Written evidence submitted by John W Strand

Thank you for the opportunity to respond to this inquiry by the United Kingdom Parliament's Defence Committee on the Security of 5G.

I founded Strand Consult in 1994 with a focus is the global mobile telecom industry. Strand Consult has a team of engineering, strategy, economic, and legal/regulatory experts to help telecom industry actors understand international policy challenges. Together we analyze market trends, publish strategic reports, and conduct executive workshops to help telecom operators optimize their business strategies.

Hundreds of telecom operators have tapped Strand Consult's knowledge over the last 25 years. Additionally, I have served on the Advisory Board for the 3GSM World Congress (the event known as the Mobile World Congress in Barcelona) and on the Arctic Economic Council Telecommunications Working Group.

Strand Consult believes the UK policy regarding the use of Chinese-made equipment from Huawei in UK mobile networks is a step in the right direction, and it underscores the need for greater scrutiny of technology from firms owned and/or affiliated with the Chinese government.[1] The security risks are real, and networks are vulnerable. Indeed, scrutiny should extend beyond the network equipment to other vulnerable products and services; systems can be compromised by devices attached to networks as well as from the software running over it.

Overall, the UK policy will send a strong signal to the rest of Europe and the world that the use of Chinese equipment poses a security risk and should be limited. The UK and French decisions were developed to protect industries, institutions, and assets of national importance in specific geographical areas. Given this recognition, it begs the question why other parts of the UK are not worthy of the same security and protection. Indeed, every enterprise, organization and household in the UK deserves the same security of communications.

Some have claimed that a ban on Huawei equipment will increase industry costs in the tens of billions of euros. This can be empirically investigated by reviewing the financial statements of mobile operators which have ended their Huawei contracts and switched suppliers. For example, Denmark’s TDC and Norway’s Telenor and Telia ended their Huawei contract, but financial statements show that costs did not increase with a new vendor. Indeed, the operators maintained investment levels and network output by switching from Huawei to Ericsson. The same can be said for KPN in Netherlands. Nor has the UK seen an increase in CAPEX for British Telecom (BT/EE) and Vodafone UK following the UK government’s complete ban of ZTE and restrictions of Huawei in 67 percent of the networks. In fact, BT estimates the impact of the Huawei ban to be only £100 million per year for the next 5 years, which compared to its total investment is a small amount. BT changed its investment schedule

[1] https://www.gov.uk/government/news/new-plans-to-safeguard-countrys-telecoms-network-and-pave-way-for-fast-reliable-and-secure-connectivity

such that instead of postponing £500 million in the future, it will make those investments today.[2] Vodafone noted similarly that the Huawei restrictions do not hurt its financial performance.[3]

Strand Consult's report "The real cost to rip and replace of Chinese equipment in telecom networks" examines the costs of restricting Huawei equipment in European networks in detail. It reviews the assumptions and calculations behind the claims of reports claiming that Huawei restrictions will increase cost and slow rollout. Notably these reports have been funded by Huawei[4] [5]. What Huawei purports to be an impact of €55 billion[6] is at most €3,5 billion[7]. This number has also been validated by the European Commission. When compared to the number of European mobile subscribes, the cost to "rip and replace" Huawei equipment is €6 per mobile subscriber.[8]

The global RAN market today is $29 billion. China's RAN market is 25 percent of the world total, twice that of Europe. Europe's share has fallen from 2000 and is only 10-15 percent today. The European market includes Russia, the former Russian republics and Turkey, about $4.4 billion; the EU only component is $2.9 billion.

RAN investments in Europe make up 20-25 percent of the operators' mobile only, 15-20 percent for integrated CAPEX, including installation of the total CAPEX, which in turn represents 3-6% of the operators' turnover. Total mobile revenues in Europe reached €143 billion in 2017 and is expected to be €144 billion by the end of 2025, a compound annual growth rate (CAGR) of 0.1 percent.

Restrictions on Huawei and ZTE equipment for 5G have little to no impact on European operators because most of the EU's operators have yet to deploy 5G. However, if modeling the impact where to forcibly require the upgrade of all Huawei 4G equipment in the EU, it would only impact those operators which have already contracted with Huawei. About half of the EU's capital expenditure on RAN equipment is from Huawei and ZTE, totaling $1.8 billion. While Huawei and ZTE together have 40 percent market share in Europe, this translates to just 6 percent of the world market for RAN. As such, Huawei's importance in overstated. Moreover, it does not own the essential patents for 5G.

The telecom industry should be forthright to customers and shareholders about cybersecurity costs. Customers expect secure communication and are willing to pay for

---

[2]https://www.btplc.com/Sharesandperformance/Financialreportingandnews/Quarterlyresults/index

[3] In its February 2020 earnings call, Vodafone noted, "This time last year, we decided to pause any further developments of Huawei in the core. We have now decided to replace Huawei in the areas deemed sensitive, i.e., the core, across the EU within 5 years at a cost of approximately EUR200 million."

