INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT

Statement on 5G suppliers

There has been a great deal of public and parliamentary debate recently as to whether the Chinese technology company Huawei should be allowed to supply equipment for the United Kingdom's 5G telecommunications network. Despite the Government's announcement in 2017 that the UK would be a global leader in 5G, the Government has yet to make a decision as to which companies will be involved.

In a sense, this is not surprising. 5G will transform our day to day lives – if it meets its full potential – and it could be key to our future prosperity. Such an important decision therefore requires careful consideration. However, the extent of the delay is now causing serious damage to our international relationships: a decision must be made as a matter of urgency.

At the heart of the public debate has been suspicion around Huawei as a Chinese company. The US and Australia have banned the company from their networks – despite it being a world leader in the development of 5G technology – voicing concern over the nature of Huawei's relationship with the Chinese state and therefore the potential risk of espionage or sabotage.

However the National Cyber Security Centre (NCSC) – which, as part of GCHQ, provides cyber security advice – has been clear that the security of the UK's telecommunications network is not about one company or one country: the 'flag of origin' for telecommunications equipment is not the critical element in determining cyber security. This is logical: we know, for example, that Russia has carried out significant hostile cyber activity against UK telecommunications networks, and yet there is no Russian equipment in the UK's networks.

The point being made in NCSC's statements thus far appears to be that this is not about whether or not Huawei – or indeed any company – might wish to, or be instructed to, sabotage the UK network or use it to spy on the UK. It is that the UK network has to be built in such a way that it can withstand attack from any quarter – whether that be malicious action from someone within the network, a cyber attack from actors outside, or simple human error. Their approach, in effect, is to assume all worst case scenarios and protect the network accordingly.

In so doing, some parts of the network will require greater protection: critical functions cannot be put at risk. But there are less sensitive functions where more risk can be carried. (It is this distinction – between the sensitivity of the functions – that must

determine security, rather than where in the network those functions are located: notions of 'core' and 'edge' are therefore misleading in this context.) We should therefore be thinking of different levels of security, rather than a one size fits all approach, within a network that has been built to be resilient to attack, such that no single action could disable the system.

NCSC have said that this can best be achieved by diversifying suppliers. The arguments for this are two-fold: reducing over-dependence and increasing competition. First, the network should not be dependent on just one vendor, as this would render it less resilient. Secondly, requiring Mobile Network Operators to use equipment from more than one vendor increases competition between those vendors which will force them to improve their security standards. And it is this raising of the bar on cyber security standards across the board that is needed – together with a requirement for more stringent regulation and enforcement of those standards.

However the telecoms market has been consolidated down to just a few players: in the case of 5G there are only three potential suppliers to the UK – Nokia, Ericsson and Huawei. Limiting the field to just two, on the basis of the above arguments, would increase over-dependence and reduce competition, resulting in less resilience and lower security standards. Therefore including a third company – even if you may have some security concerns about them and will have to set a higher bar for security measures within the system – will, counter-intuitively, result in higher overall security.

NCSC's position is eminently sensible: the UK must have a secure 5G network that is protected against the wide range of threats rather than focussing on just one potential threat. However, this issue cannot be viewed solely through a technical lens – because it is not simply a decision about telecommunications equipment. This is a geostrategic decision, the ramifications of which may be felt for decades to come.

First, there is the question of our intelligence-sharing relationship with our closest allies. From amongst our Five Eyes partners, the United States and Australia have already been vocal in their concern that the UK might employ Huawei within its 5G network. We should emphasise that this is not about any risk to the communication channels which are used for intelligence exchange – these would always be kept entirely separate. It is about perception as much as anything: our Five Eyes partners need to be able to trust the UK and we must not do anything which puts that at risk – the value of the partnership cannot be overstated.

And there is a question as to whether other countries might follow the UK's decision. The UK is a world leader in cyber security: therefore if we allow Huawei into our 5G network we must be careful that that is not seen as an endorsement for others to follow. Such a decision can only happen where the network itself will be constructed securely and with stringent regulation.

Then there is the UK's well-publicised desire for a strong economic relationship with China, and questions have been raised as to whether that is colouring our judgement on this issue. The public debate implies that we have to choose between good economic links with China and our own national security, on the basis that if Huawei were not included in our 5G network that would irretrievably damage our relationship with China. This is a simplistic viewpoint, and those promoting it do a disservice to China. As a pragmatic global power, China clearly recognises the importance of reciprocity and mutual respect in international relations: the Chinese government would not allow a British company to play a similarly significant role in China's critical national infrastructure – and they will understand if the UK decides to follow their example. There are, after all, many other important areas on which we can collaborate to our mutual benefit.

This debate must not therefore be characterised as one between those who are 'pro-China', and those who are 'anti-China'. China, with its dynamic economy and growing global influence, is – and will continue to be – a key economic and diplomatic partner for the UK, and one with which we must continue to deal with respect. Huawei itself is a remarkable company which has achieved extraordinary technological advances, and brought radical innovation and competition to a sector that, without Huawei, might lack these attributes.

Indeed one of the lessons the UK Government must learn from the current debate over 5G is that with the technology sector now monopolised by such a few key players, we are over-reliant on Chinese technology – and we are not alone in this, this is a global issue. We need to consider how we can create greater diversity in the market. This will require us to take a long term view – but we need to start now.

In terms of the immediate issue, restricting those companies who may be involved in our 5G network will have consequences: both in terms of time and cost. And the Government must weigh these, together with the security advice that any risk posed could be managed in a secure system, against the geostrategic issues outlined above. It is important to take the right decision, and take it we must: this debate has been unnecessarily protracted and this has damaged our international relationships. The new Prime Minister will no doubt have many issues to deal with in his first days in office. Nevertheless, this Committee urges him to take a decision on which companies will be involved in our 5G network, so that all concerned can move forward.