Written evidence submitted by Roslyn Layton

The Security of 5G

Testimony from Roslyn Layton, PhD

Visiting Scholar, American Enterprise Institute

Visiting Researcher, Aalborg University

Founder, ChinaTechThreat

Thank you for the honor of responding to this inquiry. As a Visiting Scholar at the American Enterprise Institute, I testify to policymakers around the world on a variety of telecom policy and regulation topics, including network security.[1] I earned a PhD in mobile network policy and economics from the Centre for Communication and Information Technologies at Aalborg University in Denmark.[2] Given the growing interest and concern about the role of the Chinese Communist Party in global networks, I created a website called ChinaTechThreat to collect research on these topics and provide a resource for policymakers.[3] As Co-Chair of the Program Committee for the Telecom Policy Research Conference, the leading academic conference for the field in the US, I review the emerging scholarship in field.[4] The positions expressed in this document represent my own views based upon my research and do not necessarily reflect the position of the organizations with which I am affiliated. I certify that these are true statements to the best of my knowledge.

[1] "Roslyn Layton - Bio," *American Enterprise Institute - AEI* (blog), accessed April 17, 2020, https://www.aei.org/profile/roslyn-layton/.
[2] "Roslyn Layton Profile," Aalborg University's Research Portal, accessed April 17, 2020, https://vbn.aau.dk/en/persons/roslyn-mae-layton.
[3] "China Tech Threat," accessed April 17, 2020, https://chinatechthreat.com/.
[4] Telecom Policy Research Conference Program Committee http://www.tprcweb.com/program-committee

The three key points of this testimony are

1. All communications networks are subject to security risk, not just 5G. The same approach and philosophy to promoting security should apply to all networks, not just 5G.
2. Security policy requires an integrated approach that recognizes that vulnerabilities are present in network equipment, devices, and software. Policy should secure all these elements.
3. While the technical vulnerabilities of equipment produced by Chinese state-owned and affiliated enterprises such as ZTE and Huawei are considerable and present opportunities for theft, surveillance, espionage, and sabotage, China's legal framework alone is reason enough to prohibit the use of technology made by Chinese state owned and affiliated enterprises in UK networks. China's regime effectively promotes information communication technology as tools of the Chinese state, requiring any data collected on any Chinese-made product or service to be confiscated by the Chinese government for any reason and with no respect to due process or UK rule of law.

Following are answers to the specific questions posed by the Committee.

- **What is the role of government in 5G cyber security?**

Security and Defence are the protection of the nation state, its citizens, economy, and institutions. They are essential duties of government. Safeguarding the nation state includes a range of activities to prevent, deter, and mitigate attacks by adversarial foreign nations, as well as strengthening the nation's security and defense through economic and technological development. "Cyber security" is a subset of security, and it can be a field of war like land, air, sea, and space. If a rogue nation launches a cyber

attack against a UK network, it is not so different from the launch of a missile. Both cause property damage and in some cases, harm and loss of life. Non-government actors including firms, scientists, and analysts play an important and complementary role to government in cyber security.

Ensuring the defense of the UK's communications networks does not mean that the UK government itself should produce the elements of networks, but it does require that the UK develop and promote policy which promotes the security of network elements and limits vulnerabilities. The government also plays an important role to develop economic policy which encourages the private investment in networks, innovation in security technologies, deployment of secure networks, availability of radio spectrum, and so on.

- **What are the risks to the UK's 5G infrastructure? How can these be mitigated?**

Per the standards of the technology, 5G infrastructure incorporates both wireless and wireline networks and some satellite communications.[5] It is therefore prudent to adopt an integrated approach of security to all communications networks. Risks to infrastructure are technical, economic, legal, and geopolitical. For example, any element of information communication technology (ICT) could have a technical vulnerability which allows the network to be compromised (e.g. backdoors, kill switch, defects, malfunctions). The field of network security seeks to prevent and protect networks from such intrusions, deficiencies, and shortcomings.

