TAKSHASHILA INSTITUTION

Open RAN – Challenges and Pathways for Adoption

Bharath Reddy

Takshashila Discussion Document 2023-10
Version 1.0, September 2023

This document explores the origins and evolving narratives of Open RAN, analyses market trends, and explores concerns surrounding its adoption. It subsequently presents recommendations to help chart a reassuring path for its adoption.

Recommended Citation:
Bharath Reddy, "Open RAN - Challenges and Pathways for Adoption" Takshashila Discussion Document No. 2023-10, September 2023, The Takshashila Institution.

Executive Summary

Open RAN began as a mobile network operator (MNO) initiative to reduce lock-in, increase competition and improve vendor diversity in the radio access network (RAN) market. A few big companies dominate this market, and with bans on Chinese vendors by many states, the vendor pool has become even more concentrated. Consequently, what started as an MNO initiative has now acquired geopolitical significance. In addition to addressing concerns around the market power of vendors, it is now expected to enhance network security, reliability, and supply chain resilience.

There are some apprehensions regarding Open RAN's ability to meet these lofty expectations. These doubts arise due to multiple challenges. The new interfaces, disaggregated components, and adoption of open-source software are expected to increase the threat surface of the network. These concerns are further exacerbated by the increased complexity of integrating various components and the current stage of relatively limited deployment maturity.

Market trends suggest the enduring presence of Open RAN, necessitating a reassuring approach to adoption that effectively mitigates these concerns.

This document has been formatted to be read conveniently on screens with landscape aspect ratios. Please print only if absolutely necessary.

Examples of mobile network operators in India include Airtel, Jio, and Vodafone-Idea. Some prominent vendors for Radio Access Network (RAN) equipment include Huawei, Ericsson, Nokia, ZTE and Samsung.

Author
Bharath Reddy is a Researcher with the High-Tech Geopolitics Programme at the Takshashila Institution.

Regulators must be adept in evaluating Open RAN solutions due to complexity and security concerns, while operators need to master operation and maintenance skills. As global Open RAN deployments increase, investing in training becomes crucial. Initiatives like the USAID Asia O-RAN Academy, involving stakeholders from academics to operators, can effectively equip participants for new roles.

Open RAN commitments under the ambit of the Critical and Emerging Technologies initiative (iCET) and Quad should be realised to demonstrate scalability of the technology. This includes setting up a joint task force on Open RAN and pilot deployments to demonstrate the scalability of the technology. This can foster confidence and broader adoption by capitalising on economies of scale.

Lastly, Open RAN deployments can help balance the cost-effectiveness of Chinese components while mitigating security risks. Incorporating specific non-intelligent components from Chinese suppliers might not present a significant danger to national security. One possible candidate is the radio unit, deployed in vast numbers at every cell site. Selectively sourcing non-intelligent components from Chinese vendors can be a strategy to deescalate the critical vulnerability to an economic dependence that is manageable.

Acknowledgments

The author would like to thank his colleagues, Pranay Kotasthane and Shambhavi Naik for their valuable feedback and comments.

Table of Contents

Open RAN - Background and Origins

Open RAN has featured in multiple pivotal bilateral and multilateral technology partnerships in the past few months. It has been mentioned in the critical technology partnership between the United States and India[1] and in a joint statement between the United Kingdom, Australia, Canada, and the United States of America on the subject of Telecommunications Supplier Diversity[2]. Open RAN has even surfaced in discussions during the Quad leadership summit[3]. It is very unusual for an esoteric telecom industry term to be referenced in statements of national leaders.

The mobile telecommunications industry, which has high entry barriers and is dominated by a few big companies. The Radio Access Network, or RAN, provides the last-mile connectivity for mobile networks. The RAN includes a network of cell towers (or base stations) and other equipment that transmit and receive radio signals to provide wireless coverage. When you make a call, send a text, or use mobile data, your mobile device communicates with the RAN to establish a connection and transmit data. This part of the network is estimated to account for at least 60% of the capital and operating expenses[4] for the operators. The RAN offerings by

most big vendors have conventionally been tightly integrated solutions that require sourcing all the components from a single vendor.

Open RAN is an approach to building mobile telecommunications networks that makes components from different vendors work together. It makes it possible to have a plug-and-play installation of different components from multiple vendors. This allows smaller vendors to enter the market by building interoperable and modular components. Open RAN aims to reduce entry barriers, promote competition, reduce costs and avoid vendor lock-in by disaggregating the RAN ecosystem.

The disaggregation is proposed not just at the interfaces between different components but also between hardware and software. This allows systems to be set up on Commercial Off-The-Shelf (COTS) hardware. The Open RAN standards also support intelligent components essential to managing complex network deployments.

