Written Evidence submitted by Dr Robert Dover, University of Leicester (SFG0008)

Author Note: I am an Associate Professor of Intelligence and International Security at the University of Leicester. I research into the areas of the government's use of intelligence, horizon scanning, and crisis communications, as well as UK defence and security policy.

Summary of Evidence

The UK government, and its agencies, have a substantial role to play in 5G cyber security. The decision to allow Huawei to provide a limited amount of technology into the 5G infrastructure does not allay the technical nor political fears surrounding this involvement. Indeed, maintaining this position is likely to cause a substantial problem for the UK in the Five Eyes group and NATO in the short to medium terms. The vulnerability to the UK's critical infrastructure and government communications comes precisely from the peripheral network. The COVID-19 crisis provides a (largely unwelcome) opportunity to reflect on security implications of the decisions made around 5G, whilst also providing an involuntary pause on further rollout as the infrastructure is physically attacked by those believing the unevidenced conspiracy theories around the masts.

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

1) Since World War Two the role of governments in core infrastructure projects has been seen in largely ideological terms. Governments of all stripes have oscillated between government being intimately involved and conversely being more remote, setting the terms and allowing the private sector to determine the operationalisation of such projects. Consequently, we can see not only private providers involved in core infrastructure but also – as with our energy provision – non-UK private interests in positions of core trust.

2) Because the 5G infrastructure will open up far greater levels of connectivity, including allowing for scaled usage of autonomous vehicles, far greater delivery of public services online, and the collection of data about individuals and individual movements to allow for smarter cities, it will generate data that is useful to and usable by competitor and adversary governments. It contains, therefore, more risks than a standard communications network, to run alongside the potential economic and social rewards.

3) The 5G infrastructure sits squarely within the definitions provided in the 1989 Security Service Act (and the similarly phrased 1994 Intelligence Services Act):

> "(2)The function of the Service shall be the protection of national security and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means.
>
> (3) It shall also be the function of the Service to safeguard the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands."

4) These existing Acts provide adequate justification for the government, in the guise of their core intelligence agencies, to be actively involved in the protection of the 5G infrastructure as it is rolled out. It also makes identification of re-routing, compromise or acting in reliance on intercepted materials part of the counterintelligence and countersubversion functions of the agencies. Whilst we think of 5G as a set of technologies that will bring economic benefits, we can see from the

acquisition and use of large internet data sets, how the economic quickly becomes relevant to the political and security spheres.

5) The threats from foreign interference include direct targeting of services and infrastructure reliant on 5G, interception of critical communications, broadcasting of disinformation or signals designed to cause disruption, and societal level profiling. The latter would provide a competitor state with an advantage over the UK, who would not be as well placed to conduct similar data capture and assessments over that target nation.

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?

6) The selective exclusion of Huawei from the 5G network misunderstands the nature of the technology.

7) It is possible to have a core and periphery within communications, and that is standard within security sectors across the globe. But it is where non-sensitive government departments communicate across the peripheral network, or officers or officials communicate across that peripheral network, or could have meta-data or movement data siphoned that presents an enduring risk. It would be impossible to ensure the sanctity of the 5G network within a core and periphery model, and it might be useful to think through a theoretical proposition of whether Parliamentarians would have been comfortable with a company that was alleged to be associated with the Soviet government having a key role in the UK's telephony network during the Cold War? The analogy is stretched, of course, but China (up to the point of COVID-19 and one would assume ongoing) is building up patterns of influence and control across the globe that present an enduring disruption to international relations. So, the 'China question' is likely to be one of the key questions akin to those posed by the Cold War in the twenty first century.

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

8) As an interested observer, the government's decision seemed to be a post-Brexit hedge between its historic allegiance to the transatlantic alliance and the likely economic realities of seeking to enhance its non-European trading position. A decision based purely on security would have looked markedly different and likely mirrored the position of the United States.

How will the UK's allies, particularly those in Five Eyes, respond to this decision?

9) The decision to allow Huawei into the infrastructure in any capacity contains a large risk that the Five Eyes arrangements will be compromised in some form. It would have been reasonable in 2019 to suggest that a UK outside of the European Union would need to make some smart choices about balancing international allegiances going forward. Written from the perspective of 2020, and amidst the COVID-19 outbreak, the notion of further de-risking our national relationship with China would seem not only to be prudent, but also essential. The main foreseeable risks to the Five Eyes alliance (from a purely open source perspective) are political and technical.

