**Huawei to be removed from UK 5G networks by 2027**

**Intoduction**

In the current era of evolution there has been drastic advancement in the field of communication. The development of 5G network is one of the major milestones in the telecom field. The main aim of 5G networks is to connect everything virtually including the machines and devices. It tries to connect the new industries by reliability, availability, uniformity, massive capacity and empowers different user experiences (Pirinen P., 2014).

 5G is the latest global wireless standard in the mobile network generation. It is designed to perform various activities that can transform human lives and connect billions of devices together. It will be making a huge impact in the areas like Artificial Intelligence, Virtual reality and IOT. It is developed to provide more network capacity, increased availability, and improved efficiency. 5G networks will be providing bandwidth to the enormous number of devices that are going to get connected in near future and virtually connect everyone to everything including the machines and devices (Tim Fisher, 2022).

Huawei is seen as a security threat and has become a target in UK to exclude people from buying its 5G equipment’s. This pertains banning UK mobile providers from buying any new 5G equipment’s from Huawei as well as removing all its networks from the country by 2027.From the past many years Huawei has set up many networks adhering to the security arrangements. But in January 2020 the government under the leadership of Boris Johnson announced a ban on using 5G equipment from Huawei and has aimed at a complete removal from the country by 2027 (Kaska K., Beckvard H. and Minárik T., 2019).

In UK there are many cities where 5G is already launched but currently only few major providers namely EE, O2, Vodafone, BT have started with the 5G plans.[2] After USA announced sanctions against Huawei, UK started collecting technical advice from the team and concluded that none of the Huawei new kit be added from January 2021 and has put up deadline to be Huawei free by 2027. This announcement created opportunity to other two leading vendor namely Nokia and Ericsson. Huawei expressed its disappointment to UK’s decision and said that the decision will make the country digitally slow and will divide the country’s network development. The ban on Huawei was seen as political driven and not based on security concerns. Huawei had laid a firm foundation across UK over the past 20 years and had committed on providing the same service. It also said that they will be providing a detailed survey and explain the government as how they can help Britain in staying connected (Pant, 2020).

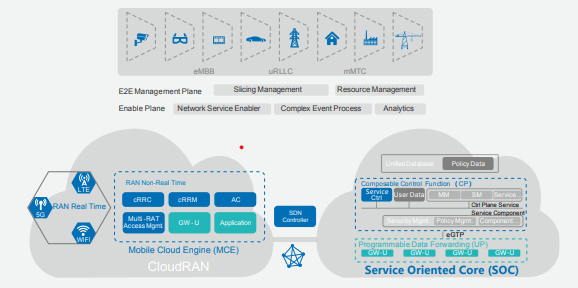
**Analysis**

5G services are organized in such a way that it not only provides faster and qualitative broadband services but also develops new service areas and connects the IOT devices. The sub-3 GHz spectrum resource used in 4G networks will be used beyond 100 GHz to ensure that it can be operated in both mmWave and lower bands. By enhancing the Orthogonal frequency-division multiplexing (OFDM) to greater levels of scalability and flexibility the OFDM can be enhanced further to provide greater access to 5G networks. It is designed with an extended capacity to empower new deployment models and provide new services. It is expected to expand the current ecosystem by providing high speed, higher reliability, and low latency to develop accurate, digitized, safe and remote mobile ecosystem

5G is designed to be the upcoming generation of wireless communication technology that will meet all the user requirements. Currently the infrastructure is set in such a way that there are different distributions made for mobile telephones, radio channels, TV channels and armed forces. 5G is developed to converge all these different distributions into one infrastructure. This is achieved through ‘network slicing’ using which all the different purpose networks are replaced by a software-based network slice. 5G is also developed for removing the limit on connected devices. This will help in connecting the devices together and prepare for the future technologies where the devices will be connected to Internet using the sensors. This will create a huge advancement in the field of IOT which will connect all the devices together and help us in monitoring them.

