RWR Advisory Group, LLC

Chinese Companies Active in the Architecture of Open RAN

April 1, 2021

TABLE OF CONTENTS

INTRODUCTION

Introduction to Open Radio Access Networks

Wireless communication is made possible by networks made of other, smaller subsystems. The "radio access network" (RAN) is the subsystem that connects individual wireless devices, such as cellular phones and computers, to the core network. As wireless communications service providers worldwide introduce fifth generation (5G) cellular systems that are built on the latest RAN technology, the impact of the growing number of restrictions being placed on the procurement of equipment from Chinese companies, especially Huawei, has raised concerns.

Until recently, Huawei has played a rapidly growing role in this market, most notably outside the United States. Their significant risk profile, however, derived from the problematic track record of the Chinese state in the cyber domain, has drastically undercut the viability and attractiveness of their offerings. As the product they sell has often been the most price competitive, made possible in large part by the subsidies they have received from the Chinese government, network operators and government representatives seeking alternatives are not surprisingly still looking for solutions that can deliver high-performing technology and security at reduced price points.

The pursuit of these objectives in the wireless equipment market has led to growing interest in a model dubbed "Open RAN," which is an approach to RAN design that is based on virtualization, automation and open interfaces between RAN subcomponents. Open RAN promises operators the ability to mix and match RAN components from different manufacturers (rather than being built as a proprietary end-to-end solution). As such, Open RAN is seen by many as a viable strategy for replacing Huawei with a similarly cost-effective solution, and one that avoids embedding untrusted Chinese companies into their 5G infrastructure.

In the enthusiasm for this new approach, however, the inconvenient reality of Chinese companies still being involved in shaping the Open RAN architecture – through their involvement in the groups establishing its specifications, particularly the O-RAN Alliance, as explained below – has not attracted much attention. While the risk and threat connotations are certainly different, it is worth remembering that the opposition to contracting with Huawei for 5G infrastructure solutions was based, not entirely on a lack of trust in the company itself, but more broadly on a lack of confidence in the Chinese Communist Party (CCP) and the risk associated with the influence it wields over Chinese companies.

As Open RAN solutions, which presumably need to be compatible with specifications developed by a group called the O-RAN Alliance, are expected to gain in popularity, this report is intended to improve the awareness and understanding of the role, influence and risk exposure that Chinese companies still play in this approach to network construction.

International Concern over China's Role in 5G Infrastructure

Despite Huawei's rise to be the largest provider of wireless equipment in the world,[1] the increasingly understood vulnerability of Chinese telecommunications companies to state-backed cyber intrusions ultimately undercut its value proposition. Market players and governments, particularly in the United States and Europe, grew concerned about Huawei's obligation to comply with directives from Beijing, including those that might stem from China's Cybersecurity Law, which went into effect in June 2017, and the National Intelligence Law that was enacted soon thereafter. These laws require Chinese corporations to comply with Beijing's aggressive national security intelligence-collection measures.[2, 3]

Despite the protestations of Huawei that saw the growing rejection of the company as politicized and a function of an overly aggressive Trump Administration, concern about Huawei and the susceptibility of Chinese technology companies to CCP interference has proliferated across parties and continents.[4, 5] Inside the United States, the Biden Administration is expected to sustain a number of the policies of its predecessor on this topic, and, internationally, the BT Group of the United Kingdom intends to replace Huawei equipment in order to comply with a UK decision from July 2020,[6] and EU countries, including France, Belgium, Sweden and Italy, have also placed procurement restrictions on Huawei equipment. Australia banned the company from supplying domestic 5G networks in 2018.[7]

While these examples pertain primarily to Huawei, the motivation behind them has been based on the exposure of the company to potential Chinese government influence, interference and control, rather than risk factors that might be considered more particular to the entity itself

[1] https://www.wsj.com/articles/huawei-loses-cellular-gear-market-share-outside-china-11615118400
[2] http://www.cac.gov.cn/2016-11/07/c_1119867116_3.htm
[3] https://www.rwradvisory.com/wp-content/uploads/2019/03/RWR-Huawei-Risk-Report-2-13-18.pdf
[4] https://www.bbc.com/news/newsbeat-47041341
[5] https://www.huawei.com/en/news/2019/2/guoping-global-3rd-party-assurance-cyber-security
[6] https://www.wsj.com/articles/huawei-loses-cellular-gear-market-share-outside-china-11615118400
[7] https://www.reuters.com/article/us-sweden-huawei-global-factbox/factbox-huaweis-involvement-in-5g-telecoms-networks-around-the-world-idUKKBN2751A1

(although such risk factors[8] are prevalent as well). Despite this shared international sentiment, China's involvement in the O-RAN Alliance (and other aspects of Open RAN), which seeks to inherit at least some of the business left behind by Huawei, has received less attention.