10) The political risk is that the current US Administration carries through with its threats to throttle back or cut off the supply of various types of intelligence product (be it signals, communications, or imagery intelligence), as a response to the threat it perceives or as a penalty for the failure of the UK to comply with its assessment. In turn we could suppose that the Australian government is likely to be supportive of any American move in this regard, because the Chinese security state is the largest

state-actor threat in their region. A change of US Administration in November is unlikely to row back from these measures, because of the reputational risk of being seen as 'soft' on security policy.

11) The technical risk will – in part – depend on the way that the US and UK security communities communicate with each other, and the possible lines of intersection that Chinese equipment might dissect. One would assume (but cannot know) that there are discrete or solely purposed infrastructure for these communications. If that is the case, then state to state communications should be preserved. If there are any lines of intersection, even tangential ones such as one UK government department communicating with another UK government department where intelligence is alluded to or imputed, then there remains a technical risk to Five Eyes intelligence product.

12) Following *The Washington Post's* January 2020 story about the joint Cold War BND / CIA *Operation Thesaurus*, that became *Operation Rubicon*, we can further suggest that the US intelligence community's particular sensitivity about Huawei and our communications infrastructure is a lesson drawn from *Rubicon*: they know the power of communications intelligence, and the insights it can bring into the workings of a competitor (or even allied) government. The 5G network is far more pervasive than the government communications cypher network that was weakened by *Rubicon* during the Cold War, thus the intelligence potential of 5G is far greater to a competitor or adversary state.

13) The other lesson of *Operation Rubicon* is the extent to which shielding corporate structures can potentially disguise intelligence community activity through proxy organisations. The intelligence community's continued assertions about corporations being compromised by Chinese state actors may be a reflection of closed source intelligence, may be an area studies reading of how political-technological culture works in China or (again) may reflect the US/German experience of *Operation Rubicon*. Regardless of which of those, or how those are blended, we can see from *Rubicon* that the intelligence and security organisations are able to successfully own and run corporations as plausibly deniable, but useful entities to assist the acquisition of intelligence.

How will this decision impact the UK's security and defence capabilities and the UK's interoperability with allies?

14) If the US Administration and the Five Eyes alliance conclude that certain types of product cannot be shared with the UK because of the presence of Huawei equipment in our core infrastructure, then this will have a stark impact on our inoperability not only with the FEYE, but also with organisations such as NATO as well.

15) The debate now should be focussed on the following issues:

a) Can the 5G rollout be suspended or phased more slowly, to allow for alternative providers to come into the market? (This would involve a discussion that balances the potential economic and societal gains, against a delay. But the immediate recovery from COVID-19 provides a window of opportunity to pause and allow some of the existing economy to re-find its footing before scaling the 5G network and therefore more ambitious economic projections. The conspiracy theories around 5G and infections will also need to be unwound, and the motivation of those seeding the conspiracies understood, before attempting to advance a more comprehensive rollout).

b) Do we have a sufficient understanding of the traction that might be gain by a competitor or adversary state able to intercept data flowing through 5G switches? Do we know enough about

ownership structures or structures of influence within the mooted suppliers to be sure that material cannot be intercepted and rerouted?

c) Do we have sufficient understanding of how Huawei technology works, and of how we would ensure constant assurance of a consistency of purpose? Could we help to create open source standards, to reduce the emphasis upon proprietary standards and to therefore diversify the market and make assurance simpler to achieve? To have made their (differing) assessments about Huawei's involvement in the 5G infrastructure the US and British security communities must have a set of standards they are benchmarking to, thus making the creation of a common standard relatively straightforward.

d) Can a US acquisition of Nokia (for example) allow for a pooling of research and development, and manufacturing to allow for an Anglosphere 5G solution? We should again note the lessons of *Rubicon*: this might well become a choice of who we prefer to be vulnerable to, the US intelligence community, or the Chinese intelligence community. This choice does not seem particularly difficult to me, but it is a choice and it needs to be made intentionally. There is sufficient research, development and manufacturing capacity within the Five Eyes nations to sustain an industrial capability in this field, made up of government technologists, university researchers and private developers.

16 April 2020