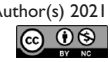
Article

European Journal of Communication
1–14


Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/02673231211028375
journals.sagepub.com/home/ejc


The geopolitical hijacking of open networking: the case of Open RAN

Jean-Christophe Plantin
London School of Economics and Political Science, UK

Abstract

This article investigates how discourses on open networking technologies provide a social imaginary that industry and government actors mobilize in an attempt to expand their control over mobile telecommunications networks. The case of recent initiatives aiming to 'open up' radio access network (or RAN, a key component of telecommunications infrastructure) with an 'open RAN' model reveals how the US Government came to promote this nascent technology to create an opposition between its own 'open' telecommunications networks versus proprietary and presumed 'untrustworthy' networks based on foreign equipment, namely Huawei. While a closer look casts doubts on the benefits of open radio access network to increase network security or to open up the equipment market, this case reveals how openness is an ambiguous notion that can be used by governments to exclude foreign trade enemies, while advocating for trust in telecommunications networks.

Keywords

Imaginary, infrastructure, openness, RAN, telecommunications networks

On 15 May 2019, then President Trump issued an executive order banning the use on the US territory of telecommunications equipment from foreign firms suspected of constituting a national security risk, predominantly targeting Huawei. The US government has in parallel been campaigning for its allies to similarly ban the company from their national networks, with success among the 'Five Eyes' countries (Australia, Canada, the United Kingdom, New Zealand and the United States), while various European Union (EU) countries are adopting similar measures. These restrictions have direct consequences for future telecommunications networks as they force telecommunications operators to choose different manufacturers to purchase the networking equipment necessary to roll

Corresponding author:
Jean-Christophe Plantin, London School of Economics and Political Science, London WC2A 2AE, UK.
Email: j.plantin1@lse.ac.uk

out their future infrastructure, especially fifth generation networks (5G). In addition, these measures have a dramatic impact on existing infrastructure, as they also require operators to remove targeted equipment from current technological configurations. As Huawei components are widely used in current networks, a ban on this manufacturer means that the concerned telecom operators have to conduct large 'rip and replace' campaigns of Huawei gear from their existing networks.

This obligation to replace Huawei components from existing networks has brought the question of alternative network equipment suppliers. In addition to considering the existing competitors to Huawei (such as the European equipment suppliers Nokia or Ericsson), operators and regulators in countries banning suspected equipment have been investigating whether open solutions could constitute a viable replacement of proprietary technologies, focusing on the Radio Access Network (or RAN). Several initiatives promote an 'open RAN' model (whose specifics will be explained in the next section) which would replace a closed architecture linking proprietary networking hardware and management software by an architecture based on open and modular interfaces, giving operators deeper control over which technologies they use and assemble. In 2020, the US Government endorsed this model and put it at the centre of its strategy to exclude Huawei from its network.

Instead of focusing on the networking or market performances of open RAN, this article analyses its openness as a discursive device mobilized by telecommunication industry or governmental actors to increase their economic and political power over networks. For the telecommunications industry, open RAN is tasked with bringing a competitive market with open standards unhindered by the bundled and proprietary technologies sold by a narrow set of leading manufacturers. For the US government, open RAN is an architectural model supposed to guarantee trust in network management and to replace untrustworthy foreign manufacturers in favor of US-based companies. Analysing open RAN as such engages with three critical perspectives on telecommunications networks and technologies. First, networks and their components – such as the RAN – are sites of political–economic struggle between various opposed stakeholders who want to increase their power, from transatlantic telegraph cables to contemporary Internet (Hills, 2002; Mattelart, 2000; Winseck and Pike, 2007). Within these macroscales of power, Mansell proposes the concept of socio-technical imaginary to emphasize that communication technologies are a site of competition for divergent sets of programmes and narratives (Mansell, 2012). Open RAN proponents similarly position this technology as instantiating an imaginary of 'openness' that they equate with 'trust' or even 'democracy' and position against 'untrustworthy' and 'black-boxed' proprietary and foreign technologies. Finally, communication networks are constituted of series of standards, for example, those constituting the RAN, whose design and selection reveal how actors with competing interests include and exclude other actors from shaping the future of networks (Abbate, 2000; Edwards, 1996; Yates and Murphy, 2019). Combining these three levels of analysis (networks, imaginaries and standards) reveals how industry and government actors can elect one specific architecture (open RAN) to convey a particular social imaginary of freedom, to eventually promote their economic and political control over communication networks.