[4] https://www.oxfordeconomics.com/recent-releases/51856cd0-46d6-409c-bcab-218875f6b510

[5] https://zpravy.aktualne.cz/domaci/site-5g-se-bez-huawei-prodrazi-o-38-miliard-tvrdi-studie-cis/r~6e44780078bb11ea9d74ac1f6b220ee8/

[6] https://www.reuters.com/article/us-huawei-europe-gsma/europes-5g-to-cost-62-billion-more-if-chinese-vendors-banned-industry-idUSKCN1T80Y3

[7] http://www.strandconsult.dk/sw8402.asp

[8] http://www.strandreports.com/sw8402.asp

it. The companies that waited to act, ended up paying more. The discussion is greater than any one country or company, and indeed Chinese technological threats are more than just Huawei.[9] However, failing to secure networks from Huawei equipment would be like NATO buying a Chinese fighter planes. NATO prohibits procurement from communist countries; the question then is if fighter planes are critical infrastructure, why is the same standard not applied to telecommunications networks?

The pressure to restrict Huawei from telecom networks is driven by the many companies which have experienced hacking, IP theft, or espionage from China.

Strand Consult´s analysis shows that the concerns about Chinese made network equipment is not limited to national governments and the military intelligence operations. Nor is the concern confined to telecom operators which build and run networks. It is the small, medium, and large enterprises that use networks which fear that their valuable data will be surveilled, sabotaged, or stolen by actors associated with the Chinese government and military. Consequently, it is the clients of telecom operators which push to restrict Chinese-made equipment from networks.

Strand Consult finds in its consultation with telecom operators that their corporate customers demand greater security. Some of these corporate customers compete with Chinese firms for global markets, and telecom operators have experienced their trade secrets, designs, plans, ideas, movies, molecules, and other intellectual property have been stolen via telecom networks.

In 2017 China implemented a National Intelligence Law which compels any Chinese subject to conduct espionage on behalf of the government. While ordinary citizens can be compelled to spy, operationalizing passive surveillance within networks through backdoors and other means is more effective. Given the increasing integration of software in network equipment, these backdoors are increasingly difficult to detect, as they can be shipped in subsequent software upgrades or activated after security clearances are concluded. Moreover the law allows the Chinese government to confiscate data on any device made by a Chinese owned firm.

A 2017 report by the bipartisan US IP Commission concluded that Chinese theft of American intellectual property currently costs $225-$600 billion annually.[10] Continued theft at that rate will seriously diminish an economy which relies of innovation and intellectual property. IP theft has been a major issue for years, and while theft has been conducted by various rogue states, China is by far the leading perpetrator. While China has taken some steps to protect intellectual property in China, it still has a long way to meet the standards of the UK.

Huawei and ZTE are formally banned in federal networks in the US, and Huawei's complaint has been struck down in US district court. The Department of Justice (DOJ) has advanced racketeering charges against Huawei and its subsidiaries.[11] The

[9] http://www.strandconsult.dk/sw8396.asp
[10] http://ipcommission.org/report/IP_Commission_Report_Update_2017.pdf
[11] https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-subsidiaries-charged-racketeering

Federal Communication Commission has barred China Mobile from obtaining a license, and its looks like China Telecom's license will be revoked for deception and breach of contract.[12]

In China, the government controls everything except the hackers attacking British companies every day.

It is well known that the Chinese government surveilles its people 24/7 with millions of CCTV cameras[13]; the "Great Firewall of China[14]" blocks access to unapproved content and tracks attempts to circumvent it; and municipal party leaders keep tabs on citizens. All networks and equipment are operated by companies either owned or affiliated with the government. This surveillance data is aggregated into a unified system of social credits intended to standardize the assessment of the social and financial reputations of individuals and firms.[15] In practice, little to no information moves outside of the government's purview. People who don't live up to the Chinese government standards are sent to camps for "transformation-through-education" and are denied due process to defend their activities, according to Amnesty International.

It's curious then why more cyberattacks originate from China than any other nation. Indeed, if China was so concerned about law and order, they could end these attacks immediately, but they don't. In fact, China's 100,000 hackers are part of its military and attack foreign targets of all kinds at the behest of the Chinese government.

Chinese hackers attack British and other companies every day.

