Report for Huawei Technologies (Belgium) SA/NV

on government measures affecting 5G network equipment suppliers

by EY LAW SA/BV

21 September 2020

Building a better working world

Reference & Disclaimer

Reference & Disclaimer

This Report was commissioned and scoped by Huawei Technologies (Belgium) SA (the 'Client' or 'you').

Anyone within the Client organization that receives a copy of this Report should note the following caveat.

This Report necessarily represents only part of the information considered in carrying out the work, being that which was considered to be most relevant to an understanding of the Client's needs.

If the Client requires any further information or explanations on the underlying work, you should contact us.

The information in this Report is correct as at 18 September 2020.

The Report is solely for the use of the Client and is not intended to and should not be used or relied upon by anyone else. EY LAW SA does not accept any duty of care, to any other person or entity other than the Client. The Report has been prepared for the purpose set out in the Engagement Letter between EY LAW SA and the client dated 27 August 2020.

EY LAW SA understands that the Client might release the Report publicly on the basis that it is published for general information only and that we do not accept any duty, liability or responsibility to any person (other than the Client) in relation to this Report. Recipients of this Report should seek independent expert advice as this Report was not prepared for them or for any other purpose than that detailed in the engagement terms with the Client and cannot be relied upon other than for this. Information contained in the Report is current as at the date of the Report, and may not reflect any event or circumstances which occurred after the date of the Report.

To the extent that this Report, in whole, part or a summary is communicated by the Client to a third party or published, the following statement shall appear alongside or in any such communication:

> "This report and its contents has been produced by EY LAW SA for and at the request of Huawei Technologies (Belgium) SA. The report is for the benefit of Huawei. While Huawei is free to publish this report or communicate its contents to third parties, EY LAW SA has no responsibility towards any such third party, who cannot rely on the contents of this report.
>
> Copying or extracting any material part of this report is permitted subject to identifying its source."

The information and views set out in this Report are those of the author(s) and do not necessarily reflect the opinion of EY LAW SA.

Authors:

Kiran Desai, EY LAW SA

Charles Bodreau, EY LAW SA

Table of Content

Table of Content

EY Law

Table of Content

Table of Content

EY Law

1

Executive summary

Executive Summary

Executive Summary

Preceding the date of this Report there has been an escalation in activity by governments concerning named suppliers of 5G network equipment. This activity has been in the realm of political announcements, pronouncements and debates, policy thinking and papers, reviews, soft laws (declarations, guidance, announcements et al. by governments and government agencies), formally and informally proposed draft laws and to a limited extent adopted laws.

Huawei approached us to consider from a legal perspective in relation to competition and cybersecurity the identification of an appropriate methodology and how it may best be applied to address government measures affecting 5G network equipment suppliers.

The geographic scope is the European Union but the Report will take account of the extent, if any, to which the European Union in law or practice is affected by the laws of the United States of America.

The objective is to use an authenticated methodology to consider the impact of the government measures. In describing and at a preliminary level applying the methodology the Report raises questions intended to act as an aid to stimulate serious consideration by stakeholders. As such, the Report may stimulate action and ideas for the production of evidence and/or technical papers that could be used by stakeholders.

The Report adopts the methodology used by the European Commission when it produces an impact assessment report, namely, a report assessing the impact of possible EU action (EU Better Regulation Toolbox) and, in relation to cybersecurity the methodology of the European Commission's Cybersecurity Toolbox. OECD methodology is also used as regards the competition law and policy optic. Together, the methodologies raise a set of questions to be addressed.