Open RAN eventually shows how questions of trust in network governance evolve as networking infrastructure increases its reliance on software and modular architecture. First, as networks become increasingly 'virtualized' – that is, with key functions managed through cloud-based software and not mainly through hardware – questions of trust in the network similarly move from hardware to software. Tellingly, open RAN brings the focus on 'openness' – more prevalent in the software world (Coleman, 2012; Kelty, 2008) – to the world of telecommunication hardware. However, the polysemic nature of 'openness' allows industry or government actors to mobilize this notion to promote their specific agenda. Second, networks increasingly adopt platform-based processes, making their architecture programmable through modules that are all compatible through shared application programming interfaces (APIs). This instance of platformization of infrastructure (Plantin et al., 2018) reformulates questions of trust in network governance; while in the past, the tight market control of a few legacy manufacturers was a guarantee of trust, this model is increasingly associated with a lack of transparency, slow innovation and unfair market advantage. With the modular architecture of open RAN, trust is less attached to a specific actor and market advantage, but involves questions, such as: which actor takes part in a modular architecture, who has access to which APIs, or which actor acts as a gatekeeper to control access to interfaces? All these questions are already routinely asked to digital platforms in society (Gillespie, 2010; Helmond, 2015; van Dijck et al., 2018). Increasingly, as the case below illustrates, they will have to be applied to networking infrastructures.

RAN and open RAN

RAN is the segment of a telecommunication network that is located between the core network and users' equipment (such as a mobile phone). In its typical form, for example, adopted for LTE or 4G networks, a RAN is constituted of a Radio Unit, which is the antenna visible on top of a cell tower, and a Baseband Unit, a set of devices linking the radio equipment to the core network. To put it simply, RAN is the series of components linking users' cell phones to the network.

While radio equipment is crucial to the deployment of telecommunications networks and users' access to connectivity, it brings many challenges to mobile telecom operators, which motivates the search for alternative models. First, their cost is high; it is estimated that RAN can cost as much as 70% of an operator's capital expenditure (Fildes, 2020). Second, the market for RAN equipment is currently divided between three companies (Huawei, Nokia and Ericsson) who have a combined revenue market share of approximately 80% (Brown, 2020). This oligopoly is criticized for keeping the prices of equipment high and the pace of innovation for RAN equipment slow, as these suppliers have small incentives to develop ground-breaking technologies that would disrupt their own market power. Finally, suppliers usually sell RAN as a bundled technology where hardware and software are closely aggregated and not interchangeable. For example, radio units, processing units, as well as the management software are sold as a bundle and operate together. While this increases reliability, this model is criticized by operators wanting to mix and match components from various manufacturers, hence selecting more recent or possibly cheaper components, and updating specific components one at

the time instead of as a whole. In addition to all these constraints, the dramatic multiplication of antennas needed for 5G deployment has also incentivized operators to look for cheaper ways to manufacture and deploy RAN at scale.

Open RAN 'opens up' the traditional proprietary RAN by relying on generic hardware and open interfaces, allowing operators to choose their own combination of hardware and software. It aims to replace the traditional RAN model, which tightly bundles hardware and software in a monolithic architecture, by providing operators with an architecture based on two key principles: first, using open interfaces between the components of the RAN (Radio Units and Baseband Units) allow operators to choose the hardware and software to operate their radio, instead of being forced to use those already integrated; second, using open interfaces, and if possible generic non-proprietary hardware, allows operators to choose, adapt, modify the technologies they want to use, as opposed to restrictive proprietary equipment.

The open RAN model was created in 2016 in a working group from the industry consortium Telecom Infra Project (TIP), which brings together telecommunication operators and manufacturers (among others) to promote, as per the official website, 'open, disaggregated, and standards-based technology solutions' in the field of telecommunications. TIP fosters an ecosystem of link-minded industry actors, compatibility between technologies, as well as live trials and deployments of open RAN technologies. Two standard bodies are involved in providing the specifications for the open interfaces at the centre of the open RAN model: 3GPP and the O-RAN Alliance. 3GPP has a much wider focus, but in the case of open RAN, it provides a 'split radio' model for 5G (3GPP Release-15) which disaggregates the various components of the RAN. O-RAN Alliance, created in 2018 specifically to promote open RAN, complements the 3GPP by defining 11 open interfaces allowing modularity between disaggregated components, for example between the RAN and the management system, or between the distributed unit and the central unit.

While proponents of open RAN emphasize the disruptive, even revolutionary nature of openness applied to network equipment, the next section shows that such model mostly aims to apply the principle of modularity, which is already used in various segments of the information technology (IT) supply chain (Baldwin and Clark, 2000; Gawer and Cusumano, 2002). Similarly, modular interfaces have already been widely discussed in the telecommunication industries with the rise of intelligent networks in the 1990s (Mansell, 1993), and their application is debated once again with the arrival of 5G. Replacing open RAN in this recent history of IT and telecommunications networks shows that operators use open modularity as an attempt to increase their control over the configuration of networking equipment they use to build their infrastructure.