What About China's Role in Open RAN?

Indeed, as described below, the participation by Chinese firms in Open RAN – and the O-RAN Alliance that develops its technical specifications, in particular – is significant. As it relates to the risk connotations of this involvement, observers from both inside and outside China have made the point that Open RAN and the O-RAN Alliance is really just another way for the Chinese state to remain engaged and influential over global wireless communications networks, making the diminishment of Huawei's access more tolerable at a national strategic level.

As noted by John Strand of Strand Consult, a Danish consulting firm specializing in mobile telecommunications,

> "The O-RAN Alliance was established in 2018 by Deutsche Telekom, NTT DOCOMO, Orange, AT&T, and China Mobile and has grown to 237 mobile operators and network equipment providers. The U.S. has 82 O-RAN Alliance members; China, 44 (3 from Hong Kong); Taiwan, 20; Japan, 14; United Kingdom, 10; India, 10; and Germany, 7. Notably the 44 Chinese member companies exert significant control on the technical specifications and supply chain of OpenRAN 5G products and services."[9, 10]

Mr. Strand also noted,

> "There is no doubt that [Chinese firms involved in Open RAN] are representing China's system, and they are definitely representing Huawei in this process. The relationship between all these Chinese companies is different from what we see in the Western world."[11]

[8] https://www.wired.com/story/huawei-threat-isnt-backdoors-its-bugs
[9] https://techblog.comsoc.org/2020/12/17/44-chinese-companies-have-joined-the-o-ran-alliance
[10] See Appendix 1 for a list of the 44 Chinese domiciled O-RAN Alliance member countries, according to research conducted by RWR Advisory Group.
[11] https://www.voachinese.com/a/china-open-ran-5g-20210106/5727415.html

For other reasons, the Wilson Center's Melissa Griffith, analyzing the array of ways that Open RAN does – and does not – meet its national security expectations, concluded,

> "These technical standards cannot solve 'the China challenge' alone, nor is that likely to be the primary benefit of Open RAN."
>
> Melissa Griffith, Wilson Center

> "Open RAN is not a geopolitical hammer. It does offer important solutions to a critical set of security problems, but the security benefits of 5G are more complex than the geopolitical rhetoric would suggest. These technical standards cannot solve 'the China challenge' alone, nor is that likely to be the primary benefit of Open RAN. Overemphasizing great power competition between the U.S. and China (a) risks promising more than Open RAN can deliver while also (b) overlooking the wider range of opportunities it presents for the U.S. and other like-minded countries."[12]

Some specialists in China also appear to see strategic benefit in Open RAN (or at least the lack of significant downside). For example, Yang Jian, the Vice President of the state-affiliated Shanghai Institutes for International Studies described part of Open RAN's attractiveness to Beijing as its likely imperviousness to foreign sanctions (and restrictions on Chinese involvement) and, accordingly, the role it could play in ushering in a new era of digital governance and a digital non-aligned movement.

> "…utilizing the O-RAN Alliance to formulate access rules to deal with the issue of strong competition from Chinese companies is much better than the alternative of the U.S. State Department's hegemonic act of undermining…market rules."
>
> Yang Jian, Vice President of the state-affiliated Shanghai Institutes for International Studies

Specifically, he wrote the following in January 2021:

> "For many decision-makers around the world, […] utilizing the O-RAN Alliance to formulate access rules to deal with the issue of strong competition from Chinese companies is much better than the alternative

[12] https://www.wilsoncenter.org/article/open-ran-and-5g-looking-beyond-national-security-hype

of the U.S. State Department's hegemonic act of undermining multilateralism and market rules.'"[13]

To that end, Yang recommended Open RAN to the Chinese government calling on the state to "raise the banner of maintaining the 'compatibility and openness of the digital ecosystem.'" He described it as a path to creating a "digital non-aligned movement" and "[initiate] a new era of digital governance."