Risks can be economic, for example the adoption of regulatory policy will, to a matter of degree, promote or deter investment in infrastructure, security technologies, and network innovation. Countries which fail to incentivize investment will have

[5] "Opinion: Huawei May Be Restricted in US 5G, but Wi-Fi Is up for Grabs," Jane's. April 16, 2020, https://www.janes.com/article/95550/opinion-huawei-may-be-restricted-in-us-5g-but-wi-fi-is-up-for-grabs.

limited deployment of networks and immature security technologies.[6]

The laws and policies a nation adopts can also impact the security of infrastructure, for example how and to what degree access to network information is required.[7]

For example in its Internet Security Law, China asserts sovereignty over cyberspace, authority over all internet products and services made in China, and obligations of producers of internet products and services to the Chinese state.[8] Moreover China's National Intelligence Law compels any Chinese subject to spy on behalf of the state.[9] As such, China's ICT firms can be legally enjoined to conduct surveillance at any time for any reason anywhere. There is no need of a warrant nor is there ability to challenge the government's demand. While a European or American government could ask one to cooperate for defence purposes, the activities are governed by strict rules and respect for evidence of cause, warrants, due process, redress, civil liberties, and so on. Moreover, the actor can decline to participate. Chinese firms cannot.[10]

It is also necessary to distinguish between the Chinese state which is made up of a single political party on the one hand, and on the other, the people of China, who are,

---

[6] Roslyn Layton and Michael Horney, "Innovation, Investment, and Competition in Broadband and the Impact on America's Digital Economy," Mercatus Center, August 8, 2014, https://www.mercatus.org/publications/technology-and-innovation/innovation-investment-and-competition-broadband-and-impact.

[7] Roslyn Mae Layton and Silvia Elaluf-Calderwood, "A Social Economic Analysis of the Impact of GDPR on Security and Privacy Practices," in *2019 12th CMI Conference on Cybersecurity and Privacy (CMI)* (2019 12th CMI Conference on Cybersecurity and Privacy (CMI), IEEE, 2020), 8962288, https://doi.org/10.1109/CMI48017.2019.8962288.

[8] "网络安全法（草案）全文_中国人大网," October 29, 2016, https://web.archive.org/web/20161029174914/http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm.

[9] "National Intelligence Law of the People's Republic," June 27, 2017, https://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf.

[10] Roslyn Layton, "Trump Should Ignore Chinese Manufacturers' Phony Promises," Forbes, accessed April 17, 2020, https://www.forbes.com/sites/roslynlayton/2019/02/20/trump-should-ignore-chinese-manufacturers-phony-promises/.

in effect, modern slaves in a totalitarian system. As such, the critique made is not of the Chinese people, but of the Chinese government.

The best way to eliminate the risks posed by Chinese technology is not to acquire Chinese technology in the first place, and to remove them from UK networks. In any event, the practices necessitated by Chinese law violate UK privacy law and norms.

Naturally, state-owned and affiliated entities in Russia, North Korea, Iran, and Venezuela could pose similar risks, but there are limited examples of such ICT firms.

Geopolitical factors play a role in infrastructure, particularly in communications networks where transmissions can transverse the globe and space. Some countries attempt to exert sovereignty over such transmission, demanding for example that they be stored, generated, or copied within the boundaries of certain nation states. Defence and intelligence actors need of secure communications and understandably have distinct network security requirements. However, the same concerns of surveillance, theft of information, and sabotage also motivate private actors to employ a range of technologies to protect their communications including building bespoke networks.

- **To what degree is it possible to exclude Huawei technology from the most sensitive parts of the UK's 5G network while allowing it to supply peripheral components?**

5G networks, by definition, are intelligent; there is no smart part nor dumb part of the network. The notion of a network core and periphery is an archaic typology which does not apply to 5G. In practice, each cell site of a 5G network is a de facto core. There is no periphery as such. The speed and near zero latency of 5G comes from the fact that data processing occurs within each cell site, not in a central server room. As such, there is no periphery in a 5G network where Huawei could exist to reduce risk, as it were. As such, no solution that includes Huawei is acceptable to have a secure network.