The O-RAN alliance and the Telecom Infrastructure Project have been at the forefront of Open RAN standardisation efforts. These initiatives were initially promoted by Mobile Network Operators (MNOs) in an effort to generate more competition and increase vendor diversity. However, these consortia have grown to include MNOs, software and hardware vendors, and research and academic institutions over the years.

While Open RAN was gaining traction over the past few years, telecom equipment from Chinese vendors such as Huawei and ZTE were banned or restricted from a growing list of countries, citing national security concerns. The list of countries includes India, the US, the UK, Australia, Canada and others. These bans further limit vendor choice and competition in an already concentrated market.

Following these bans, government interest has increased in promoting Open RAN. In December 2022, the United Kingdom, Australia, Canada, and the USA issued a joint statement on promoting diversity in telecommunications suppliers[5] . They emphasise their commitment to open and interoperable network architectures and outline collaborative efforts, including information sharing, joint R&D, ensuring security, supporting transparent standards, avoiding market fragmentation, and cooperating with international partners.

In June 2022, as part of the Critical and Emerging Technologies (iCET) initiative between India and the US, they announced the launch of public-private Joint Task Forces[6]. These were accompanied by funding support with the specific goal of advancing Open RAN systems in both countries. The objective is to showcase the scalability of this technology, thereby enhancing its competitiveness in global markets.

Thus, Open RAN, which started as an MNO-led initiative to increase vendor diversity, has also gained geopolitical significance and is expected to address network security concerns and supply chain resilience. While Open RAN could potentially address some of these expectations, it comes with additional challenges of low levels of maturity, complexities in system integration and security challenges. It is, therefore, essential to chart a reassuring, gradual path for its adoption.

Risks of Chinese Vendors Deploying Advanced Telecom Networks

Chinese telecom equipment vendors such as Huawei and ZTE have gained a significant portion of the global RAN market share by aggressively investing in research and development while maintaining competitive pricing[7]. Favourable policies and incentives from the Chinese government have facilitated this growth[8]. This equipment presents a value proposition to many operators seeking to deploy cost-effective solutions.

However, the widespread adoption of equipment from Chinese vendors is seen as a critical national security vulnerability for communication networks, leading to bans by many countries. Huawei's unclear ownership structure and susceptibility to Chinese government mandates add to the threat perception[9]. The potential risks include the existence of backdoors

that could enable espionage or sabotage of network equipment, particularly in times of conflict[10] [11].

Open RAN does not directly address the concerns linked to Chinese vendors. It's worth noting that Chinese vendors and operators are actively involved in shaping the Open RAN standards through organizations like the O-RAN Alliance. Nevertheless, the expectation is that Open RAN could increase competition and vendor options, particularly as the market has become more concentrated due to bans on Chinese vendors.

A Simplified Representation of Open RAN Deployments

For the discussion that follows a simplified representation of Open RAN deployments and a comparison with conventional RAN deployments will be useful. It is important to note that the many interfaces between Open RAN components or the different possible deployment options have not been shown here. The primary objective of this simplified illustration is to highlight the main features of Open RAN deployments.

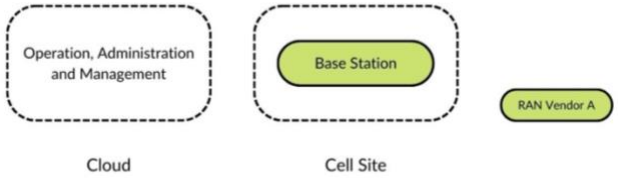

Figure 1: Conventional RAN deployment

Convention base station deployments are typically a black box base station deployed at the cell site, as shown in Figure 1. The operations, administration, and management functionality are typically located in the cloud, allowing the operator to configure and monitor the base station remotely. Typically, all components are sourced from a single vendor, which might sometimes include white-labelled components from other vendors. Operators might, however, use different vendor deployments for different geographies to have supplier diversity.

In an Open RAN deployment the base station can be broken down into the following components:

- Radio Unit (O-RU) which is like a translator and booster for wireless signals, making sure they are sent and received quickly and clearly between the mobile devices and the network.
- Distributed Unit (O-DU) handles traffic management, ensuring that the data is sent and received reliably.

- Centralised Unit - User Plane (O-CUUP) and Centralised Unit - Control Plane (O-CU-CP) handle activities like session management, authentication and mobility for mobile devices. They also control the operation of the O-DUs.
- Near Real-Time RIC (RAN Intelligent Controller) and Non-Real-Time RIC (RAN Intelligent Controller) are the brains behind the base station, handling spectrum management, load balancing, interference management and other functions.