> "[The Chinese state should] raise the banner of maintaining the 'compatibility and openness of the digital ecosystem.'"
>
> "[Open RAN is a path to creating a] digital non-aligned movement [and] a new era of digital governance."
>
> Yang Jian, Vice President of the Shanghai Institute for International Studies

Chinese Companies Involved in Open RAN

Chinese companies, as individual entities, have reacted differently to the emergence of Open RAN. Whereas Huawei has made comments opposing the emergence of the solution as a viable alternative, the project has been backed enthusiastically by other Chinese firms, including the country's "Big Three" state-owned telecom companies, China Mobile, China Telecom and China Unicom.[14] These and other Chinese entities have been founders, leaders, participants and

Example Risk Factors Facing China Mobile, China Telecom, China Unicom

- In January 2021, China Mobile, China Telecom and China Unicom were delisted from the New York Stock Exchange following the issuance of Executive Order 13959, which prohibits any transaction in the publicly traded securities of companies designated by the U.S. Department of Defense as Communist Chinese Military Companies (CCMCs).
- China Mobile and China Telecom were listed as a CCMCs by the U.S. Department of Defense under the names of their parent entities (China Mobile Communications Corp. and China Telecommunications Corp.) in June 2020. China Unicom was listed under the name of its parent entity (China United Network Communications Group Co.) in August 2020.

[13] http://www.siis.org.cn/UploadFiles/file/20210315/当全球数字生态遭遇霸权政治_5G 市场谈判中的_华为冲突_杨剑.pdf;

[14] Citations for breakout section: https://www.reuters.com/article/us-china-usa-telecom/nyse-to-delist-three-chinese-telecoms-in-dizzying-about-face-idUSKBN29B1TR;

contributors in the O-RAN Alliance, the entity that is developing, approving and administering Open RAN's underlying technical specifications.

Each of these companies is exposed to risk factors, some similar to those that previously plagued Huawei. This report includes reference throughout to these risk factors in the context of some of the more significant and influential Chinese companies involved in advancing Open RAN initiatives – and its technical specifications in particular.[15]

Additional Risk Factors Facing China Mobile, China Telecom, China Unicom

- All telecommunications in China are supervised by the Ministry of Industry and Information Technology under the State Council. These three companies are obliged to comply with government policies and directives, as well as to uphold and protect China's national security and state secrets. This has resulted in these companies participating in national strategic initiatives (e.g., military-civil fusion) and strategic infrastructure projects (e.g., the telecom infrastructure linking illegally claimed islands in the South China Sea), the enabling of censorship (e.g., the suspension of services in selected areas), and alleged involvement in malicious cyber activities (e.g., the redirecting of internet traffic).

- All three companies have reportedly provided communications systems in the disputed Spratly Islands, not only to service civilian and military personnel, but also to upgrade daily operations, including signals intelligence and location services. In February 2018, the three operators signed a framework agreement with the PLA Navy South China Fleet to upgrade the 4G networks of the Paracel and Spratly Islands.

https://www.defense.gov/Newsroom/Releases/Release/Article/2472464/dod-releases-list-of-additional-companies-in-accordance-with-section-1237-of-fy/;

[15] Citations for breakout section: http://www.xinhuanet.com/english/2018-02/02/c_136944795.htm

The Role and Influence of Chinese Entities within Leading Open RAN Industry Groups

Two of the world's leading groups with regard to the development and advancement of Open RAN solutions are the O-RAN Alliance and the OpenRAN Project Group of the Telecom Infra Project (TIP). The O-RAN Alliance seeks to define the specifications underpinning Open RAN, while TIP's OpenRAN Project Group works to advance innovation and commercialization of the concept with new products and solutions. Chinese entities are present in each group, but most prominently in the O-RAN Alliance, where it features:

- over forty Chinese entities among its members and contributors, including China Mobile, China Telecom, and China Unicom;
- China Mobile as a founding and permanent member of its Board of Directors and Executive Committee, providing durable influence over the work of both groups;
- China Mobile as a member of its influential Technical Steering Committee; and
- over three dozen additional Chinese entities participating as contributors.

