedish Institution of International Affairs' Europe program. He is based in Germany. Contact: ruehlig@dgap.org

[70] Gabriel Brown. "Open RAN security is a collaborative endeavor". Light reading. 3 July 2022. https://www.lightreading.com/open-ran-security-is-collaborative-endeavor/a/d-id/775849.

Digital Power China

A European research consortium