What advanced technology China has not been able to develop itself, it appropriates through other methods, whether forced technology transfer or theft. U.S. cybersecurity vendor Cybereason issued a report describing "an ongoing global attack against telecommunications providers that has been active since at least 2017." The report concludes the perpetrator is the APT10, an "advanced persistent threat," and a state-supported Chinese espionage group. [16]

In December 2018, the U.S. government has indicted APT10 members with conspiracy to commit computer intrusion, conspiracy to commit wire fraud, and aggravated identity theft.[17] The indictment noted the hackers worked in tandem to steal intellectual and technological information from dozens of commercial and defense technology companies throughout the continental United States. Additionally, APT 10 is also responsible for the theft of personnel information for 100,000 U.S. Navy personnel.

---

[12] https://www.justice.gov/opa/pr/executive-branch-agencies-recommend-fcc-revoke-and-terminate-china-telecom-s-authorizations
[13] https://www.youtube.com/watch?v=pNf4-d6fDoY
[14] https://en.wikipedia.org/wiki/Great_Firewall
[15] https://www.bbc.com/news/world-asia-china-34592186
[16] https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers
[17] https://www.fbi.gov/wanted/cyber/apt-10-group

Breaches like these are not new. China is responsible for the greatest number of cyberattacks by any nation over the past dozen years.[18] The true depth of China's efforts, and successes, in penetrating western networks is probably still unknown.

In 2018 in Norway, Visma, a supplier of cloud-based financial systems discovered that Chinese hackers tried to steal client data, a treasure trove of information for state-sponsored Chinese companies which want to sell to clients whose data was exposed.[19] Germany's Bayer also withstood a Chinese hacker attack in 2018.[20]

Australian intelligence officials believe China may have accessed thousands of files and 19 years' worth of data – to include tax and banking records – on Australian National University' students and staff. [21] Many of ANU's graduates serve in the country's intelligence and security agencies. Symantec unveiled in June how Chinese hackers have attacked satellite and telecommunications infrastructure outside of China.[22]

Telecommunications network equipment is one means to conducting hacking, but devices attached to networks also present a risk. Consider the hack of the financial and customer data of 1,800 Target stores via a digital scale in the deli department. This should give one pause about empowering the Internet of Things with millions, if not billions, of cheap Chinese made devices.

A new report from the Center for Cyber Security in Denmark declares cybersecurity threats in telecom networks have reached unprecedented levels. While the UK, US, Australia and Japan have pursued explicit restrictions on known malicious vendors, many European nations prefer a different path that requires minimum security standards.[23] The threat is hardly limited to Huawei and ZTE.[24] Other Chinese government owned firms present similar vulnerabilities and are listed in the US National Vulnerabilities Database including Hangzhou Hikvision Digital Technology Co., Ltd. (surveillance cameras), Lenovo (laptops), Lexmark (printers), and TCL Corporation (smart TVs).The recent report Stealing from the States: China's Power Play in IT Contracts documents how these firms are embedded in state and local government networks, home to treasure troves of sensitive government data, but overseen with fewer controls and resources than federal networks.[25]

---

[18] https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents
[19] https://www.reuters.com/article/us-china-cyber-norway-visma/china-hacked-norways-visma-to-steal-client-secrets-investigators-idUSKCN1PV141
[20] https://www.theregister.co.uk/2019/04/04/chinese_hackers_bayer_but_german_giant_says_it_withstood_attack/
[21] https://www.theguardian.com/australia-news/2019/jun/06/china-behind-massive-australian-national-university-hack-intelligence-officials-say
[22] https://www.telecomstechnews.com/news/2018/jun/20/symantec-chinese-hacking-telecoms-satellites/
[23] https://fe-ddis.dk/cfcs/nyheder/arkiv/2019/Pages/trusselsvurdering-telesektoren.aspx
[24] http://www.strandreports.com/sw8281.asp
[25] https://chinatechthreat.com/special-report-state-contracts-with-banned-chinese-tech-manufacturers/

With the dawn of the internet and the growth of networks, many policymakers downplayed security concerns. Afterall, the internet started as a project amongst trusted users who knew each other. However, now that connected networks underpin so many aspects of the economy, society, and government, we need to be more concerned not just about who runs the networks, but also who supplies them, their subcontractors, and the products they use. The days of just doing things on the cheap are over. We have learned that cutting corners on price and accountability entails a risk that's too high to take. That is, if policymakers truly care about their obligations in national defense and whether they see the nation's information, technology, and secrets just something to be traded away for access to China's markets and cheap financing.

It is understandable and justified that companies should scrutinize the choice of network provider and equipment. Telecommunications networks bind people, employees, companies and machines in UK together, and data in large quantities flows through the British networks. Given many negative experiences with Chinese theft of intellectual property, systematic industry espionage and hacking, it is only reasonable that companies would request a non-Chinese vendor. This is no different than the many regulations imposed by governments on companies to protect data. If governments care so much about protecting data, they should be doing more to protect people and enterprise from the many tech threats posed by the military and government of China and its affiliates.