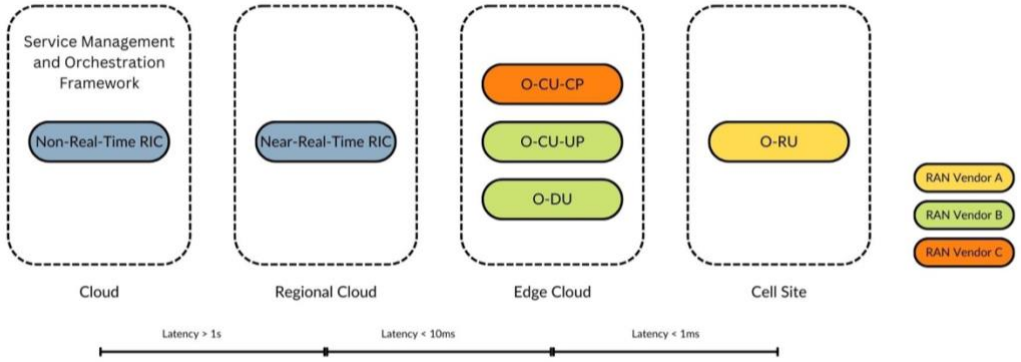

Figure 2a: A multi-vendor Open RAN deployment for illustration

Compared to traditional deployments, Open RAN deployments offer more flexibility in choosing vendors and deployment options. Figure 2a illustrates a potential deployment scenario, to convey three key points.

- Open RAN enables the possibility of deploying various components from different vendors, allowing these components to seamlessly work together through standardised interfaces established by the ORAN Alliance.
- It's not mandatory for all base station components to be situated at the actual cell site. Based on the latency requirements between modules, the O-RU component can be positioned at the cell site. Meanwhile, low latency components like the O-DU, O-CU-UP and OCU-CP components can be situated at an edge cloud server up to 20km from the cell site. The Near-Real-Time RIC can be located at a regional cloud server up to 200km away from the cell site. Additionally, the service management and orchestration framework, which includes the Non-Real-Time RIC, can be centralised to serve an even larger geographical area.
- Lastly, the different components can be deployed on general purpose COTS hardware at locations that offer the greatest efficiency for their intended purposes. In other words, the entire hardware and software need not be deployed at each cell site as with conventional base stations.

The last two points are not specific to Open RAN but are features of V-RAN (virtualised RAN) and C-RAN (cloud RAN) both of which are increasingly being adopted for 5G deployments.

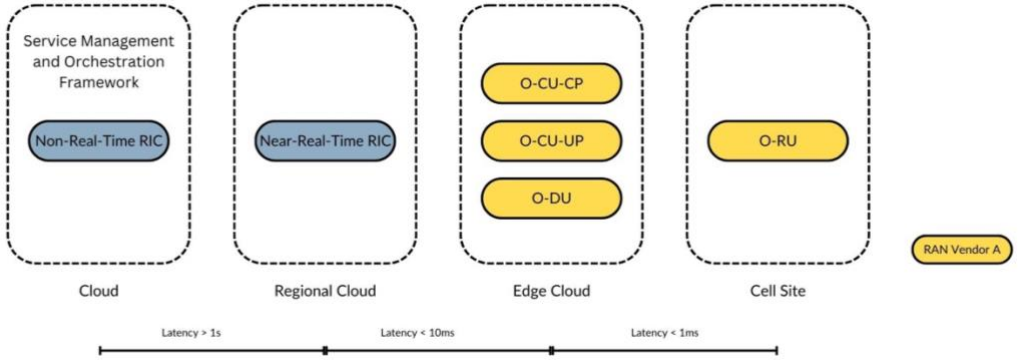

Figure 2b: A single-vendor Open RAN deployment for illustration

Figure 2b illustrates a deployment scenario using Open RAN compliant components but sourced from a single vendor. Due to the increased complexity in integrating components from multiple vendors initial Open RAN deployments are likely to be single vendor deployments.

It is important to note that the single vendor deployments do not increase interoperability or vendor diversity which are the primary objectives of adopting Open RAN.

Market Trends

The research and consulting firm Dell'Oro projects Open RAN deployments to constitute a substantial 15 to 20 per cent of the global RAN market by 2027[12]. The North American and Asia Pacific regions are leading the

commercial rollout, with over 95 per cent of the Open RAN revenue in the first three quarters of 2022 coming from these regions[13] .