A new battle for the control of open interfaces

The open RAN model in effect disaggregates the different parts of the radio access network and make them modular through open interfaces. With such a model, an operator can buy, for example, antenna equipment from one manufacturer and networking equipment from another, and components are still compatible as they share common open interfaces. Borrowing a concept from management scholars, open RAN brings a modular

architecture to radio equipment, in which 'modules are units in a larger system that are structurally independent of one another, but work together' (Baldwin and Clark, 2000: 63). Modularity is already amply used across the IT supply chain, with Intel, Microsoft or Cisco presented as successful early adopters of such 'platform strategy' (Gawer and Cusumano, 2002). A modular architecture facilitates the integration of different components and purportedly leads to higher specialization and faster innovation. A similar goal leads current experiments with radio equipment through open RAN.

Beyond considerations of innovation, Russell links the concept of modularity to questions of control and power, and invites us to 'critically examine modular discourse for insights on how system architects used modular concepts to order, coordinate, and control' (Russell, 2012: 260). This perspective emphasizes that open RAN industry contenders present open RAN as an emancipatory technology that would allow them to break free from the limitations of the bundled approach of network hardware manufacturers. Open RAN advocates claim that the open RAN model will, for example, 'open the network stack and enhance vendor competition' (Wang et al., 2019: 5); similarly, 'Open interfaces allows a new freedom – the use of one supplier's radios with another's processors' (Mavenir, n.d.). This open model – and the freedom it is supposed to afford – is presented in opposition to the existing model of procurement, where customers are 'held hostage to big company development timelines [. . .]' as it favours 'integrated products under their exclusive control' eventually leaving network operators unable 'to gain control over RAN equipment due to proprietary interfaces and licensing restrictions' (Brown, 2020: 3). For open RAN advocates, modularity and openness are emancipatory notions that will lead operators to regain control of their own infrastructure.

Replacing these debates in the recent history of telecommunication reveals that network operators have not waited for the arrival of 5G networks to try to break free from manufacturers. Calls for modularity were already voiced in the telecom sector in the 1990s and with the rise of 'intelligent networks', when databases and software were increasingly used to expand and manage telecommunications networks (Mansell, 1993). Such change of architecture brought the question of open interfaces, which would allow 'access by competing service suppliers to the unbundled intelligent functionality within the public telecommunication network' (Mansell, 1993: 37). Looking at current debates on RAN in this historical perspective reveals that modular architecture and open standards are consistently presented as the solution against an oligopolistic market and tight control on procurement through proprietary technologies.

Network operators leverage the open RAN model – revolving around modularity and openness – in a bid to bypass existing component manufacturers and to gain deeper control over which components they choose to assemble in their RAN. Before critically examining the reality of such claims in the last two sections, the next part reveals how the principle of openness was also employed by the Trump administration, albeit for a different goal: to break free from the Chinese equipment manufacturer Huawei.

The geopolitical hijacking of open RAN

In 2020, open RAN unexpectedly left the highly specific industry debates around radio equipment to enter the geopolitical arena. In addition to banning Huawei equipment from

current and future networks, the Trump administration concurrently brought open RAN to the centre of its strategy for secure networks. While in the networking industry, 'openness' is used by its proponents to call for increased competition and innovation through open interfaces, the Trump administration used the same term to *oppose* the trust and transparency of 'open' equipment from allied countries to black-boxed and untrustworthy foreign gear. Some commentators have summarized such politicization of the technology as the 'hijacking of open RAN' by the previous US Government, with the objectives not being 'about cost savings, competition or even openness', but 'about shutting out the Chinese' (Morris, 2020b).

The interest of the US government in open RAN rapidly increased in 2020 through key milestones. On 24 April 2020, the US Senate passed the bipartisan legislation *Utilizing Strategic Allied* (*USA*) *Telecommunications Act*, which requires the FCC to create a US$750 million grant scheme to create a research and development fund dedicated to open RAN (Warner, 2020). In effect, it means that the US Federal Communications Commission (FCC) now directly subsidizes the development and future deployment of open RAN in actual networks. In addition to this grant scheme, the Act would create a 'transition plan' to facilitate the purchase of open RAN-compatible equipment especially by small and rural carriers.