Executive Summary

Executive Summary

In light of the preliminary analysis undertaken in addressing those questions, the following recommendations are made:

1. **Encourage a deeper review of the situation**:

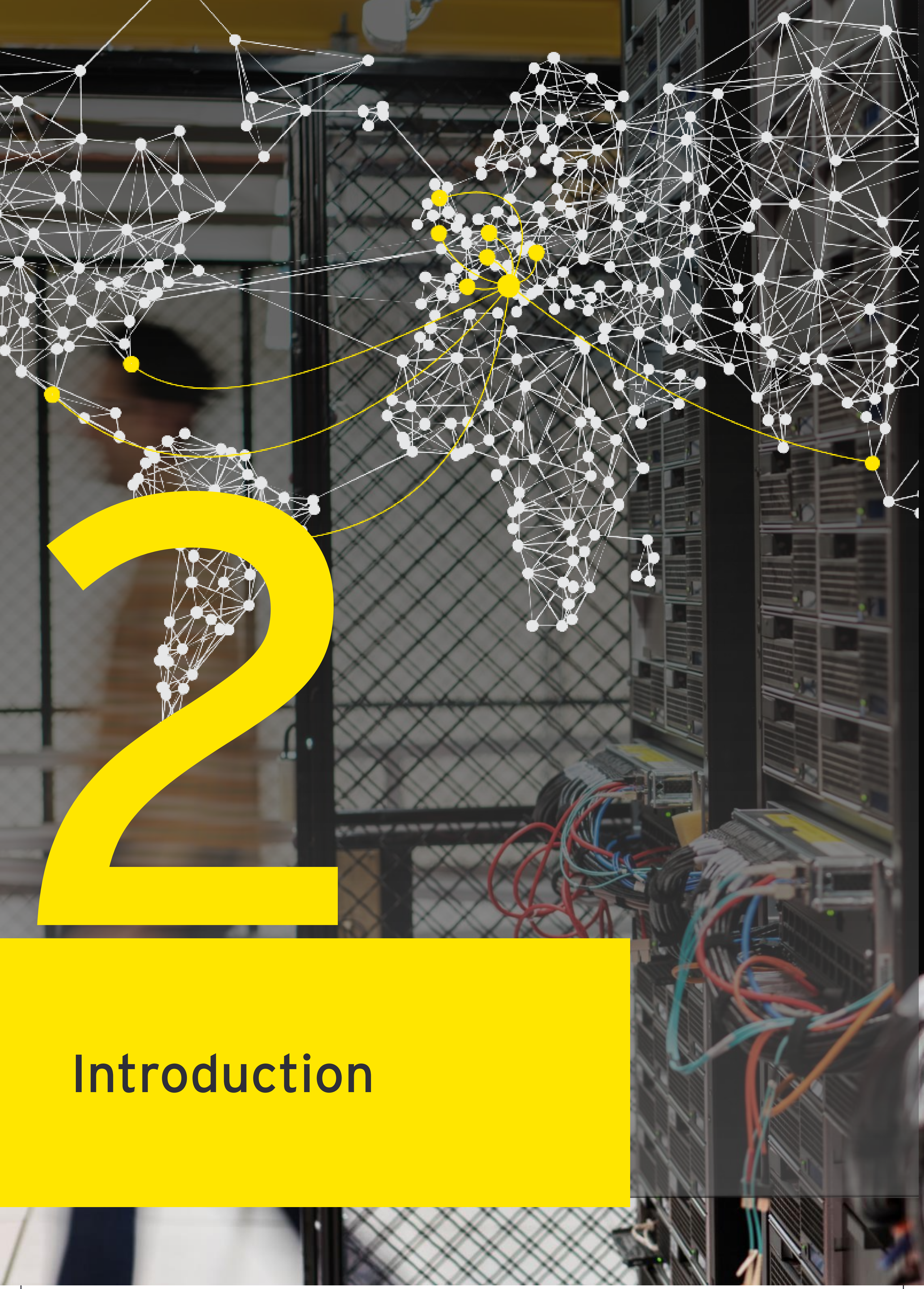
   It is proper for all governments to review the situation and to strengthen the review where the subject is important. It is also proper to simplify the actual or proposed measures without negatively affecting the achievement of the underlying policy goal. To achieve this objective a REFIT-like review would allow a comprehensive and transparent review. Speculatively stated, a more focused measure than the blanket prohibition of named suppliers' products from a 5G network might both achieve the desired objectives and mitigate the negative knock-on effects.

2. **Encourage an antitrust investigation**:

   A competition investigation could be undertaken to determine the consequences of the government measures. This would be a prequel to and might lead to ex-ante actions intended to negate or reduce anticompetitive outcomes foreseen by such analysis.