- **What credible alternatives are available to Huawei systems?**

Many policymakers are under the delusion that Huawei is necessary for UK's 5G networks; it is not. This myth is perpetuated by marketing promoted by Huawei. In point of fact, US 5G networks are built without Huawei technology. Moreover, Huawei does not hold the essential patents for 5G; these are held by Qualcomm, Ericsson, Nokia, Intel and others. Australia is another country which has banned Huawei for years and has not suffered a delay in its 5G development.

Fortunately, there are many alternatives to Huawei including Ericsson, Nokia, Samsung, and variety of long tail providers, such as the Latvia-based MikroTik.[11] These vendors are price competitive with Huawei. Best of all, they present neither the security nor legal vulnerabilities of Huawei.

5G operators can also vary the equipment they purchase by sharing cell sites with other operators, increasing power levels from towers to reduce the need for small cites, plan their purchases over time, and opt for software-defined networking. Indeed, 5G networks are more than hardware; software is a significant component, and the software providers are largely American.

The need for 5G equipment is also highly dependent on spectrum. The more spectrum the government allocates for 5G, the less equipment is needed on the ground. Maximizing spectrum for 5G is one of the most important strategies to deter Huawei and to develop a counterbalance to China's state-centered ecosystem where the entire value chain can be delivered by a state-owned or affiliated enterprise. China already has some 500 MHz of mid-band spectrum allocated for 5G and has the equipment providers, device makers, mobile operators, operating systems, and platform providers to deliver a

[11] "MikroTik," accessed April 17, 2020, https://mikrotik.com/.

5G network with services on top.

Moreover, China is developing its own internet architecture. While we could accept that China decides to go its own way and uses only native technology within China; there will be a problem of China exporting its technology, particularly to countries in Asia, Africa, and South America. As such, Western entities must develop 5G technologies and promote them globally.

Economic risk compounds the longer we wait to deploy 5G. The issue is not the choice of vendor; indeed, rollout policy matters much more than choice of vendor. The 5G equipment itself matters less than the services we use it for. While the West may have an advantage in semiconductors (the building blocks of 4G/5G networks), the leadership and provenance of new technologies in quantum computing, artificial intelligence, and space are up for grabs. There is nothing to stop China from dominating these fields. In fact, China expects to and will deploy all manner of tactics to do so.[12]

More to the point, if Huawei provided high value for money in its network equipment, then Europe would not have a network investment gap of €150 billion. Indeed, if Huawei was such a bargain, Europe would have long ago closed the investment gap. It is not the choice of equipment vendor that drives 5G deployment (or vendor restrictions thereof), but rather the deployment policy itself, the investment incentives, availability of spectrum, the local permissions to erect cells, masts and towers. Consider how the US has a comprehensive 5G policy focusing on spectrum, infrastructure deployment, and modernized regulation.[13]

- **To what extent was the UK Government's decision on Huawei driven by political rather than technical factors?**

[12] Ward, Jonathan. *China's Vision of Victory*. Atlas Publishing and Media Company, 2019.
[13] "The FCC's 5G FAST Plan," Federal Communications Commission, September 15, 2016, https://www.fcc.gov/5G.

A technical and legal analysis would demand that any ICT product or service produced by a company owned or affiliated with the Chinese government should be restricted in UK networks. That policy should apply to the network equipment, Wi-Fi routers, and phones by ZTE and Huawei but also Hangzhou Hikvision Digital Technology Co., Ltd. (surveillance cameras), Lenovo (laptops), Lexmark (printers), and TCL Corporation (smart TVs) to name a few.

The political part of the decision was the UK government holding back from a complete ban of Huawei, which appears to be motivated by a fear of upsetting the Chinese government. Perhaps it was meant to allow the Chinese government save face. However diplomatic that may be, diplomacy is not a failsafe strategy for network security. The UK needs more reliable methods for 5G security.