Second, the FCC held on 14 September 2020, a day-long event entitled 'Forum on 5G Open Radio Access Networks' which brought together telecom operators (AT&T, Jio), equipment manufacturers (IBM, Nokia), members of the open RAN community (Open RAN Policy Coalition) and various legislators to assess the needs of the telecom community and the capacity of open RAN to fulfil them. In his introductory address, then FCC Chairman, Ajit Pai (2020), lauded open RAN as providing 'an exponential growth in the number and diversity of suppliers [and] more cost-effective solutions'. The geopolitical dimension of the technology was not forgotten, as Pai also enthusiastically claimed that open RAN puts 'the keys to security in the hands of network operators, as opposed to a Chinese vendor', but also that key open RAN companies – such as the solution providers Altiostar, Mavenir or Parallel Wireless – are US-based companies.

Finally, the open RAN community saw the creation of a new policy body in 2020, the *Open RAN Policy Coalition*, which is independent from the FCC and US government but whose goals align directly with them. While the open RAN community was so far structured around dedicated standardization bodies (O-RAN Alliance) or industry consortia to accelerate real-world deployment (Telecom Infra Project), the Open RAN Policy Coalition constitutes the clearest form of political lobbying for open RAN. The fact that its membership is constituted exclusively of US members or allied countries (such as Japan, South Korea or the United Kingdom) and without Chinese telecom or manufacturers led commentators to present this consortium as mostly promoting a US-based version of open RAN independent from China. It was similarly reported that this organization has lobbied the UK government to exclude Huawei from its national infrastructure (Fildes, 2020).

This promotion of open RAN technologies by the FCC and policy bodies directly meets the goal of the 'Clean Network', a bipartisan programme spearheaded by then Secretary of State Michael Pompeo (who gave an opening talk during the FCC forum on open RAN). It explicitly aims to protect the United States and allied countries from

'aggressive intrusions by malign actors, such as the Chinese Communist Party (CCP)' (Pompeo, 2020). The programme has produced a series of recommendations, such as the 'Prague proposals' (Government of the Czech Republic, 2019) and a checklist to determine trustworthiness and security in network, the 'Criteria for Security and Trust in Telecommunications Networks and Services' (CSIS, 2020).

These guidelines reveal how the discourse of open RAN – promoting openness, transparency and modularity – is extracted from the industry context and used in the geopolitical arena to support the political campaign of the United States against China. The 'Prague proposals', written by experts from EU and North Atlantic Treaty Organization (NATO) states at the Prague 5G Security Conference on May 2019, presents the following principles for the roll out of 5G: using 'international, open, consensus-based standards' (Government of the Czech Republic, 2019: 3), advocating for 'transparency and equitability, taking into account the global economy and interoperable rules' (Government of the Czech Republic, 2019: 3), and relying on a 'diverse and vibrant communications equipment market and supply chain [which] are essential for security and economic resilience' (Government of the Czech Republic, 2019: 4). Such desire to provide a community-based standard that promotes transparent procurement and open interfaces between actors directly echoes the key characteristics of open RAN, and are presented here as the desirable model for technology development.

Conversely, the transparency of open networking equipment is presented as opposed to the opaqueness of other providers' practices, with Chinese manufacturers in mind. The checklist 'Criteria for Security and Trust in Telecommunications Networks and Services' published in May 2020 by the Center for Strategic and International Studies (CSIS) as part of the 'Clean Network' initiative defines 'Opaqueness [as] indicated by unusual ownership arrangements that disguise who owns, controls, or influences the supplier company or use any other mechanisms to conceal dependencies between the supplier and a foreign state' (CSIS, 2020: 16). As opposed to 'transparent' networks, 'opaque' technology would allow access by the Chinese government to the 5G infrastructure once installed in foreign countries. Opaqueness similarly concerns the financial structure of network equipment providers, encompassing,

> opaque financial support or incentives, subsidies, or other financing mechanisms that are not commercially reasonable; lack of transparency; are part of a larger effort involving predatory pricing intended to eliminate competition; force other suppliers from the market; or are part of other government actions intended to disadvantage competitors unfairly. (CSIS, 2020: 17)

As often repeated during the FCC forum on open RAN, Huawei components are considered by its opponents as subsidized by the Chinese Communist Party, thereby presumably skewing the competition and allowing the company to expand its market presence through low prices (especially in countries with high infrastructure costs, such as Africa, c.f. Tang, 2020: 4563). This directly contrasts with claims made about open RAN, which is presented by its proponents as creating a transparent market where all players would be equal and able to compete.