3. **Encourage using 5G network technologies as a test case in relation to the Cybersecurity Act**:

   This would contribute to the better understanding of how the Cybersecurity Act would work in practice. It would allow for a focus on the technical aspects of cybersecurity. It would also facilitate a level playing field across the EU and, given the influence of EU regulations generally, inform other countries.



2

Introduction

2. Introduction

2.1. Scope

This report uses the optics of (a) competition law and policy and (b) cybersecurity law and policy as regards the impact on

(i) telecommunication 5G network operators, and

(ii) governments,

of government measures that exclude or limit the use of named suppliers' 5G network equipment (**the 'Report'**).

The geographic scope will be the European Union but the Report will take account of the extent, if any, to which the EU in law or practice is affected by the laws of the United States of America. The Report does not materially address the situation in every EU Member State but where appropriate the Report notes developments in the EU Member States and, given its importance within Europe, the United Kingdom. For certain purposes there is a focus on the United Kingdom and France.

The Report takes account of government measures as at the date of issue of the Report. The government measures taken account of are those (presumed) lawful adopted measures but not statements about possible future measures or recommendations that are not implemented into law. However, account is taken of the (i) EU's Cybersecurity Act, (ii) FY 2021 NDAA; (iii) Cyberspace Solarium Commission Report; (iv) U.S. State Department's announcement regarding the 5G Clean Path; (v) Prague Proposals; (vi) the Joint Declarations between the United States and each of Czech Republic, Estonia, Latvia, Poland, Romania and Slovenia; (vii) UK NCSC advice reviewed in July 2020; (viii) France's law on national security interest in connection with mobile radio networks; and (viii) draft legislation on the subject in Poland and Romania. The measures are set-out in Annex 1.

Of the EU-27 Member States and the United Kingdom, 5G commercial services had been deployed in 10 as at end March 2020.[1] For the majority of those coverage is limited. Consequently, this Report addresses a nascent market and consideration of the impact of government measures is speculative given some of the measures are not formally adopted or have yet to have a market effect.

A diagram representing the different parts of a 5G network can be found in Annex 2.