The European Commission and the European Cybersecurity Agency released an important report on coordinated risk assessment and cybersecurity for 5G. [26] The report was created with limited stakeholder dialogue with telecommunications companies, infrastructure providers, and national authorities responsible for cybersecurity. The engagement did not include corporate users and institutions, the users that make a large part of network traffic. In its coverage of the report, the FT asked EU Security Commissioner Sir Julian King whether the report is a" fig leaf "for countries to use Huawei products, that is a means of political cover for countries to use dangerous equipment from China (The term "fig leaf" is metaphorical reference to Adam how Adam covered his nudity in the garden of Eden.).[27] who responded, "It doesn't look like a fig leaf to me." [28] While some may prefer voluntary standards, it is likely that many governments will require telecom companies rip and replace parts of the equipment from China – Core network and in some cases Core and radio access network (RAN) equipment.

The is systematic espionage of industry in the UK.

While security analysts and military intelligence officials have described the vulnerability of supply chains various industries, policymakers are finally paying attention.

---

[26] https://europa.eu/rapid/press-release_IP-19-6049_en.htm
[27] https://www.ft.com/content/90d53db6-ea7f-11e9-a240-3b065ef5fc55
[28] https://ec.europa.eu/commission/commissioners/2014-2019/king_en

Last year, the Department of Homeland Security in USA formed an Information and Communications Technology supply chain task force filled with representatives from both the public and the private sectors. A law passed last December led to the creation of the new Federal Acquisition Security Council, which held its first meeting last month. And the White House recently released an executive order prohibiting the acquisition or use of any information and communications technology or service coming from a company deemed a national security threat.

China has been engaged in a decades long, systematic, state-sponsored effort to steal UK technology. Beijing has relied heavily on stolen trade secrets and intellectual property to build its own indigenous manufacturing and technology base. Recent U.S. intelligence community estimates suggest that China employs 30,000 military cyber spies and 100,000 private sector cyber experts whose job is to steal foreign secrets and technology.[29]

The launch of China's new stealth fighter J20 has some components that are believed to have been stolen[30] from Lockheed Martin and some of its subcontractors.[31] Is it a coincidence that China's J20 (which first flew in 2011) looks very close to an the USA's F35, which first flew in 2006? Probably not.

Earlier this year, the US Central Intelligence Agency informed its counterparts in Australia, Canada, New Zealand, and the UK that Chinese technology company Huawei has received funding from the Central National Security Commission of the Communist Party of China, the People's Liberation Army, and a "third branch of the Chinese state intelligence network." This further demonstrates Huawei's ties to the Chinese government and military, which is continues to deny.

What the future looks like for the telecommunications industry in Europe

To see the future of the telecom industry, look at what happened with banking. European banks have been required to implement Anti-Money Laundering and the Counter Terrorist Financing.[32] Telecom authorities will likely see cybersecurity as vital and telecom infrastructure as important. So just as the banks have been put under a regulatory regime to address corruption, the telecom industry will be required to implement deterrence of cyberattacks.

National telecom regulatory authorities in Europe publish information about the telecom industry including the number of customers, mobile coverage, percentage of landline infrastructure, speed, pricing, and other obligations such as antidiscrimination/net neutrality. This information is likely to expand to the resilience of networks. In the long term the EU will find ways to assess the security of each operator's network.

---

[29] http://telecoms.com/opinion/in-china-the-government-controls-everything-except-the-100000-hackers-attacking-western-targets-every-day/

[30] https://nationalinterest.org/blog/buzz/hacked-how-china-stole-us-technology-its-j-20-stealth-fighter-66231

[31] https://nationalinterest.org/feature/chinas-secret-tunnel-heart-americas-defense-industry-64116

[32] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/anti-money-laundering-and-counter-terrorist-financing_en

Just as speed data is published today, safety and security data will be published in future, e.g. number of data breaches etc. In this way, security could become a competitive parameter like price, mobile coverage, speed etc. Indeed, it could become a marketing point for operators to say that the network was free of malicious vendor.

Governments around the world will impose increasing responsibility on telecommunications companies for security.

It is likely that the UK governments will impose increasing responsibility on telecommunications companies to protect their clients against cyberattacks in the same way as the financial sector has been required to monitor and report—if not deter, money laundering and fraud. These obligations on telecommunications companies are similar to requirements that Facebook and Twitter police news and content.

Strand Consult's goal is to create transparency so that telecommunications companies and their customers make decisions on an informed basis. This response is based on real world experience and the many negative experiences of theft of intellectual property, espionage, and hacking perpetrated by actors and firms associated with the Chinese government and military. Policymakers must recognize the Chinese tech threat and secure the nation accordingly.

April 16, 2020