Chinese entities participating in TIP's OpenRAN Project Group include China Unicom,[16] which leads one of its

Additional Risk Factors Facing China Unicom

- On March 17, the U.S. Federal Communications Commission (FCC) announced that it had "launched a proceeding to determine whether to end China Unicom Americas' authority to provide domestic interstate and international telecommunications services within the U.S..."
- The FCC added, "China Unicom Americas is indirectly and ultimately owned and controlled by the government of the People's Republic of China. The Commission has raised concerns regarding the vulnerability of subsidiaries of Chinese state-owned enterprises to the exploitation, influence, and control of the Chinese government."
- "FCC staff reviewed China Unicom Americas' responses as well as comments from Executive Branch agencies that identified a number of significant national security and law enforcement concerns."

[16] Citation for breakout section: https://docs.fcc.gov/public/attachments/DOC-370866A1.pdf

specialized subdivisions, the Indoor 5G NR Small Cell Subgroup.

According to *Voice of America*, a survey report by Huaan Securities published in November 2020 stated that China is already an "important link" in the global Open RAN industrial chain, particularly in components including filters and connectors.[17] As the Open RAN project moves forward, it seems likely that this trend would continue, or even accelerate, as more Chinese firms enter the industry to manufacture the subcomponents for Open RAN networks.

The O-RAN Alliance

The O-RAN Alliance was founded in February 2018 as the result of a merger between the xRAN Forum and the C-RAN Alliance, the latter of which was established by the China Mobile Research Institute in 2010.[18, 19] Today, the O-RAN Alliance is the leading international body seeking to establish shared specifications and standards for 5G Open RAN architecture.[20]

Over the past three years, as Open RAN solutions loomed as a possibly more attractive option in light of Huawei's decline and increased government activism, the O-RAN Alliance has expanded into a community of over 220 mobile network operators and equipment suppliers, as well as a smaller number of research and academic institutions, all working toward the development of a standardized, shared and open architecture for products and solutions. Chinese entities make up a significant portion – roughly 20 percent – of these contributors, which is second only to the United States in terms of representation.

The O-RAN Software Community, an affiliated group, is a Linux Foundation project funded by the O-RAN Alliance to support the creation of software for Open RAN specifications that is derived from open-source contributions.[21] This is another avenue of potential Chinese input and involvement in the final Open RAN solution (addressed further below).

As a matter of policy, the O-RAN Alliance claims to "stay neutral in any political, governmental or other areas of any country or region." It says it does "not get involved in any policy-related topics." The nature of its business, however, involves solutions that have significant policy-related implications, as Huawei discovered over the course of the past few years.

---

[17] https://www.voachinese.com/a/china-open-ran-5g-20210106/5727415.html
[18] https://static1.squarespace.com/static/5ad774cce74940d7115044b0/t/5b8f55944ae237d9c09c46a0/1536120213353/xRAN+Press+Release+MWC2018+180227.pdf
[19] http://labs.chinamobile.com/focus/C-RAN
[20] https://www.o-ran.org/about
[21] https://www.o-ran.org/software

Chinese Entities in the Leadership Structure of the O-RAN Alliance

As one of the group's founders, China Mobile is a permanent member of the group's Board of Directors and a member of its Executive Committee.

According to the O-RAN Alliance Constitution, the Board is "responsible for the management and administration" of the O-RAN Alliance[22] and for creating any "activity," e.g., initiative, project, work-stream or task forces.[23] It also decides whether an entity can participate in the group. Resolutions on technical matters related to projects, however, are decided by two thirds majority.

The smaller Executive Committee, meanwhile, serves a supporting role, proposing the agendas, priorities, projects, and releases for the Board to consider and approve. It also serves to advise the Board and break ties that surface during votes at the annual meetings.[24]

China's other "Big Three" state-owned telecommunications operators (i.e., China Telecom and China Unicom) also play a significant role in the O-RAN Alliance, with all three among the group's 28 network operator members.

Additional Risk Factors Facing China Mobile

- China Mobile has been deeply involved in the efforts of the People's Liberation Army (PLA) to improve military communications. Past projects include constructing local military telephone networks, developing smart military bases, and providing emergency communication support during major military exercises and events.
- China Mobile signed a strategic agreement on military-civil fusion with the PLA on December 9, 2016. Under the agreement, China Mobile was to play a role in building an integrated army network information system to bolster multi-domain combat effectiveness. The two sides agreed to cooperate in seven areas: information infrastructure, emergency communications support, command and control, smart military bases, information systems and resource development, information security, and informatization talent training.