As shown in the last two sections, the term 'openness' possesses the strategic polysemy that allows different actors to use it to push for different agenda. This term is part

of a social imaginary that can travel across national sociopolitical contexts and communities of practice (Mager and Katzenbach, 2021; Mansell, 2012) to serve specific interests. In the networking industry, it is used to promote competition and innovation through open interfaces and modular architecture. In the geopolitical context, it is endorsed by the US administration to carry values of freedom, transparency and democracy. In the next section, we extract open RAN from partisan debates and assess the reality of its assets, and look next at the position of the EU on open RAN and network governance.

The benefits of open RAN in question

The ambiguity around the use of the term 'openness' to promote open RAN is twofold: on one hand, open RAN is tasked with *opening up the equipment market to competitive entry*. Relying on open and modular interfaces is supposed to give room for new suppliers, hereby decreasing the influence of the three leading companies. On the other hand, open RAN is presented as *opening up the proprietary RAN technologies* by allowing operators to mix and max the hardware and software they purchase from different vendors. However, despite this ambitious programme, many critiques have voiced their concerns regarding the capacity of open RAN to fulfil these two goals.

Regarding the ability of open RAN to open up the vendors' market, two elements of caution are important. First, leading vendors, primarily Nokia and Ericsson, are currently increasing their participation in open RAN, either through participation to consortia (both are members of the O-RAN Alliance, Nokia of TIP as well), or through direct development (Nokia announced on 7 July 2020, the release of O-RAN-defined interfaces expected in 2021, c.f. Nokia 2020). This involvement in such a nascent model can be interpreted as a cautious investment in the future, should the open RAN model take off, but similarly calls into question the capacity of this new model to radically open up competition in the vendor market if the leading manufacturers that it is supposed to displace are already involved in the technology design.

Second, open RAN can provide an opportunity for tech giants – such as Facebook, Google, Amazon or Microsoft – to increase their control over network infrastructure through their cloud capacities, something that telecommunications operators are wary of letting happen (Lee-Makiyama and Hosuk, 2020). By disaggregating hardware from software, open RAN allows the 'virtualization' of network functions, as they can be performed through the cloud rather than hardware on premise. While this model allows for a more efficient network management, it also offers an opportunity for the tech giants – currently leading the cloud market with Microsoft Azure, Google Cloud or Amazon Web Service – to become an important infrastructural component of the networking infrastructure (Plantin et al., 2018; van Dijck et al., 2018). Moreover, by making access technologies more easily available to industry newcomers, open RAN similarly meet existing initiatives from tech companies to increase global connectivity (e.g. *Facebook Connectivity*, which hosts the widely discussed *Free Basics* initiative). The presence of tech giants in several open RAN consortia (Facebook is a founding member of the Telecom Infra Project, and Facebook, Google and Microsoft are part of Open RAN Policy Coalition) also reveals their interest in this trend. Interestingly, the endorsement of open RAN by tech giants goes against their common strategy to expand their market

power by promoting intraoperable systems – that is, the vertically integrated proprietary platforms that Google, for example, promotes in primary education (Kerssens and van Dijck, 2021). Here, tech giants favour the interoperability that open RAN brings between components, against the intraoperability promoted by legacy suppliers. Open RAN therefore brings the risk for network operators of swapping one dependence for another one: either towards legacy vendors in the proprietary RAN model, or towards large tech companies in the open RAN model.

A different set of critiques has targeted the capacity of open RAN to open up the proprietary RAN technologies. First of all, open RAN is not in itself an open source technology, rather it provides a series of open interfaces that allows the connection of various components (e.g. antenna and processing unit). However, while the interfaces are open and negotiated through standardization bodies, the components linked together to constitute the RAN can remain proprietary. Moreover, open interfaces have raised security concerns. A recent report from Ericsson emphasizes that the multiplication of open interfaces with open RAN dramatically expands the 'threat surface' for potential cyberattacks (Boswell and Poretsky, 2020). The report generated some pushback from open RAN advocates, who contended that Ericsson has a vested interest in undermining this competing model, and that openness of the technology is the best guarantee to continuously monitor network security (Nolle, 2020).

Most importantly, the US strategy of promoting open RAN to reduce the role of Chinese manufacturers in the building of the 5G infrastructure is a fallacy. Beyond Huawei, other Chinese companies have already been massively involved in the design of open RAN specifications. With 44 companies from Mainland China (and three from Hong Kong), China has the second-largest number of members in the O-RAN alliance (after the United States, with 82 members, and before Taiwan, with 20 members). Similarly, the standard body 3GPP has 131 Chinese companies (and two from Hong Kong) and over 688 individual members, as of early 2021. As some commentators put it, if the goal of the Chinese state is to influence the future of telecom technologies, then it is already doing this through open RAN, without needing Huawei (Strand, 2020). The effort of the United States to exclude Chinese companies from open RAN (most notably by setting a dedicated policy body excluding Chinese companies – the Open RAN Policy Coalition, mentioned earlier) does not reflect the already important part that Chinese manufacturers play in shaping open RAN. It also runs the risk of artificially multiplying efforts between a purported 'China-free' open RAN, and an open RAN including Chinese companies, both following the same architectural principles.