Although the primary objective of Open RAN is to enhance vendor diversity and promote interoperability, achieving this goal in the near future seems unlikely. Operators often prefer to source all RAN components from a single vendor to avoid the complexities of systems integration. Consequently, this has resulted in a rise of Open RAN-compliant deployments that rely on a single vendor. For instance, Samsung offers end-to-end equipment aligned with Open RAN standards, and customers are deploying such single-vendor Open RAN solutions. Such deployments are likely till operators and vendors develop the expertise to handle the complexity of multi-vendor deployments.

Opting for a single-vendor solution is also expected to be more cost effective than a multi-vendor approach. Bundling end-to-end solutions as a single offering allows vendors to cut down on marketing and distribution expenses, minimise inventory requirements, and enhance the overall value of orders. Thus, the challenges for specialised vendors entering the market with specific RAN components remain substantial.

Even though Open RAN has gained traction, its influence on the overall concentration of the RAN market has remained rather modest. The combined market share of the five major RAN suppliers - Huawei, Ericsson,

Nokia, ZTE, and Samsung - only saw a slight decline of less than one percentage point between 2021 and 2022[14].

From an Indian perspective, despite initial expectations, telecom operators appear reluctant to embrace open RAN technology fully. This hesitancy is evident in recent 5G contract awards, as major players like Reliance Jio and Bharti Airtel have opted for traditional vendors such as Nokia, Ericsson, and Samsung for their 5G deployments[15]. The delayed rollout of 5G in India was expected to give a fillip to open RAN deployments, as the technology would have had time to mature. However, the decisions to stick to conventional deployments indicate that the maturity levels of Open RAN solutions for brownfield deployments are not yet up to the mark.

Another interesting dynamic of the Open RAN debate are the decisions on where and how to define the interfaces between modules. One of the interfaces, in particular, has significant implications for the cost and complexity of the components. Nokia, NEC, Fujitsu and others back the ORAN Alliance compliant “7.2x” standard, which keeps the design and functionality of the radio unit simple, whereas Ericsson, Huawei, ZTE and others prefer a more complex radio unit in order to implement certain high bandwidth applications effectively[16].

Increasing the complexity of the radio unit increases the hardware requirements, raises costs and also makes it more challenging for smaller

players to compete with the big vendors. This could adversely impact the goal of having a multi-vendor network. Such architectural decisions, which are ongoing, will have a significant impact on the cost and adoption of Open RAN systems.

The Prominent Advocates of Open RAN

O-RAN Alliance

The O-RAN Alliance was established in 2018 by merging two existing organisations: the xRAN Foundation in the US and the C-RAN consortium in China. It was founded by five major operators - AT&T, China Mobile, Deutsche Telekom, NTT DOCOMO, and Orange[17]. What began as a partnership among these five operators has since evolved into a worldwide community comprising more than 300 members, including operators, vendors, and academic institutions.

Officially registered in Germany, the governance of the O-RAN Alliance is outlined in its membership documents. A board of directors, made up of up to 15 members, governs the alliance. Decisions are reached through consensus or majority voting, with no individual possessing veto power.

The O-RAN Alliance seeks to enable a competitive and innovative RAN ecosystem to create open, intelligent, interoperable solutions. The Alliance's initiatives revolve around three main areas:

- Specification: This focuses on expanding RAN standards to incorporate openness, interoperability and intelligence.
- Software Development: This works towards creating and contributing open-source software for the RAN components within the Open RAN architecture.
- Testing and Integration: This guides Alliance members involved in testing and integrating their Open RAN-compliant solutions. It also does certification and badging of Open RAN-compliant solutions, which are awarded only to O-RAN Alliance members or participants

The O-RAN Software Community

The O-RAN Software Community (SC) is a collaboration between the O-RAN Alliance and the Linux Foundation[18]. The O-RAN SC is sponsored by the ORAN Alliance, with the objective of creating open-source solutions aligned with the architecture specified by the O-RAN Alliance that can be utilised for industry deployment.

Telecom Infrastructure Project

In 2016, the Telecom Infra Project (TIP) was established as an engineeringcentred effort to unite operators, infrastructure providers, system integrators, and various technology companies[19]. They aim to collaborate on creating innovative technologies and reimagining conventional methods for constructing and deploying telecom network infrastructure. The TIP has over 500 members and is jointly steered by its group of founding tech and telecom companies, which form its board of directors.

The TIP has a large ambit focusing on three broad areas - access, transport, core, and services. The Open RAN is one of the focus areas under the access vertical, and the TIP focuses on the disaggregation of RAN hardware and software on vendor-neutral, general-purpose-processor-based platforms. The TIP focuses more on deployment and execution, working to integrate equipment from various vendors to assess the readiness of products for commercial use. As an early advocate for Open RAN, the TIP has played a crucial role in raising awareness and bringing together a diverse community of stakeholders to concentrate on real-world deployment scenarios.