[22] https://static1.squarespace.com/static/5ad774cce74940d7115044b0/t/5fc0dba3173fb5383bc206b0/1606474661974/O-RAN+e.V.++Constitution+27-06-2018+Exhibit+A+v01+EN+clean.pdf
[23] https://static1.squarespace.com/static/5ad774cce74940d7115044b0/t/5fc0da39eaf37e3b64bbaa2a/1606474297855/O-RAN+Participation+Guidelines+27-06-2018+v03.pdf
[24] Citation for breakout section: http://military.people.com.cn/n1/2016/1212/c1011-28941711.html

Prevalence of Chinese Companies among the O-RAN Alliance Membership

There are also numerous Chinese entities among the O-RAN Alliance's participants. Most entities (including those based in China) participate in the alliance as contributors, a category which includes manufacturers, vendors, and research institutes.

The O-RAN Alliance differentiates between "members" (i.e., mobile operators that test the resulting technology) and "contributors" (i.e., organizations that propose standards, such as enterprises and research institutes). Chinese entities participate as members and contributors, including equipment suppliers and research institutions.

Chinese contributors to the O-RAN Alliance are diverse. They include: the China Academy of Information and Communications Technology (CAICT); the China Information and Communication Technologies Group Corporation (CICT); Inspur Group; Lenovo; State Grid Information & Telecommunication Group Co., Ltd.; Tsinghua University; and ZTE.[25] Most of these entities are

Example Risk Factors Facing Tsinghua University

- Tsinghua University was designated "very high risk" by the Australian Strategic Policy Institute for its high level of defense research and alleged involvement in cyber-attacks.

Example Risk Factors Facing ZTE Corporation

- On March 12, 2021, the U.S. Federal Communications Commission (FCC) designated five Chinese companies, including ZTE, as national security risks. By law, the FCC is required to determine which companies producing telecommunications equipment and services "have been found to pose an unacceptable risk to U.S. national security."

Example Risk Factors Facing Inspur Group

- Inspur Group was listed as a CCMC by the U.S. Department of Defense in June 2020.

Example Risk Factors Facing CAICT

- According to New America, CAICT experts contribute to major policy initiatives and CCP legislative efforts, such as the same Cybersecurity Law that has contributed to governments around the world questioning the wisdom of inviting Chinese companies into their 5G infrastructure.

[25] Citations for breakout section: https://unitracker.aspi.org.au/universities/tsinghua-university/; https://docs.fcc.gov/public/attachments/DOC-370755A1.pdf; https://www.newamerica.org/cybersecurity-initiative/digichina/blog/profile-china-academy-information-and-communications-technology-caict/;

state-owned. CAICT in particular is a subordinate organ of China's Ministry of Industry and Information Technology (MIIT).

Chinese Entities Involved in Setting Specifications as Part of the Steering Committee of the O-RAN Alliance

Another important aspect to China's role in the O-RAN Alliance comes via China Mobile's participation in the group's Technical Steering Committee (TSC).[26] The TSC "decides or gives guidance on O-RAN technical topics and approves O-RAN specifications prior to the Board's approval and publication."[27]

The TSC is currently co-chaired by a Professor at Stanford University, Dr. Sachin Katti and the Chief Scientist of China Mobile, Dr. Chih-Lin I, an industry-recognized leader in wireless communications who joined China Mobile in 2011. Dr. I was previously a participant in China's National Thousand Talents Program, which has come under scrutiny outside China for allegedly facilitating technology