Finally, additional commentators mention that despite such a momentum in industry or government settings, the open RAN model is still in its early roll out and is not mature yet. While the key actors of open RAN, either consortia such as the Telecom Infra Project or companies like Rakuten, generate significant media coverage retrospectively for early deployment in Turkey and in Japan, others contend that it will take some time before the real costs and benefits of deployment are visible (Fildes, 2020). The economic gains of replacing a proprietary model by an open model are uncertain, as the costs of integration for open and disaggregated solutions would for some offset the gains resulting from skipping the expensive traditional equipment providers (Townsend, 2020). Moreover, even if the use of open RAN becomes more generalized across the industry, the market

penetration is presented as low, with a limited impact of 10% of the market by 2025 (Kapko, 2020). Finally, some commentators emphasize that open RAN is not in a position to compete with the main equipment manufacturers, such as Huawei, Nokia and Ericsson, which will most likely keep their market power in a near future (Fildes, 2020), especially if they strategically invest in open RAN initiatives.

Despite the ambitious benefits it is supposed to bring – opening up the market to newcomers, making technology more transparent and more trustworthy – many commentators express doubts over open RAN. The model is therefore currently characterized by a paradox between, on one hand, the important limitations highlighted earlier, and on the other hand, the strong support from the Trump administration in an attempt to quickly find an alternative to Huawei as 5G equipment supplier. While the Biden administration has not yet taken a specific position on open RAN, the *USA Telecommunications Act* passed in 2020 was as a bipartisan legislation, hence supported by the Democrats. The new FCC chairwoman, Jessica Rosenworcel, is also presented as a supporter of open RAN (Baldock, 2021).

The EU position on 5G and open RAN

In this context, Europe is more cautious in its position towards open RAN. On one hand, several EU countries are increasingly taking measures against Huawei, leading commentators to state that 'Europe is showing Huawei the exit' (Morris, 2020a). At the time of writing, the United Kingdom, France, Germany, Italy and Poland have implemented various restrictions towards Huawei, ranging from a complete ban to a new approval process to the non-renewal of licences. On the other hand, the EU emphasizes the question of security for 5G networks by promoting a concerted approach within EU members, at the opposite of the US unilateral measures to ban or promote one specific technology. This is evidenced by a series of recommendations concerning 5G. First, the European Union Agency for Cybersecurity (ENISA) published in November 2019 a 'toolbox' providing a detailed assessment of the 58 major threats of the 5G infrastructure (Lourenço and Marinos, 2019) – which does not focus on Huawei specifically, but try to assess the general threat landscape for future 5G networks. It was followed in July 2020 by a report from the same agency on the progress of EU member states' actions against the risks highlighted in the 2019 report (NIS Cooperation Group, 2020). These two documents signal RAN as a key point of failure of national networks and call for the diversification of suppliers in order to prevent over-reliance on high-risks suppliers (NIS Cooperation Group, 2020: 42). As opposed to similar US policy guidelines, however, these documents do not mention nor promote open RAN as a specific solution for safer networks.

In addition, the position of the EU differs from the United States as it is the home of the two other world leading equipment manufacturers (Ericsson and Nokia), while the United States does not similarly possess a national supplier. The readiness of these two European market leaders to jump in and replace Huawei gear creates less of an incentive for the European Union to quickly find alternative suppliers and models for procurement, especially since Nokia and Ericsson are contributing to the early design of open RAN. Moreover, the EU industrial policy favours open competition between various standards

without direct intervention through state subsidies and national mandates (which, ironically enough, is the strategy adopted by both China with Huawei and the US with open RAN). It is therefore unlikely that the EU will directly intervene to promote open RAN over other radio access solutions.[1] For all these reasons, commentators claim that 'Open RAN will have a limited impact on EU deployment of 5G' (Lee-Makiyama and Hosuk, 2020: 16).

Conclusion

Considering open RAN less for its technological and economic value and more as conveying a social imaginary revolving around openness and transparency shows how different actors mobilize this architecture and its associated standards – albeit recent and barely tested – in their attempts to gain control over mobile telecommunications networks. For network operators, openness is purported to bring the modularity and flexibility necessary to unleash innovation and to break free from the proprietary control of leading suppliers; for the past US Administration, openness was touted as guarantee of trust and transparency in its attempts to swiftly replace Huawei by alternative suppliers of networking equipment.

