Jeremy Wright's Oral Statement on the Telecoms Supply Chain Review

Mr Speaker, with permission I would like to make a statement.

New telecoms technologies and next generation networks like 5G and full fibre can change our lives for the better. They can give us the freedom to live and work more freely, they can help rural communities to develop thriving digital economies and help the socially isolated maintain relationships. They can transform manufacturing and make possible connected and autonomous vehicles, smart clothes and agriculture.

But we can only begin this revolution with confidence if our critical infrastructure remains safe and secure.

We know that there are those who have the intention and the capability to carry out espionage, sabotage and destructive cyber attacks against our communications sector.

And the move to 5G brings a new dimension to these risks, given the increased dependence that our national infrastructure is likely to have on those networks over time.

That's why soon after taking up this office I commissioned a review into the UK Telecoms Supply Chain, involving government, industry, international partners and the National Cyber Security Centre, and designed to assess the security and resilience of the UK's telecoms networks, and determine what should be done to improve them.

Today I have published it's conclusions.

The Review identified three key areas of concern.

Firstly, that existing arrangements may have achieved good commercial outcomes but have not incentivised cyber security risk management.

Secondly, that policy and regulation in enforcing telecoms cyber security needs to be significantly strengthened to address these concerns.

And finally, that the lack of diversity across the telecoms supply chain creates the possibility of national dependence on single suppliers, which poses a range of risks to the security and resilience of UK telecoms networks.

The Review has concluded that the current level of protections put in place by industry are unlikely to be adequate to address the identified security risks and deliver the desired security outcomes.

So, to improve cyber security risk management, policy and enforcement, the Review recommends the establishment of a new security framework for the UK

telecoms sector. This will be a much stronger, security based regime than at present.

The foundation for the framework will be a new set of Telecoms Security Requirements for telecoms operators, overseen by Ofcom and government.

These new requirements will be underpinned by a robust legislative framework. We will pursue legislation at the earliest opportunity to provide Ofcom with stronger powers to allow for the effective enforcement of the Telecoms Security Requirements and to establish stronger national security backstop powers for government.

Until the new legislation is put in place, government and Ofcom will work with all telecoms operators to secure adherence to the new requirements on a voluntary basis.

Operators will be required to subject vendors to rigorous oversight through procurement and contract management. This will involve operators requiring all their vendors to adhere to the new Telecoms Security Requirements.

They will also be required to work closely with vendors, supported by government, to ensure effective assurance testing for equipment, systems and software, and to support ongoing verification arrangements.

In addition, we must have a competitive, sustainable and diverse supply chain, if we are to drive innovation and reduce the risk of dependency on individual suppliers.

The Government will therefore pursue a targeted diversification strategy, supporting the growth of new players in the parts of the network that pose security and resilience risks.

We will promote policies that support new entrants and the growth of smaller firms.

This includes research and development support, promoting interoperability and demand stimulation, for example through the Government’s 5G Trials and Testbeds Programme.

And we will also seek to attract trusted and established firms to the UK market.

Because a vibrant and diverse telecoms market is not just good news for our consumers, but it is good news for our national security too.

The review also concludes that there should be additional controls on the presence in the supply chain of certain types of vendor which pose significantly greater security and resilience risks to UK telecoms.

The House naturally will be particularly concerned, of course, with the position of the Chinese technology firm Huawei. The government is not yet in a position to decide what involvement Huawei should have in the provision of the UK’s 5G network and I want to explain why that is.

On 16th of May the US government added Huawei Technologies Ltd and 68 affiliates to its Entity List on national security grounds.

US companies now have to apply for a licence to export, re-export or transfer a specified range of goods, software and technology to Huawei and named affiliates, with a presumption of denial. On 20th May the US government issued a 90 day Temporary General Licence that authorises transactions in relation to specified areas. These measures could have a potential impact on the future availability and reliability of Huawei's products together with other market impacts and so are relevant considerations in determining Huawei's involvement in the network.

Since the US government's announcement we have sought clarity on the extent and implications but the position is not yet entirely clear. Until it is, we have concluded it would be wrong to make specific decisions in relation to Huawei.

We will do so as soon as possible.

But I also believe Mr Speaker that it would be unnecessary and unwise to delay the introduction of the remainder of the Telecoms Supply Chain Review's Conclusions.

The Telecoms Security Requirements the Review proposes must apply to all companies that want to supply equipment and services in our telecoms supply chain, wherever they come from.

The Review I commissioned was not designed to deal only with one specific company and its conclusions have much wider application.

And the need for them is urgent. The first 5G consumer services are launching this year.

And the equally vital diversification of the supply chain will take time.

We should get on with it.

Mr Speaker, I recognise that colleagues may wish to pursue further the technical detail of the proposals the Telecoms Supply Chain Review makes, not least with officials at the National Cyber Security Centre, who will be available to answer questions in Room O from 10.00am to 11.00am tomorrow morning.

But I hope the whole House will agree that the future of our digital economy depends on trust in its safety and security.

And that if we are to encourage the future scale-up of new technologies that will transform our lives for the better, then we need to have the right measures in place to make our telecoms supply chain both safe and secure. That is what the approach proposed in this review will deliver, and I commend it and this statement to the House.