**Architecture**:

The 5G network architecture is designed in such a way that it is flexible and meets the varying service requirements. The physical infrastructure is supported by software-defined network (SDN) and Network Functions Virtualization (NFV). All the access and core networks are stored in the cloud and provides better support for different 5G services. Different technologies like component-based network function, E2E network slicing, and on-demand deployment of service anchors are enabled (Ansah F., Majumder M., de Meer H., Jasperneite J, 2019).



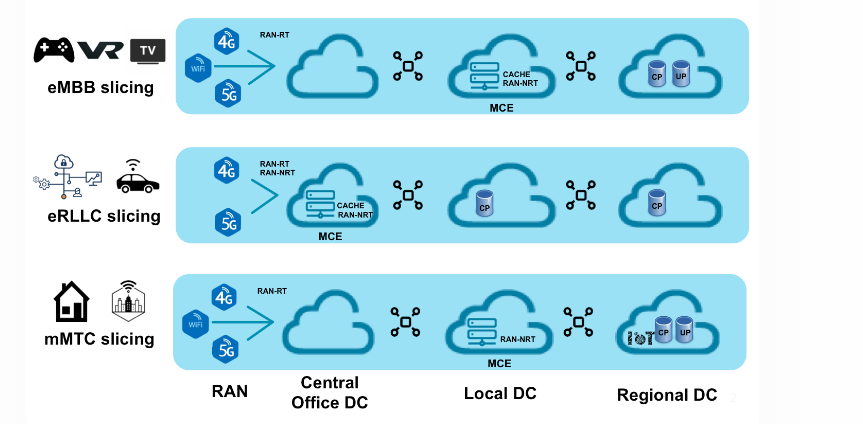
*Figure 1 Service-Driven 5G Architecture (Pliatsios D., Sarigiannidis P., Goudo S., Karagiannidis G., 2018).*

As shown in above figure, to coordinate between multiple services different site types of radio access network (RAN) and varying operating standards cloudRAN is built consisting of sites and mobile cloud engines. To meet the increasing demand for RAN non-real time resources multi-connectivity facility is implemented. Dynamic policy, static network and semi-static user are used to regulate the policy control of the network. Based on Component-based control planes and programmable user planes, the network function orchestration picks the corresponding control-plane as per the service requirements. The transport network comprises of SDN controllers and underlying forwarding nodes. SDN controllers brings out required data forwarding paths depending on the service requirements and network topology generates a series of data. Network optimization gets implemented in the form of API by the enabling plane and it analyzes the network capabilities. The top layer of the architecture uses network resource management and E2E automatic slicing (Pliatsios D., Sarigiannidis P., Goudo S., Karagiannidis G., 2018).

**Working**

In the existing model the Information and communications technology (ICT) network is implemented by using SDN and NFV and have retained a conventional architecture model. But in case of 5G networks they require continuous innovation as they require on demand network implementation and automatic O&M. This is achieved by adopting cloud models to customize the network requirements. The resource utilization is maximized by constructing physical networks based on Dcs to pool hardware resources. It is further simplified by using E2E network slicing which separates the virtualized network slices. CloudRAN is built over MCE and helps in addressing challenges or any uncertain events (Mark Stone, 2021).

In current generation the mobile networks are demanded to provide diversified services. Customizing the control functions for required service is not possible in current mobile networks and can provide only a single set of logical control functions for all the different purposes. To overcome this 5G networking model is intended to provide diversified services using mobile networks. The main technology used for achieving this is E2E network slicing. Each network will have multiple logically separated network slices and every slice will have its own network topology, resource allocation and network function. The slices can be automatically generated and terminated based on the requirements which reduces the overall operating expenses.



*Figure 2 Network Slicing Requirements (Selinis I., Katsaros K., Allayioti M., Vahid S., Tafazolli R., 2018).*

As shown in the above figure, 5G networks are designed into Enhanced Mobile Broadband (eMBB), Ultra-reliable and Low-latency Communications (uRLLC) and Massive Machine Type Communications (mMTC) demanding different requirements for network control functions. eMBB slicing requires high bandwidth for deploying cache in the mobile cloud and gives high speed services at low cost. It tries to improve the services like bandwidth needs, high quality videos and better AR and VR requirements. uRLLC slicing has strict requirements and focuses on improving the digital demands and provides services like assisted driving and remote management. mMTC focuses on satisfying the high requirements like smart agriculture and smart city (Selinis I., Katsaros K., Allayioti M., Vahid S., Tafazolli R., 2018).