Critiques of open RAN show, however, that neither assumption is supported by evidence: the history of telecommunications networks reveals a pattern of recurrent calls for modular and open interfaces in the telecom spaces, none of which managed to overthrow the monopoly of manufacturers. Similarly, open RAN is not 'open' for everyone, as legacy companies are already investing in the technology and tech giants are also strong supporters. Finally, the security gains of open RAN are still contested, and so are the financial gains. Open RAN is therefore less relevant for its purported goals of increasing innovation and security, but rather for revealing how the same principle of openness can be mobilized by various actors in their attempts to gain control over mobile telecommunications networks.

New models need to be designed to adapt traditional institutional governance to how platforms shape public discourse – a debate to which this special issue contributes in multiple ways. In this context, this article acts as a cautionary tale. An imaginary of openness and trustworthiness can easily be weaponized by industry and government actors to push for their specific agendas. As shown, the discourse about open standards, modularity and interoperability circulates from industry to government and becomes included into geopolitical debates. In a context of increasing virtualization and platformization of communication networks, further migration of the concept of trust – and its related ambiguity in terms of governance – is to be expected as software and the open source model are increasingly integrated into the architecture of communications networks.

Acknowledgements

The author would like to thank José Van Dijck and the editors of the European Journal of Communication for their invitation to contribute to this special issue and for the quality of their feedback. His gratitude also goes to Robin Mansell, Meghanne Barker and the other contributors to the special issue for their useful comments on earlier versions of the article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

Note

1. Financial support can still come from individual EU member states. The German government included €2 million funding for open RAN research and development as part its post-COVID stimulus package of €130 billion announced in June 2020 (le Maistre, 2021).

References

Abbate J (2000) *Inventing the Internet*, 58839th edn. Cambridge, MA: MIT Press.

Baldock H (2021) Biden selects Jessica Rosenworcel to replace Ajit Pai as FCC chair. Total telecom. Available at: https://www.totaltele.com/508405/Biden-selects-Jessica-Rosenworcel-to-replace-Ajit-Pai-as-FCC-chair (accessed 25 June 2021).

Baldwin CY and Clark KB (2000) *Design Rules: The Power of Modularity*, vol. 1. Cambridge, MA MIT Press.

Boswell J and Poretsky S (2020) *Security Considerations of Open RAN*. Stockholm: Ericsson.

Brown G (2020) TIP OpenRAN: Toward disaggregated mobile networking. A heavy reading white paper produced for the telecom infra project. *Heavy Reading*. Available at: https://telecominfraproject.com/event/light-reading-tip-openran-towards-disaggregated-mobile-networking/.

Coleman EG (2012) *Coding Freedom: The Ethics and Aesthetics of Hacking*, Illustrated edn. Princeton, NJ: Princeton University Press.

CSIS (2020) Criteria for security and trust in telecommunications networks and services. *CSIS Working Group on Trust and Security in 5G Networks*, 13 May. Available at: https://www.csis.org/analysis/criteria-security-and-trust-telecommunications-networks-and-services.

Edwards PN (1996) *The Closed World: Computers and the Politics of Discourse in Cold War America*. Cambridge, MA: MIT Press.

Fildes N (2020) Telecoms networks look to fix Huawei problem with open source software. *Financial Times*, July. Available at: https://www.ft.com/content/6d77f69a-cd52-4f1d-b8c8-86b5df2ca689.

Gawer A and Cusumano MA (2002) *Platform Leadership: How Intel, Microsoft, and Cisco Drive Industry Innovation*, Illustrated ed. Boston, MA: Harvard Business School Press.

Gillespie T (2010) The politics of 'platforms'. *New Media & Society* 12(3): 347–364.

Government of the Czech Republic (2019) Prague 5G security conference announced series of recommendations: The Prague proposals. Available at: https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/.

Helmond A (2015) The platformization of the web: Making web data platform ready. *Social Media + Society* 1: 603080.

Hills J (2002) *The Struggle for Control of Global Communication: The Formative Century*. Urbana, IL: University of Illinois Press.

Kapko M (2020) Open RAN set to capture 10% of market by 2025. *SDxCentral*, 2 September. Available at: https://www.sdxcentral.com/articles/news/open-ran-set-to-capture-10-of-market-by-2025/2020/09/.

Kelty CM (2008) *Two Bits: The Cultural Significance of Free Software*, Illustrated edn. Durham, NC: Duke University Press.

Kerssens N and Dijck J van (2021) The platformization of primary education in The Netherlands. *Learning, Media and Technology* 0(0): 1–14.