Additional Risk Factors Facing China Mobile

- The China Mobile Grand Connection Strategy Civil-Military Integration Summit was held in Beijing on July 30, 2018 in commemoration of the 91st anniversary of the establishment of the People's Liberation Army (PLA). The forum was sponsored by several branches of the company including: China Mobile Beijing; China Mobile Government and Enterprise; China Mobile International; and China Mobile Internet of Things, jointly with the Civil-Military Integration (Beijing) Equipment Technology Research Institute.
- Attendees included representatives from the Civil-Military Integration Promotion Department of China's Ministry of Industry and Information Technology, the Science and Technology Committee of the PLA General Armament Department (renamed the Equipment Development Department), the PLA Air Force Equipment Research Institute, and the PLA Academy of Military Sciences.
- Fan Yunjun, general manager of China Mobile Beijing, gave a speech at the event on the importance of information and communications technology (ICT) in strengthening the PLA. Fan stated that China Mobile "fully implements Xi Jinping Thought on building a strong military" and pledged to deepen the company's participation in the national strategy of military-civil fusion.

https://www.defense.gov/Newsroom/Releases/Release/Article/2472464/dod-releases-list-of-additional-companies-in-accordance-with-section-1237-of-fy/

[26] Citation for breakout section: https://www.sohu.com/a/244271478_727324

[27] https://www.o-ran.org/about

theft.[28, 29] It has been described by the Federal Bureau of Investigation (FBI), for example, as a vehicle for unconventional espionage.[30]

The OpenRAN Project Group of the Telecom Infra Project

Founded in 2016, the Telecom Infra Project (TIP) is a group of companies that came together "to develop, test, and deploy open, disaggregated, and standards-based solutions that deliver the high-quality connectivity that the world needs."[31] TIP has reached agreement with the O-RAN Alliance to adopt its specifications within its OpenRAN 5G NR project, a key research and development (R&D) initiative of the group that involves the development of 5G base station equipment.[32] The mission of TIP's OpenRAN Project Group is to "accelerate innovation and commercialization in [the] RAN domain with multi-vendor interoperable products and solutions that are easy to integrate into the operator's network and are verified for different deployment scenarios."[33]

The Involvement of Chinese Entities in TIP and the TIP OpenRAN Project Group

Chinese companies are participants in TIP, which currently has a membership of over 1,000 entities. Arguably the most notable Chinese entity participating in TIP is China Unicom. The China Mobile Research Institute, which has been active in the O-RAN Alliance, is also a member. Other Chinese members of TIP include Beijing Huahuan Electronics Co., Ltd., Fu Hua Ke Precision Industry (Shenzhen) Co., Ltd., and Nanjing Huastart Network Technology.[34]

[28] https://ieee-wf-5g.org/biography-of-chih-lin-i/
[29] https://www.nytimes.com/2020/02/06/us/chinas-lavish-funds-lured-us-scientists-what-did-it-get-in-return.html
[30] https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states
[31] https://exchange.telecominfraproject.com/rfi
[32] http://www.iccsz.com/site/cn/News/2020/02/28/20200228034329048396.htm
[33] https://telecominfraproject.com/openran/
[34] https://telecominfraproject.com/members/

The Influence of Chinese Entities within TIP

China Unicom, which joined TIP in 2018, seems to be the most active Chinese entity in the organization.[35] Among the OpenRAN Project Group's subdivisions, China Unicom is an integral part of shaping the indoor deployment of 5G through its leadership in the Indoor 5G NR Small Cell Subgroup. The group is jointly led by Rong Huang of China Unicom and a representative of T-Mobile. China Unicom has made several substantive contributions to the subgroup since joining in 2018.[36]

In February 2020, for example, China Unicom signed a joint R&D agreement with the OpenRAN Project Group to build the first community laboratory in China in support of OpenRAN 5G NR's work and to promote China Unicom's efforts to conduct development, test verification, and commercial deployment of 5G open base station

Additional Risk Factors Facing China Unicom

- China Unicom has been a significant contractor to the PLA, including its provincial branches for the supply of switchboards, fiber-optic cables, smart military base systems, and other equipment for PLA units – in particular, newly formed or reorganized corps-level units. China Unicom also provides PLA engineering training.
- A Mandiant report published in February 2013 found that the APT1 cyber espionage unit was based in the PLA General Staff Department's 3rd Department, 2nd Bureau (Unit 61398). APT1 has primarily targeted U.S. corporations in various sectors, including aerospace, information technology, government, energy, and transportation. The majority of cyber-attacks by APT1, which involve injecting malware and gaining remote desktop or software access, reportedly originated from Chinese IP addresses registered to China Unicom Shanghai Network.
- China Unicom reportedly enabled North Korea's first full-time, wide-bandwidth internet connection, linking the country via a connection through China. Subsequent reports showed many IP addresses from the country registered as having been assigned by China Unicom.