Similar to previous versions 5G is also [OFDM](https://en.wikipedia.org/wiki/Orthogonal_frequency-division_multiplexing)-based (Orthogonal frequency-division multiplexing) and will be operating on similar mobile networking protocols. The enhancement of 5G NR (New Radio) will increase OFDM to provide higher levels of flexibility and scalability. Based on the service requirements the logical control functions can be managed to perform the independent functional tasks. Tightly coupled control functions are complex and result in difficulty in service deployment. So, to overcome this, 5G networks use control plane component which simplifies the deployment of new services and forms a strong foundation for 5G E2E network slicing.

**Challenges**

There have been many challenges in implementing the 5G model. We lack the digital infrastructure and do not have the required applications that needs to be connected to the network. But the true potential of 5G infrastructure will take some time to get realized. The 5G development will support as the base foundation to the upcoming advancements and will be the most critical infrastructures. This is one of the main reasons for considering the security aspects of 5G. Even though there were challenges with the 4G networks, but the risk associated with it was minimal. But this is not the case with 5G networks. 5G incites more security concerns as this will be the backbone for the upcoming automated systems and if there is any risk associated then it will have a huge impact over the system (Paul Sandle, 2020).

The securitization of 5G is not considered as a matter of great importance. But when the security experts started realizing the societal function which 5G could have in the coming future and how they could get exploited by the attackers, their arguments got stronger. Based on this concern, the political macro securitization of China might have been considered as malicious actor if they were given 5G access and security would also be compromised (Al-Falahy N., 2017).

**Discussion**

There were many warnings given from the past decade by the US experts that Chinese telecommunication networks in US could pose a security threat to the country and were suspicious over their foundation on US markets. The Chinese telecoms company Huawei became the first target over the securitization in 5G technology in the US. Huawei was having a strong network and had potential to get many contracts over 5G networks. But the administration under the leadership of Trump took a firm stance against the company stating security risks. They claimed that Huawei could pose a serious threat to the security of the nation as their 5G networks could get misused by Chinese intelligence and would be used for destruction by China (Ewan Sutherland, 2021).

The campaign against Huawei is not restricted only to telecom networks. There have been incidents in 2019 where the Chief financial officer of Huawei has been accused of breaking the law and misusing the trade secrets. The dispute against Huawei is just one part from the from the large US-China battle and is trying to limit China’s access to American technology factoring to geopolitics and economic rivalry. The securitization of Huawei is just more than the 5G networks and is a part of comprehensive and global securitization from China (Lamb, 2019).

There are many countries that are concerned over the security issues of 5G network. Poland conducted rigorous evaluation of suppliers based on their ethical behavior of the vendors and the ownership structure of the firm. They prohibited importing products from countries which do not have a formalized security cooperation agreement with them and reduced the amount of production of networks without security agreements. In 2019 Norway declared that a minimum of 50 percent of 5G network base stations should be from the countries which have security cooperation with them. This resulted in reducing the Huawei set up in the country as they could not satisfy the 50 percent rule. The European countries too had securitized 5G but avoided explicit securitization of Chinese companies and limited it to legal-political aspect (Couzigou I., 2018)

Some of the countries wanted to have securitized network but did not want to have adverse relation with China. Hence rather than implementing a complete ban over Chinese products they choose to implement some strict measures in which the Chinese firms would fail out. The administration under the power of Biden declared that US won’t force any of its allies to favor China or US. But on the bigger side the future relationship with the West and China will have bad effect on the global digital technology (Tao T., 2014)

UK also tried with the same approach as above countries. It limited the role of non-core elements of 5G networks from beginning of January 2020. Later it permitted only up to 35 percent of base station with exceptions to not have it near high-risk sites like nuclear station and military camps. But US opposed UK’s decision stating it a momentous decision and demanded a complete ban over Huawei network. Later UK government announced to not only ban Huawei from 5G network but also prohibit it from earlier generation networks too. The British security agencies argued on this, and it was stated that since Huawei was barred from using US technology in its system, it would reduce the security of Huawei equipment and will lead to security concerns.

