Baroness Morgan's Oral Statement on UK Telecommunications

My Noble Lords, with leave, I will make a statement on the security of the telecoms supply chain

This Government is committed to securing nationwide coverage of gigabit-capable broadband by 2025.

Because we know the benefits that world-class connectivity can bring.

From empowering rural businesses…

To enabling closer relationships for the socially isolated…

To new possibilities for our manufacturing and transport industries.

We are removing the barriers to faster network deployment and have committed five billion pounds of new public funding to ensure no area is left behind.

It is, of course, essential that these new networks are secure and resilient. That is why the Government has undertaken a comprehensive review of the supply arrangements for 5G and full fibre networks.

Telecoms Supply Chain Review

The Telecoms Supply Chain Review – laid in the Other Place in July last year – underlined the range and nature of the risks facing our critical digital infrastructure – from espionage and sabotage to destructive cyber attacks.

We have looked at the issue of how to maintain network security and resilience over many months and in great technical detail.

We would never take decisions that threaten our national security or the security of our Five Eyes partners.

As a result, the technical and security analysis undertaken by GCHQ's National Cyber Security Centre is central to the conclusions of the Review. Thanks to their analysis we have the most detailed study of what is needed to protect 5G, anywhere in the world.

It is also because of the work of the Huawei Cyber Security Evaluation Centre Oversight Board, established by NCSC, that we know more about Huawei, and the risks it poses, than any other country.

We are now taking forward the Review's recommendations in three areas.

World-leading regulation

First, world leading regulation.

We are establishing one of the strongest regimes for telecoms security in the world – a regime that will raise security standards across the UK's telecoms operators and the vendors that supply them.

At the heart of the new regime, the NCSC's new Telecoms Security Requirements guidance will provide clarity to industry on what is expected in terms of network security.

The TSRs will raise the height of the security bar and set out tough new standards to be met in the design and operation of the UK's telecoms networks.

The Government intends to legislate at the earliest opportunity to introduce a new comprehensive telecoms security regime – to be overseen by the regulator, Ofcom, and Government.

Market diversification

Second, the Review also underlined the need for the UK to improve diversity in the supply of equipment to telecoms networks.

Currently, the UK faces a choice of only three major players to supply key parts of our telecoms networks.

This has implications for the security and resilience of these networks, as well as for future innovation and market capacity. It is a 'market failure' that needs to be addressed.

The Government is developing an ambitious strategy to help diversify that supply chain. This will entail the deployment of all the tools at the Government's disposal, including funding.

We will do three things simultaneously:

We will seek to attract established vendors who are not present in the UK, to our country…

We will support the emergence of new, disruptive entrants to the supply chain…

And we will promote the adoption of open, interoperable standards that will reduce barriers to entry…

The UK's operators are leading the world in the adoption of new, innovative approaches to expand the supply chain.

The Government will work with industry to seize these opportunities.

And we will also partner with like-minded countries to diversify the telecoms market.

Because it is essential that we are never again in a position of having limited choices when deploying important new technologies.

High Risk Vendors

The third area covered by the Review was how to treat those vendors which pose greater security and resilience risks to UK telecoms.

As I know the House has a particular interest in this area, I will cover this recommendation in detail.

Those risks may arise from technical deficiencies or considerations relating to the ownership and operating location of the vendor.

As noble Lords may recall, the Government informed the Other Place in July that it was not in a position to announce a decision on this aspect of the Review.

We have now completed our consideration of all the information and analysis – from the National Cyber Security Centre, industry and our international partners.

And today, I am able to announce the final conclusions of the Telecoms Supply Chain Review in relation to high risk vendors.

In order to assess a vendor as high risk, the Review recommends a set of objective factors are taken into account. These include:

- the strategic position or scale of the vendor in the UK network…
- the strategic position or scale of the vendor in other telecoms networks, particularly if the vendor is new to the UK market…
- the quality and transparency of the vendor's engineering practices and cyber security controls…
- the vendor's resilience both in technical terms and in relation to the continuity of supply to UK operators…
- the vendor's domestic security laws in the jurisdiction where the vendor is based and the risk of external direction that conflicts with UK law…
- the relationship between the vendor and the vendor's domestic state apparatus…

And finally, the availability of offensive cyber capability by that domestic state apparatus, or associated actors, that might be used to target UK interests.

New controls on high risk vendors

To ensure the security of 5G and full fibre networks, it is both necessary and proportionate to place tight restrictions on the presence of any companies identified as higher risk.

The debate is not just about ‘the core’ and ‘the edge’ of networks. Neither is it just about trusted and untrusted vendors.

Threats to our networks are many and varied, whether from cyber criminals or state sponsored malicious cyber activity.

The most serious recent attack on UK telecoms has come from Russia, and there is no Russian equipment in our networks.

The reality is that these are highly complicated networks relying on global supply chains, where some limited measure of vulnerability is inevitable.

The critical security question is: how to mitigate such vulnerabilities and stop them damaging the British people and our economy?

For 5G and full fibre networks, the Review concluded that, based on the current position of the UK market, high risk vendors should be:

Excluded from all safety related and safety critical networks in Critical National Infrastructure…

Excluded from security critical network functions…

Limited to a minority presence in other network functions up to a cap of 35 per cent…

And be subjected to tight restrictions, including exclusions from sensitive geographic locations.

These new controls are also contingent on an NCSC-approved risk mitigation strategy for any operator who uses such a vendor.

We will legislate at the earliest opportunity to limit and control the presence of high risk vendors in the UK network, and to allow us to respond as technology changes.

Over time, our intention is for the market share of high risk vendors to reduce as market diversification takes place.

I also want to be clear that nothing in the Review affects this country’s ability to share highly sensitive intelligence data over highly secure networks, both within the U.K. and with our partners, including the Five Eyes.

GCHQ has categorically confirmed that how we construct our 5G and full fibre public telecoms networks has nothing to do with how we share classified data.

And the UK’s technical security experts have agreed that the new controls on

high risk vendors are completely consistent with the UK's security needs.

NCSC industry advice

In response to the Review's conclusions on high risk vendors, the Government has asked NCSC to produce guidance for industry. This guidance was published earlier today on the NCSC's website.

The NCSC has helped operators manage the use of vendors that pose a greater national security risk, such as Huawei and ZTE, for many years.

This new guidance will include how it determines whether a vendor is high risk…

The precise restrictions it advises should be applied to high risk vendors in the UK's 5G and full fibre networks…

And what mitigation measures operators should take if using high risk vendors.

As with other advice from the NCSC on cyber security matters, this advice will be in the form of guidance.

The Government expects UK telecoms operators to give due consideration to this advice, as they do with all their interactions with the NCSC.

Conclusion

I hope the whole House will agree that if we are to achieve our digital connectivity ambitions, it is imperative that we trust the safety and security of our telecom networks.

Risk cannot be eliminated in telecoms.

But it is the job of Government, Ofcom and industry to work together to ensure that we reduce our vulnerabilities and mitigate the risks.

This Government's position on high risk vendors marks a major change in the UK's approach.

When taken together with the tough new security standards that will apply to operators, this approach will substantially improve the security and resilience of the UK's telecoms networks, which are a critical part of our national infrastructure.

It reflects the maturity of the UK's market and our world-leading cyber security expertise, and follows a rigorous and evidenced-based review. It is the right decision for the UK's specific circumstances.

The future of our digital economy depends on trust in its safety and security.

And if we are to encourage the takeup of new technologies that will transform our lives for the better then we need to have the right measures in place.

That is what this new framework will deliver and I commend this statement to the House.