[35] https://telecominfraproject.com/events/mwc-2018/

[36] Citations for breakout section: http://www.zbytb.com/s-zb-1691549.html; http://www.huixinsy.com/article/936.html; http://blog.sina.com.cn/s/blog_a3f2f5990102y2qa.html; http://www.chinaunicombidding.cn/jsp/cnceb/web/info1/detailNotice.jsp?id=2861703300000010774; http://www.sdzps.com/knowledge/1503911320832.html; http://his.wmxa.cn/h/201506/249239.html; http://zx.ejmrh.com/mcjhtml/armyInformationBuild/20180102/21555.html; http://changsha.caiep.net/changsha_wenjiaodanwei/content.php?id=59787; https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-083.pdf; https://arxiv.org/pdf/1602.07128v1.pdf; https://www.38north.org/2017/10/mwilliams100117/; https://nknetobserver.github.io; https://www.whoishostingthis.com/blog/2016/11/09/north-korea-internet/; https://www.northkoreatech.org/2011/06/26/north-koreas-chinese-ip-addresses/

systems.[37] More recently, in October 2020, China Unicom published the requirements for disaggregated indoor small cells, within the Indoor subgroup.[38]

[37] http://www.iccsz.com/site/cn/News/2020/02/28/20200228034329048396.htm

[38] https://telecominfraproject.com/tip-community-achieving-significant-momentum-on-the-path-to-open-interoperable-disaggregated-and-standards-based-networks/

OTHER CHINESE ENTITY ACTIVITIES RELATED TO OPEN RAN

Beyond state-owned Chinese corporate involvement in Open RAN standard-setting groups, Chinese entities are also involved in a variety of other aspects of Open RAN's development as well as its current and potential future product offerings.

Open RAN's Use of Open-Source Code and the Associated Risks

As also noted by Dr. Griffith from the Wilson Center, "the usage of Open RAN as a generic industry or policy term has expanded to also include two processes aided by open interfaces," one of which is "the decoupling of the software layer of the network from the underlying hardware (i.e., the ability to run one vendor's software - increasingly the layer where the core functions of the network are located – on another vendor's hardware)." Pointing to the role of open-source code in the software layer of the network, Dr. Griffith adds,

> "The second mechanism for addressing security concerns hinges on a core bi-product of standards-based, interoperable interfaces: visibility into the network. While the breadth and functionality of software in 5G networks brings with it a host of security concerns, disaggregating the network and decoupling the hardware and the software allows for greater visibility into the hardware and software comprising these networks. Harkening back to the longstanding debate over the relative security of open vs proprietary systems, the argument here is that more eyes are better than less. Or as Dish's Stephen Bye noted, 'it's a lot easier to find the cockroaches when the lights are on.'
>
> However, when it comes to the broader security of 5G networks, Open RAN leaves more open questions than it does closed. More eyes are not always better. More can also mean more malicious eyes. Moreover, more eyes does not necessarily correspond with greater and more valuable scrutiny."[39]

Although "open-source" code is predicated on the notion that its "openness" would allow for other contributors to identify bad faith actors and dubious code (and thus could be self-monitoring) this outcome assumes that the community is able to carefully review the code in its entirety. U.S.-based technology company, Synopsis, is among those that have pointed to the associated risks, noting in a report, entitled "2020 Open Source Security and Risk Analysis

[39] https://www.wilsoncenter.org/article/open-ran-and-5g-looking-beyond-national-security-hype

Report," that 99% of codebases audited in 2019 contained open source components, of which 49% contained high-risk vulnerabilities."[40] While these vulnerabilities were not attributed and cannot necessarily be determined to have been intentional, use of open source code inherently raises the possibility of exploitation by bad actors in the cyber domain, including those backed by the Chinese state.