**Conclusion**

The ban imposed by UK on 5G networks must be justified based on trade agreements and the security concerns must be explained. The allegations made against Huawei were related to security of network equipment’s, but the Government never stopped the people from purchasing its devices or ordered to switch to alternative devices. It can also be noted that Huawei is a Chinese manufacturing company and UK politicians must have found some threat as Huawei can easily monitor over the activities of the UK’s population. Also, assumptions are made that Chinese authorities can easily exploit the system and get direct access to the data resulting in denial of service or unauthorized access. There are also chances that there would have been some suspicious activities and UK government might know of vulnerabilities that would have been used to perform an attack over the Huawei systems. The ban on Huawei cannot be merely on economical or security decision but might also be a political decision for many countries as Chinese government is trying to weaponize trade and it might be of great concern ( David Sutton, 2020).

We can also observe how the US's macro securitization of China impacted the global telecom company. The 5G security cannot be resolved just at the technical level but also needs to be scrutinized on the political levels. The ban on the Huawei is just a method to screen out the potential risk but there needs to be a alternative solution that would secure the 5G architecture and reduce the associated risks. The British government is also aware that this decision will cost them on the global markets, delay the 5G set up across the country and will come with some serious strategic costs as well. But for UK the security, integrity, and confidentiality of data matters.

# References

David Sutton, 2020. UK 5G What’s Next?. *ITNOW,* 62(4), pp. 42-43.

Al-Falahy N., A. O., 2017. Technologies for 5G networks: Challenges and opportunities. *It Professional,* 19(1), pp. 12-20.

Ansah F., Majumder M., de Meer H., Jasperneite J, 2019. Network slicing: An industry perspective.. *24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA),* pp. 1367-1370.

Couzigou I., 2018. Securing cyber space: the obligation of States to prevent harmful international cyber operations. *International Review of Law, Computers & Technology,* 32(1), pp. 37-57.

Ewan Sutherland, 2021. 5G security – The politics of Huawei equipment in the United Kingdom. *LINK Centre, University of the Witwatersrand,* pp. 36-54.

Kaska K., Beckvard H. and Minárik T., 2019. Huawei, 5G and China as a security threat. *NATO Cooperative Cyber Defence Center for Excellence (CCDCOE),* Issue 28.

Lamb, H., 2019. Huawei 5G ban would be ‘big loss’ for UK.. *Engineering & Technology,* 14(9), pp. 12-13.

Mark Stone, 2021. *What is 5G security? Explaining the security benefits and vulnerabilities of 5G architecture.* [Online]   
Available at: https://cybersecurity.att.com/blogs/security-essentials/what-is-5g-security

Pant, H., 2020. Shutting the door on Huawei.

Paul Sandle, W. J., 2020. *UK bans Huawei from its 5G network.* [Online]   
Available at: https://www.reuters.com/article/us-britain-huawei-reaction-instantview-idUSKCN24F1JL

Pirinen P., 2014. A brief overview of 5G research activities. *1st International Conference on 5G for Ubiquitous Connectivity,* November.pp. 17-22.

Pliatsios D., Sarigiannidis P., Goudo S., Karagiannidis G., 2018. Realizing 5G vision through Cloud RAN: technologies, challenges, and trends. *EURASIP Journal on Wireless Communications and Networking,* Volume 1, pp. 1-15.

Selinis I., Katsaros K., Allayioti M., Vahid S., Tafazolli R., 2018. he race to 5G era LTE and Wi-Fi.. *IEEE Access,* Volume 6, pp. 56598-56636.

Tao T., C. W., 2014. The Huawei Story. *SAGE Publications India.*

Tim Fisher, 2022. *Where Is 5G Available in the UK.* [Online]   
Available at: https://www.lifewire.com/5g-uk-4178867