Lee-Makiyama H and Hosuk F (2020) *Open RAN: The technology, its politics and Europe's response*. ECIPE policy brief no. 8/2020. European Center for International Political Economy (ECIPE). Available at: https://ecipe.org/wp-content/uploads/2020/11/PR-PB-82020.pdf.

Lourenço M and Marinos L (2019) Threat landscape for 5G networks. *European Union Agency for Cybersecurity*. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks.

Mager A and Katzenbach C (2021) Future imaginaries in the making and governing of digital technology: Multiple, contested, commodified. *New Media & Society* 23(2): 223–236.

Mansell R (1993) *The New Telecommunications: A Political Economy of Network Evolution*. London; Thousand Oaks, CA: SAGE.

Mansell R (2012) *Imagining the Internet: Communication, Innovation, and Governance*, 1st edn. Oxford: Oxford University Press.

Mattelart A (2000) *Networking the World, 1794–2000*, 1st edn. Minneapolis, MN: University of Minnesota Press.

Mavenir (n.d.) Understanding OpenRAN. Mavenir.Com (blog). Available at: https://mavenir.com/portfolio/access-edge-solutions/radio-access/understanding-openran-5g/.

Morris I (2020a) Europe is showing Huawei the exit. *Light Reading*. 9 October. Available at: https://www.lightreading.com/5g/europe-is-showing-huawei-exit/d/d-id/763814.

Morris I (2020b) The political hijacking of Open RAN. *Light Reading*, 5 June. Available at: https://www.lightreading.com/5g/the-political-hijacking-of-open-ran/a/d-id/759454.

NIS Cooperation Group (2020) *Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity*. NIS Cooperation Group. Available at: https://www.enisa.europa.eu/news/enisa-news/member-states-report-on-eu-5g-toolbox-released-today.

Nolle T (2020) Is Ericsson right about Open RAN security? – Welcome to CIMI corporation's public blog. CIMI Corporation's Public Blog (blog), 15 September. Available at: https://blog.cimicorp.com/?p=4289.

Pai A (2020) Remarks of FCC Chairman Ajit Pai at the FCC forum on 5G open radio access networks. *Presented at the FCC, FCC Forum on 5G Open Radio Access Networks*, 14 September. Available at: https://docs.fcc.gov/public/attachments/DOC-366866A1.pdf.

Plantin J-C, Lagoze C, Edwards PN, et al. (2018) Infrastructure studies meet platform studies in the age of Google and Facebook. *New Media & Society* 20(1): 293–310.

Pompeo M (2020) Announcing the expansion of the clean network to safeguard America's assets. United States Department of State (blog). Available at: https://www.state.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets/ (accessed 5 November 2020).

Russell AL (2012) Modularity: An interdisciplinary history of an ordering concept. *Information & Culture* 47(3): 257–287.

Strand Consult (2020) 44 Chinese companies have joined the OpenRAN effort, a strategy to reduce Huawei's presence in 5G. Available at: https://strandconsult.dk/44-chinese-companies-have-joined-the-openran-effort-a-strategy-to-reduce-huaweis-presence-in-5g/ (accessed 25 June 2021).

Tang M (2020) Huawei versus the United States? The geopolitics of exterritorial Internet infrastructure. *International Journal of Communication* 14: 22.

Townsend W (2020) Deconstructing the real impact of Open RAN. *Forbes*, 15 July. Available at: https://www.forbes.com/sites/moorinsights/2020/07/15/deconstructing-the-real-impact-of-open-ran/.

van Dijck J, Poell T and de Waal M (2018) *The Platform Society*. New York: Oxford University Press.

Wang J, Roy H and Kelly C (2019) Open RAN: The next generation of radio access networks. *Accenture*. Available at: https://telecominfraproject.com/openran/

Warner M (2020) Utilizing Strategic Allied (USA) Telecommunications Act, OLL20034. Available at: https://www.warner.senate.gov/public/index.cfm/2020/1/national-security-senators-introduce-bipartisan-legislation-to-develop-5g-alternatives-to-huawei.

Winseck D and Pike R (2007) *Communication and Empire: Media, Markets, and Globalization, 1860-1930 – American Encounters/Global Interactions*. Durham, NC: Duke University Press. Available at: https://www.amazon.co.uk/Communication-Empire-Globalization-Encounters-Interactions/dp/0822339285/ref=sr_1_2?keywords=dwayne+winseck&qid=1578833976&s=books&sr=1-2.

Yates JA and Murphy CN (2019) *Engineering Rules: Global Standard Setting since 1880*. Baltimore, MD: Johns Hopkins University Press.