The Open RAN Policy Coalition

The main objective of the Open RAN Policy Coalition is to advocate for the standardisation and openness of protocols and interfaces within the RAN ecosystem. This aims to establish a modular deployment scenario that isn't reliant on a single vendor. However, in contrast to the other consortia, the Coalition primarily acts as an advocacy organisation[20] and highlights the role of the U.S. Federal Government in advancing Open RAN solutions. This includes activities like lobbying for government adoption of Open RAN technology[21], establishing partnerships to promote Open RAN[22], and providing funding for Open RAN research[23], among other initiatives. Notably, Chinese vendors and operators are absent from the Coalition[24], indicating the growing narratives around de-risking from China.

Apprehensions Regarding Open RAN Adoption

Increased Threat Surface

Abdalla et al., in their paper on what Open RAN can and cannot do, discuss the increased threat surface and security risks arising from Open RAN[25]. They point out that the Open RAN architecture with open interfaces and

interoperable components from multiple vendors raises security concerns such as:

- Interface Risks: These include improper ciphering across open interfaces, lack of proper authentication between components, or decision conflicts between components across interfaces, such as the "7.2x" standard discussed earlier could lead to security vulnerabilities.
- Disaggregation Risks: Functional decoupling and multi-vendor support result in the absence of a single source of trust. In addition, decoupling software and hardware without adequate safeguards could lead to vulnerabilities.
- Open-Source Software Risks: Implementing Open RAN using opensource software can expose the system to potential replication, testing, and hard-to-detect attacks.

Attacks could exploit these potential vulnerabilities to attack Open RAN systems. To counter these risks, it's crucial to establish robust security practices and raise awareness among all stakeholders within the RAN ecosystem.

Increased Complexity of Deploying Multi-Vendor Solutions

As discussed earlier, the deployment of multi-vendor Open RAN solutions is complex. However, opting for a single-vendor solution undermines the fundamental purpose of selecting Open RAN.

MNOs traditionally haven't been responsible for integrating components from multiple vendors, making this an exceptionally demanding endeavour. There are, however, other more viable alternatives for deploying Open RAN solutions. The first option involves a system integrator to integrate the various components into a functional solution. Early market trends indicate a preference for this approach in deploying multi-vendor Open RAN solutions[26].

The second approach, endorsed by the Telecom Infra Project (TIP), revolves around a blueprint detailing system requirements as specified by operators. Subsequently, TIP evaluates, validates, and certifies components that meet these criteria. This approach still entails some system integration effort on the part of operators.

Even post-integration and deployment, maintaining and upgrading Open RAN solutions would demand a skill set that operators might find formidable but necessary to acquire gradually. Operators of varying sizes might adapt differently to such transitions. Larger operators with greater

technical expertise should theoretically navigate this transition more smoothly than their smaller counterparts.

Open RAN's Evolving Narratives: Vendor Diversification to Geopolitical De-risking

Initially, Open RAN emerged as an initiative led by Mobile Network Operators (MNOs) to enhance vendor diversity. However, over the past few years, the bans on Chinese vendors have led to a further concentration within the vendor ecosystem. This, coupled with the growing entanglement of technology and geopolitics, has led to a change in narratives around Open RAN. Now, it also revolves around bolstering network security, reliability, and the resilience of supply chains. As discussed, particularly in the foreseeable future, objectives such as security and reliability could pose challenges when transitioning to Open RAN.

Conclusion and Recommendations

Open RAN introduces significant challenges, notably security concerns and additional deployment complexities. Transitions in stakeholder roles and responsibilities are also on the horizon. Prevailing market trends suggest

that Open RAN is here for the long term. This necessitates a systematic and reassuring approach to adoption to its adoption. The first two recommendations below focus on enhancing stakeholder capabilities and showcasing real-world scalability. These measures are poised to bolster confidence and encourage broader adoption by demonstrating the technology's viability in practical scenarios. The final recommendation attempts to leverage Open RAN's potential for capitalising on the cost-effectiveness of components offered by Chinese vendors while mitigating the potential national security risks.

Enhancing Capabilities for Operators and Regulators

Given the heightened complexity and security implications, regulators must be proficient in evaluating and authorising Open RAN solutions. Similarly, operators must cultivate the skills necessary to operate and maintain these systems effectively. As global Open RAN deployments continue to rise, the need for investing in training initiatives to foster expertise becomes paramount. These requirements will be felt across markets globally, and collaborative efforts can help address them effectively.