Nor does it help that the WPP's Wavemaker inked a $350 billion contract with Huawei.[14] In addition to its considerable budget for marketing communications, Huawei is a top spender in lobbying. Its goal is to convince the UK public that Huawei is a maker of cool technologies while distracting from the heinous surveillance conducted in China with these tools.[15] [16]

Consider the video developed for the UK market "Huawei – A new future is on the Horizon" touting the company's artificial intelligence, user interface, mobile services, operating system, and 5G network-- all running over Huawei devices.[17] How difficult it must be for UK Members of Parliament to have a fact-based discussion on 5G security in

[14] Laurens Cerulus, "Huawei's $350M Branding Contract," POLITICO, March 5, 2020, https://www.politico.eu/article/huawei-350-million-branding-contract-wavemaker-5g/.
[15] *China: "The World's Biggest Camera Surveillance Network" - BBC News*, accessed April 17, 2020, https://www.youtube.com/watch?v=pNf4-d6fDoY.
[16] *Breaking into Huawei's 5G Tech Castle - BBC News*, accessed April 17, 2020, https://www.youtube.com/watch?v=ECFf6gMZOj4.
[17] *Huawei - A New Future Is on the Horizon*, accessed April 17, 2020, https://www.youtube.com/watch?v=lbGPv1L7abY.

the face of such slick advertising and influence. It is inconsistent that the UK should regulate the messaging of social media platforms but allow the free flow of messaging from an agent of the Chinese Communist Party.

- **How will the UK Government's decision impact the UK's geopolitical position?**
- **How important it is for the UK, separately or with allies, to maintain industrial capability in this field?**

The UK Parliament's first and foremost duty is the people of the UK, not the people or governments of other nations. The UK stands at a historic moment in its history. Its people voted to restore their sovereignty from the European Union. As such, it is quite right that the Defense Committee size up the many risks facing the nation and chart a forward course.

The people of the UK want defence and leadership from their government; they are rightly concerned about the threats posed by China, and they want effective action to guard their safety and security. It is likely that actions to further restrict harmful Chinese technology from the UK will be welcomed by the people.

By all means, the UK should consider playing a greater role in the world stage as an independent nation with the great strengths of its universities, scientists, enterprises, productive capacity, and natural resources. It should grow its ability to patent intellectual property of all kinds including networks. It should investigate any and all opportunities where it can create an advantage, and Defence needs to evolve to support this development.

The Chinese make tempting offers; they dangle money and make a lot of false promises. While China's market may be considerable, it is not open to UK technology. No Western company can grow market share in China with advanced technology. Any

technology which the government deems strategic will be appropriated.[18] That is the goal of the Made in China 2025 strategy.

The future is what the UK will make it. The UK need not be prisoner to conventional wisdom and obsolete ideas. There is no reason why the UK should not develop its own capabilities, whatever and however they decide to make them. Moreover, the UK can cooperate with trusted partners to find new opportunities. There is no shortage of capital or know-how in the UK; only the political will needs to be secured.

- **How will the UK's allies, particularly those in Five Eyes, respond to this decision?**
- **How will this decision impact the UK's security and defence capabilities and the UK's interoperability with allies?**

The UK's allies, particularly Five Eyes countries, will likely welcome the UK playing a greater leadership role. Naturally they would like the UK to be tougher on Chinese tech threats. They want greater trust, security, and confidentiality to cooperate. Using Huawei and other Chinese state-owned equipment in networks breaks the security of allied cooperation.

When the US banned Huawei, it did not reduce competition. In fact, it created the opportunity for Samsung to enter the 5G network space. By making its security requirements clear and limiting Huawei and other malicious vendors, the UK will signal to trusted partners and vendors the increased opportunity for enterprise. This will incentivise the long-tail of non-Chinese 5G suppliers to emerge.

17 April 2020

[18] The goals and practices of the modern Chinese state are described at length. See Gertz, Bill. *Deceiving the Sky: Inside Communist China's Drive for Global Supremacy*. Encounter Books, 2019.Pillsbury, Michael. "The 100 Year Marathon. China's Secret Strategy to Replace America as the Global Superpower." *Hudson Institute* (2015).