5G- and Huawei's-Mobile Wireless Network-Technology: Is the UK-Compromise of excluding Huawei from its Core-Network Sufficient?

By Frank Umbach

Dr. Frank Umbach, Research Director at the European Centre for Climate, Energy and Resource Security (EUCERS), King's College, London

This year will decide how fast and secure the newly introduced mobile wireless-network technology of 5G for Europe's industries and critical infrastructures will be deployed and to which extent Europe will become technologically dependent on Huawei and an ever more nationalistic and authoritarian China, which is officially been viewed by the EU as a "systemic rival". Alongside, it will also become clear to which extent the EU member states will accept increasing cybersecurity risks of industrial and political espionage as well as potential sabotage as the result of its wider economic dependencies on China. At the same time, these decisions of the EU member states will also show, to which extent the EU is able to agree on common strategies of its industry, technology and cyber security policy, such as determining and implementing common cyber security standards for 5G networks.

The British government has decided on January 28 that Huawei will be excluded from the core 5G network and restricted to its periphery. It also imposed a future market share cap for Huawei in UK's non-core 5G network from presently 44% to 35% in 2023. Without the British governmental intervention, Huawei would have acquired a future market share of the UK's 5G network up to 70% within the next three years. Within the EU, also other member states – such as Germany – need to decide about Huawei's technology inclusion by taking into account complex as well as difficult conflicts of objectives and interests. They all need to balance shorter- with longer-term strategic interests of its industry-, technology- and cybersecurity policies as the EU only recommends security guidelines and leaves the technological sovereignty of the 5G-network build-up und Huawei's involvement in the responsibility of the individual member states.

The British Security Council and UK's National Cyber Security Centre (NCSC) have stated that it can manage the remaining risks of deeply entrenched Huawei technologies and shrink them to "acceptable levels" in order to mitigate the key threats of industrial and political espionage, theft or alteration of data, blackmail and network sabotage. But the NCSC has also admitted that the risks of using Huawei's technologies in its 5G network can never be completely removed. Already previously, the NCSC has evaluated Huawei as Britain's only high-risk vendor to build its new ultra-fast high-speed mobile network. The assessment is not only based on China's National Intelligence Law of 2017, which allows the Chinese government to "compel anyone in China to do anything". The NCSC has also warned that China's state and associated actors "have carried out and will continue to carry out cyberattacks against the UK and our interests". It has also repeatedly criticized (as many independent international

cyber security experts for years) that "Huawei's cybersecurity and engineering quality is low and its processes opaque". In its 2019 report it confirmed that the Chinese company has also made "no material progress" in addressing "major defects" and significant security concerns already being raised the year before.

Huawei's 5G technology policies are a perfect example of China's long-term thinking by defining the future disruptive technologies and industry applications. As Huawei's technologies are very hardware-centric, they are deliberately not compatible with most of other vendor's technologies. That creates technology path-dependencies over several technology generations. It is another example of China's supply and value chain strategies which seek to control the worldwide research and development, the critical raw materials for the new technologies up to semi-finalized and end products in future key technology sectors.

Cyber Security Challenges beyond Huawei

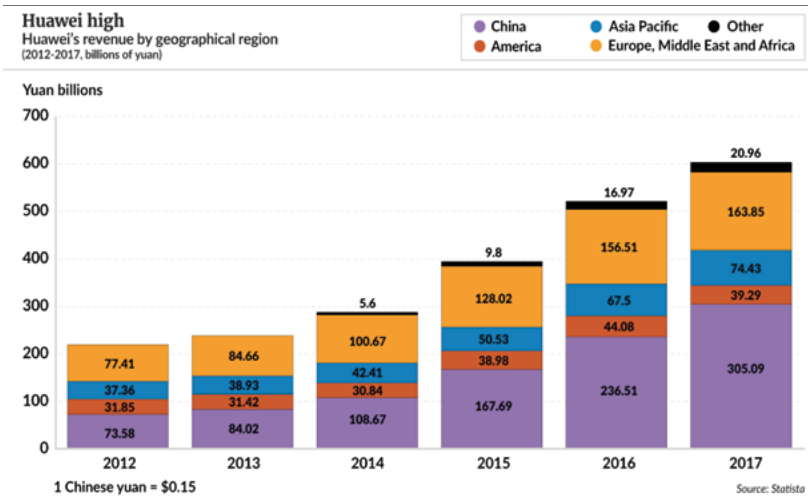
The build-up of national 5G mobile networks might result in a dramatic increase of cyber risks and vulnerabilities as it will connect the future networks of critical infrastructures and "industry 4.0" with millions of unsafe Internet-of-Things-appliances. With every additional connection, it becomes harder to figure out any vulnerabilities of the system. They will also increase as the traditionally defined "core" (where customer information is stored and processed) of the future 5G-network can't be clearly separated any longer from the periphery (Huawei's antennas and base stations) in contrast to the 3G and 4G networks. More computing power, clouds, servers and processes will move from the core to the periphery as the numerous appliances of the industry 4.0 demand much more decentralized 5G networks.

The future mobile networks will run on advanced software in an increasingly virtualised network that includes the traditional core and the system that manages all the hardware from smartphones to automated factories, driverless cars and telemedicine for rapidly processing data and communication with the network. The various hardware, software application, protocol and code layers include proprietary information, which makes it almost impossible to verify network messages over the hardware back to end consumers such as Huawei (and ultimately China's KP or its secret services).

The dynamic deployment of 5G networks will dramatically change the cybersecurity landscape by increasing the scale of surface attacks and restricting effective surveillance and control. Traditional monitoring methods will become ineffective and obsolete. The 5G network may become so complex that managing the risks of China's involvement could overwhelm all national resources. Therefore, cyber security experts have demanded to disclose the source and programme codes for the 5G networks. But it is contradicting traditional commercial businesses.

Restricting Huawei's technologies to the 5G's periphery alone – as suggested by UK's policies and the EU's recommendations – won't solve many fundamental cybersecurity challenges of the new virtualised networks and, therefore, is not sufficient. Moreover, UK, Germany and few other EU member states may be able to define and implement "acceptable levels" of remaining cybersecurity risks. But 10 other EU member states have neither any institutionalized cybersecurity expertise and capacity nor do they have comparable rigorous security-risk mitigation strategies and any entrenched cybersecurity risk culture to evaluate new cyber risks of new disruptive technologies such as 5G.

Figure 2
Huawei: Revenues by Region 2012 – 2017



www.GISreportsonline.com
Source: FT 2019