One such initiative is the USAID Asia O-RAN Academy, established by the US to equip participants from the Indo-Pacific region with the capabilities to test and implement Open RAN systems effectively[27]. The Telecom Regulatory Authority of India (TRAI) should take on the pivotal role of

promoting involvement from various stakeholders in order to encourage Indian participation in these capacity-building initiatives. Such multistakeholder skilling initiatives involving academics, technologists, operators, regulators, and vendors can help build capabilities and cross-domain knowledge sharing to equip participants to deal with the new roles and responsibilities effectively.

Demonstrate Scalability of Open RAN Deployments

The announcements under iCET to implement and demonstrate the scalability of Open RAN systems need to be put into action. The recent joint statement from India and the United States[28] mentions setting up a Joint Task Force focussed on Open RAN collaboration. It also refers to a 5G Open RAN pilot with a leading Indian telecom operator using equipment from a U.S. Open RAN manufacturer. Airtel or Jio could be promising candidates for such a pilot. Airtel has already contracted U.S.- based Mavenir to deploy Open RAN solutions in rural areas[29]. Collaborating initially with established operators with the technical know-how for dealing with the complexity of Open RAN deployments should prove beneficial.

As previously discussed, Open RAN deployments might be more costly in the near term than conventional systems, which will be a deterrent to adoption. The funding support announced under iCET could help incentivise Open RAN solutions for operators. The incentives should also promote

multi-vendor Open RAN deployments over single-vendor solutions. The initial demonstrations of scalability can build confidence and economies of scale, leading to wider adoption.

The commitment of the Quad leaders to Open RAN[30] also presents an opportunity to combine their complementary strengths and address the challenges faced in deploying Open RAN.

Open RAN Could Mitigate Risk of Deploying Chinese Vendor Equipment

Open RAN offers a means of taking advantage of the cost-effectiveness of equipment offered by Chinese vendors while mitigating the potential national security risks. Selectively sourcing non-intelligent components from Chinese vendors might not present a significant danger to national security. It can be a strategy to deescalate the critical vulnerability to an economic dependence that is manageable[31].

One possible candidate is the radio unit, deployed in vast numbers at every cell site. It translates and boosts radio signals at each cell site. On the other hand, the RIC (Radio Intelligent Controller) or Centralized Unit are less suitable choices because they handle more sophisticated functions, are centralized, and cover larger areas.

The Ministry of Communications and the Ministry of Home Affairs in collaboration with the Telecom Regulatory Authority of India, should evaluate the potential risks and impose bans on specific components from Chinese vendors instead of implementing a blanket ban on all components from these vendors.

Increased capital expenditures on telecom infrastructure contribute to increased costs for end consumers. Affordable internet access has positive externalities, including improved access to education, knowledge, and digitised government services. Bans on specific components instead of a blanket ban will reduce infrastructure costs without compromising on security concerns.

References

[1] The White House. “FACT SHEET: Republic of India Official State Visit to the United States.” The White House, 22 June 2023, https://www.whitehouse.gov/briefingroom/statements-releases/2023/06/22/fact-sheet-republic-of-india-official-state-visitto-the-united-states/. Accessed 4 Sept. 2023.

[2] UK Government. "Joint Statement on Telecommunications Supplier Diversity." GOV.UK, 8 Dec. 2022, https://www.gov.uk/government/publications/joint-statementbetween-the-united-kingdom-australia-canada-and-the-united-states-of-america-ontelecommunications-supplier-diversity/joint-statement-on-telecommunicationssupplier-diversity. Accessed 4 Sept. 2023.

[3] Open RAN Policy Coalition. "Update from the Quad Leaders' Summit." Open RAN Policy Coalition, 23 May 2023, https://www.openranpolicy.org/update-from-the-quadleaders-summit/. Accessed 4 Sept. 2023.

[4] Parallel Wireless. "Reducing the Total Cost of Ownership with Open RAN-Parallel Wireless." Parallel Wireless, 19 Aug. 2021, https://www.parallelwireless.com/blog/reducing-total-cost-of-ownership-tco-withopen-ran/. Accessed 4 Sept. 2023.

[5] UK Government. "Joint Statement on Telecommunications Supplier Diversity." GOV.UK, 8 Dec. 2022, https://www.gov.uk/government/publications/joint-statement-between-the-united-kingdom-australia-canada-and-the-united-states-of-america-ontelecommunications-supplier-diversity/joint-statement-on-telecommunicationssupplier-diversity. Accessed 4 Sept. 2023.

[6] The White House. “FACT SHEET: Republic of India Official State Visit to the United States.” The White House, 22 June 2023, https://www.whitehouse.gov/briefingroom/statements-releases/2023/06/22/fact-sheet-republic-of-india-official-state-visitto-the-united-states/. Accessed 4 Sept. 2023.