Although it is difficult to ascertain just how much code Chinese state-backed entities could be contributing to Open RAN software, contributors based in China have been very involved in projects of a similar nature. Per some sources, for example, Chinese developers represent the third-largest block of developers contributing to Cloud Native Computing Foundation projects, and the second-largest group contributing to GitHub-hosted repositories.[41]

The Kubernetes example is a particularly suitable one. Kubernetes is an open-source system for automating deployment, scaling, and management of containerized applications. Initially skeptical, Huawei has been a user and vendor of the software since 2016, acquiring a seat in the Kubernetes Steering Committee – a 7-member body, overseeing the governance of the Kubernetes project – in November 2017.[42, 43] In a statement, the company referred to itself as "core member of the Kubernetes community since its establishment" and as having the top spot among Chinese vendors in terms of contribution to the Kubernetes Community. According to Stackanalytics, Huawei and ZTE jointly account for roughly 5% of the total commits – a raw measure of contributions – to the Kubernetes code repository.[44] By way of raw comparison, Google and Red Hat (the two largest contributing entities) account for 40.3% and 15.7%. These numbers, however, serve as a general metrics for contributions and does not speak to the length or quality of each contribution.

Kubernetes is also an example of how Chinese state-affiliated entities' contributions to different open-source projects can become layered and compounded overtime. Because of the value of cloud-native architecture to the development of Open RAN, Kubernetes, as one of the leading systems for container-orchestration, is among the platforms that will reportedly play an increasingly important role in the development of Open RAN.[45]

[40] https://www.synopsys.com/software-integrity/resources/analyst-reports/2020-open-source-security-risk-analysts.html
[41] https://www.techrepublic.com/article/how-china-became-a-hero-in-open-source/
[42] https://kubernetes.io/case-studies/huawei/
[43] https://www.huawei.com/en/news/2017/11/Huawei-Kubernetes-member
[44] https://www.stackalytics.com/cncf?project_type=cncf-group&release=all&metric=commits&module=kubernetes
[45] https://www.ericsson.com/en/blog/2020/8/the-four-components-of-cloud-ran

Testing and Integration

Testing and integration are two major aspects of developing Open RAN due to the project's focus on vendor-neutrality and interoperability. As with contributions to code, in this respect too some Chinese entities have become active contributors to the process. The clearest example of Chinese participation in testing and integration efforts is China's hosting of trials, better known as "plugfests," that take on functional, interoperability and performance challenges to verify the readiness of Open RAN implementation.

The Asia Session of the O-RAN Alliance's first international "plugfest" in late 2019 was held in the China Mobile International Information Port, an Open Test and Integration Center (OTIC) with physical attendance well over 200 attendees from over 70 companies, in addition to online attendance of over 70 participants.

The OTIC initiative was launched in September 2019 by a group composed of primarily Chinese entities, including China Mobile, with the goal of helping make products and solutions functionally compliant to the specifications of the O-RAN Alliance.[46] Despite some concurrent activity in Japan, the second "plugfest" that was held over the summer of 2020 also counted on a portion being held in Chinese OTIC labs.[47]

[46] https://www.prnewswire.com/in/news-releases/global-operators-collaborate-with-industry-partners-to-facilitate-o-ran-testing-and-integration-882975147.html

[47] https://www.o-ran.org/blog/2020/10/24/second-global-o-ran-alliance-plugfest-demonstrates-the-accelerated-readiness-of-multi-vendor-o-ran-compliant-network-infrastructure

DISCLAIMER

This document is intended for general informational purposes. RWR disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any acts or omissions made based on such information.

RWR does not provide legal, regulatory, audit, or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals. This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services. No person should rely on the contents of this publication without first obtaining advice from a qualified professional person.

Appendix 1: O-RAN Alliance Member Companies that Appear Domiciled in China

- AsiaInfo
- BOELINK
- CAICT
- Certusnet
- DIGITGATE
- Foxconn Industrial Internet
- GDCNi
- Shenzhen MTC
- GRENTECH
- H3C
- HGTech
- ICT
- III
- Innogence Technology 创智联恒
- Inspur Group
- IPLook
- ITRI
- JEZETEK
- Kindroid
- Lenovo— Hong Kong
- Mikwave
- NTS
- Phytium
- Purple Mountain Laboratories
- Raisecom
- RF MICAS
- RIMMATT
- Ruijie
- SAGERAN
- State Grid Info & Telecom Group
- SPIDERADIO
- Sunwave
- T&W
- Tianyi
- Tongyu Communication
- Tsinghua University
- Vavitel
- HRST China
- Zealync
- ZTE
- China Mobile
- China Telecom
- China Unicom
- ArrayComm