[7] Bloomberg News. “Huawei Rivals Apple, Meta With R&D Spending to Beat U.S. Sanctions.” Bloomberg, 25 Apr. 2022, https://www.bloomberg.com/news/articles/2022-04-25/huawei-rivals-apple-metawith-r-d-spending-to-beat-sanctions. Accessed 5 Sept. 2023.

[8] Kania, Elsa B. “Opinion.” Politico, 25 Feb. 2020, https://www.politico.com/news/agenda/2020/02/25/five-g-failures-future-americaninnovation-strategy-106378. Accessed 5 Sept. 2023.

[9] Kewalramani, Manoj, and Anirudh Kanisetti. “Takshashila Discussion Document - 5G, Huawei & Geopolitics - An Indian Roadmap — The Takshashila Institution.” The Takshashila Institution, 20 Sept. 2020, https://takshashila.org.in/research/takshashilareport-5g-huawei-geopolitics-an-indian-roadmap. Accessed 5 Sept. 2023.

[10] Uren, Tom. “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. Accessed 24 Sept. 2023.

[11] Federal Communications Commission. “FCC Designates Huawei and ZTE as National Security Threats.” Federal Communications Commission, 30 June 2020, https://www.fcc.gov/document/fcc-designates-huawei-and-zte-national-security-threats. Accessed 24 Sept. 2023.

[12] Dell’Oro Group. “5-Year Open RAN Forecast Revised Downward, According to Dell’Oro Group.” Dell’Oro Group, 19 July 2023, https://www.delloro.com/news/5-yearopen-ran-forecast-revised-downward/. Accessed 5 Sept. 2023.

[13] Light Reading. “Dell’Oro: Open RAN Beats Q3 Expectations.” Light Reading, 1 Dec. 2022, https://www.lightreading.com/open-ran/delloro-open-ran-beats-q3- expectations/d/d-id/782070. Accessed 5 Sept. 2023.

[14] Morris, Iain. “Open RAN Take-up Has Barely Left a Scratch on Big Vendors.” Light Reading, 1 Dec. 2022, https://www.lightreading.com/open-ran/open-ran-take-up-hasbarely-left-scratch-on-big-vendors/d/d-id/782099. Accessed 5 Sept. 2023.

[15] Kaur, Gagandeep. “Does Open RAN Have a Future in India?” Fierce Wireless, 18 Nov. 2022, https://www.fiercewireless.com/tech/does-open-ran-have-future-india. Accessed 5 Sept. 2023.

[16] Morris, Iain. “Ericsson and Pals Split Open RAN Community with Massive MIMO Plan.” Light Reading, 26 June 2023, https://www.lightreading.com/open-ran/ericssonand-pals-split-open-ran-

community-with-massive-mimo-plan/d/d-id/785432. Accessed 5 Sept. 2023.

[17] O-RAN Alliance. “Open and Transparent Way towards Open RAN.” O-RAN Alliance, https://www.o-ran.org/blog/open-and-transparent-way-towards-open-ran-by-the-oran-alliance. Accessed 5 Sept. 2023.

[18] O-RAN Software Community. “O-RAN Software Community.” O-RAN Software Community, 7 Dec. 2020, https://o-ran-sc.org/about/. Accessed 5 Sept. 2023.

[19] Meta. “Introducing the Telecom Infra Project.” Meta, 22 Feb. 2016, https://about.fb.com/news/2016/02/introducing-the-telecom-infra-project/. Accessed 5 Sept. 2023

[20] Weissberger, Alan. “Open RAN Policy Coalition: U.S. Attempt to Exclude Chinese 5G Network Equipment Vendors? – Technology Blog.” IEEE Communications Society, 5 May 2020, https://techblog.comsoc.org/2020/05/05/open-ran-policy-coalition-u-sattempt-to-exclude-chinese-5g-network-equipment-vendors/. Accessed 5 Sept. 2023

[21] Fletcher, Bevin. “Dish, Open RAN Coalition Cheer Senate Tech Bill Passage.” Fierce Wireless, 9 June 2021,

https://www.fiercewireless.com/tech/dish-open-ran-coalitioncheer-senate-tech-bill-passage. Accessed 5 Sept. 2023.

[22] The White House. "Quad Leaders' Joint Statement." The White House, 20 May 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/quadleaders-joint-statement/. Accessed 5 Sept. 2023.

[23] The White House. "FACT SHEET: Republic of India Official State Visit to the United States." The White House, 22 June 2023, https://www.whitehouse.gov/briefingroom/statements-releases/2023/06/22/fact-sheet-republic-of-india-official-state-visitto-the-united-states/. Accessed 4 Sept. 2023.

[24] Open RAN Policy Coalition. "Members." Open RAN Policy Coalition, 11 Aug. 2020, https://www.openranpolicy.org/about-us/members/. Accessed 5 Sept. 2023.

[25] Abdalla, Aly S., et al. "Toward Next Generation Open Radio Access Networks: What O-RAN Can and Cannot Do!" IEEE Network, vol. 36, no. 6, Nov. 2022, pp. 206–13, https://doi.org/10.1109/mnet.108.2100659.

[26] Dyer, Keith. "Who Will Integrate Open, Disaggregated Networks?" The Mobile Network, 28 Oct. 2022, https://the-mobile-network.com/2022/10/who-will-integrateopen-disaggregated-networks/. Accessed 5 Sept. 2023.

[27] U.S. Agency for International Development. “Launch of USAID Asia O-RAN Academy to Advance Connectivity in the Indo-Pacific.” U.S. Agency for International Development, 1 July 2022, https://www.usaid.gov/philippines/press-releases/jul-1- 2022-launch-usaid-asia-o-ran-academy-advance-connectivity-indo-pacific. Accessed 5 Sept. 2023.

[28] The White House. “Joint Statement from India and the United States.” The White House, 8 Sept. 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/09/08/joint-statement-from-india-and-the-united-states/. Accessed 24 Sept. 2023.

[29] ETTelecom. “Airtel ‘Looking Forward’ to Strengthening Partnership with Open RAN Vendors.” ETTelecom, 11 Aug. 2023, https://telecom.economictimes.indiatimes.com/news/industry/airtel-looking-forward-to-strengthening-partnership-with-open-ran-vendors/102643029. Accessed 24 Sept. 2023.

[30] Open RAN Policy Coalition. “Update from the Quad Leaders’ Summit.” Open RAN Policy Coalition, 23 May 2023, https://www.openranpolicy.org/update-from-the-quadleaders-summit/. Accessed 4 Sept. 2023.

[31] Kumar, Amit. “Takshashila Discussion Document – Defining Dependence-Induced Vulnerabilities in Asymmetrical Trade Interdependence: A

Conceptual Framework — The Takshashila Institution." The Takshashila Institution, 20 July 2023, https://takshashila.org.in/research/takshashila-discussion-document-definingdependence-induced-vulnerabilities-in-asymmetrical-trade-interdependence-aconceptual-framework. Accessed 5 Sept. 2023.

[32] Rühlig, Dr. Tim, and Jan-Peter Kleinhans. "The False Promise of Open RAN Why Open RAN Does Not Solve the '5G China Challenge.'" Publications Office of the EU, 10 Aug. 2022, https://dgap.org/en/research/publications/false-promise-open-ran. Accessed 4 Sept. 2023.

[33] Polese, Michele, et al. "Understanding O-RAN: Architecture, Interfaces, Algorithms, Security, and Research Challenges." arXiv.Org, 2 Feb. 2022, https://arxiv.org/abs/2202.01032.

[34] Balding, Christopher, and Donald C. Clarke. "Who Owns Huawei?" SSRN Electronic Journal, 2019, https://doi.org/10.2139/ssrn.3372669.

[35] Brown, Gabriel. TIP OpenRAN: Toward Disaggregated Mobile Networking. June 2020, https://telecominfraproject.com/tip-openran-toward-disaggregated-mobilenetworking/. Accessed 5 Sept. 2023.

[36] Quad Critical and Emerging Technology Working Group. "Open RAN Security Report." National Telecommunications and Information

Administration, May 2023, https://www.ntia.gov/report/2023/open-ran-security-report. Accessed 5 Sept. 2023.

[37] Morris, Iain. “Open RAN’s 5G Course Correction Takes It into Choppy Waters.” Light Reading, 17 July 2023, https://www.lightreading.com/open-ran/open-rans-5g-coursecorrection-takes-it-into-choppy-waters/d/d-id/785678. Accessed 5 Sept. 2023.

The Takshashila Institution is an independent centre for research and education in public policy. It is a non-partisan, non-profit organisation that advocates the values of freedom, openness, tolerance, pluralism, and responsible citizenship. It seeks to transform India through better public policies, bridging the governance gap by developing better public servants, civil society leaders, professionals, and informed citizens.

Takshashila creates change by connecting good people, to good ideas and good networks. It produces independent policy research in a number of areas of governance, it grooms civic leaders through its online education programmes and engages in public discourse through its publications and digital media.