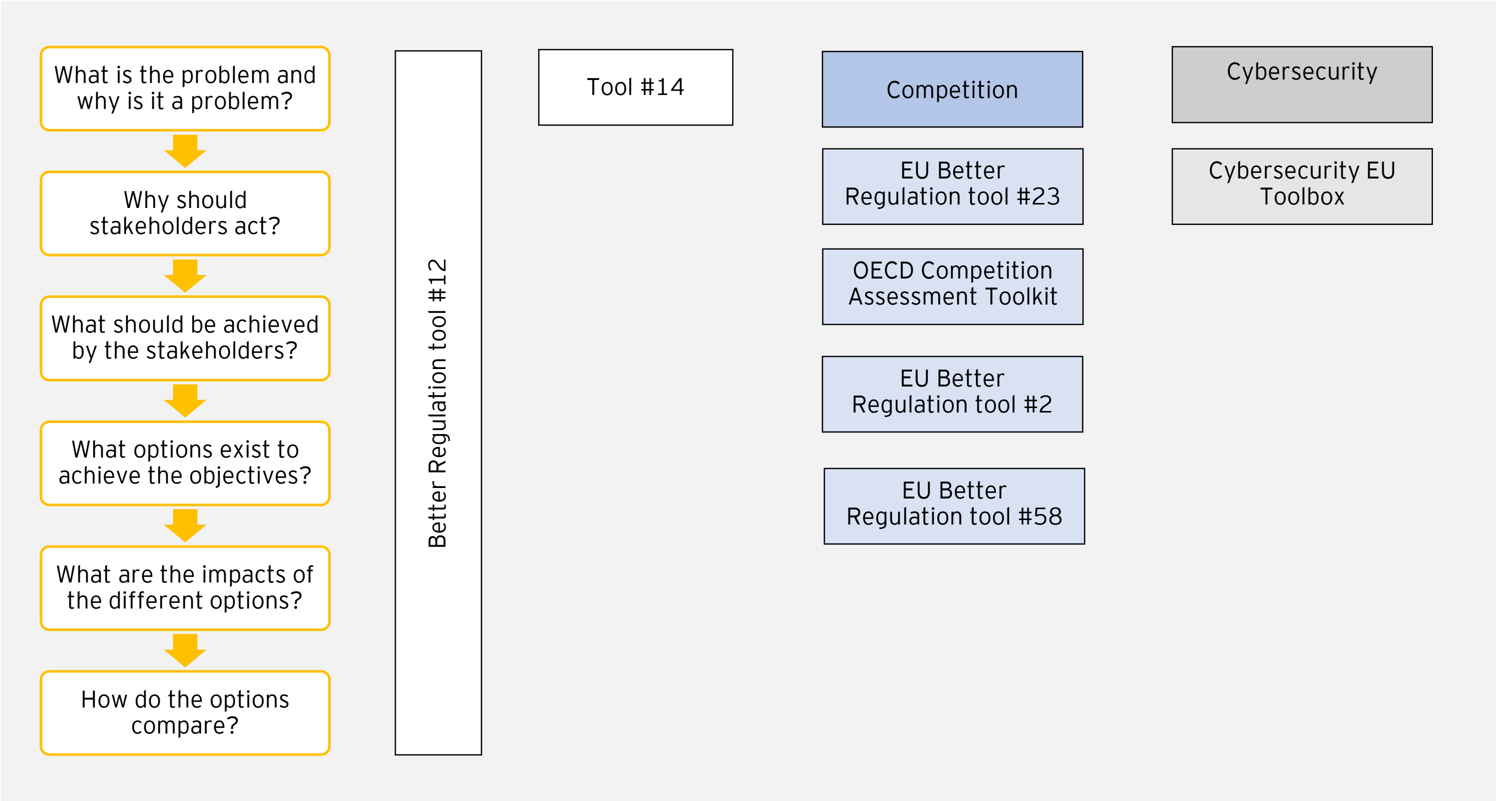
2.2. Objective

The objective is to use an authenticated methodology to consider the impact of the government measures. In describing and at a preliminary level applying the methodology the Report raises questions intended to act as an aid to stimulate serious consideration by stakeholders. As such, the Report may stimulate action and ideas for the production of evidence and/or technical papers that could be used by stakeholders.

1. European Commission, 5G Observatory, see https://5gobservatory.eu/market-developments/5g-services/.

2.3. Methodology

The Report adopts the methodology used by the European Commission when it produces an impact assessment report, namely, a report assessing the impact of possible EU action. This has the benefit of being a well-regarded and institutionally accepted methodology. As regards the specifics of the methodology, Better Regulation tool #12 has been used as closely as possible for the format of the Report and the key steps, as shown on the left hand-side of the diagram below.[2] As regards the first step, 'What is the problem and why is it a problem?', the Report uses the methodology in 'Better Regulation tool #14. How to analyze problems'.[3]



As regards the optic of competition law and policy we reference the impact assessment methodology used by the European Commission[4] and by the OECD[5] when assessing competition issues.

As regards the optic of cybersecurity/cyber resilience law and policy, we reference the EU Commission's toolbox used by it for risk mitigating measures for the cybersecurity of 5G networks.[6]

2. European Commission, *Better Regulation Toolbox, tool #12. Format of the IA Report*, see https://ec.europa.eu/info/sites/info/files/file_import/better-regulation-toolbox-12_en_0.pdf.
3. European Commission, *Better Regulation Toolbox, tool #14. How to analyze problems*, see https://ec.europa.eu/info/sites/info/files/file_import/better-regulation-toolbox-14_en_0.pdf.
4. European Commission, *Better Regulation Toolbox, tool #23. Competition*, see https://ec.europa.eu/info/sites/info/files/file_import/better-regulation-toolbox-23_en_0.pdf.
5. OECD, Competition Assessment Toolkit, see http://www.oecd.org/competition/assessment-toolkit.htm.
6. European Commission, *Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures*, see https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

3

What is the problem & why is it a problem?

3. Why and What is the problem?

When analyzing a problem, the following five issues should be addressed

1. What is the problem and why is it problematic?
2. Assess the magnitude of the problem.
3. Establish the causes (drivers) namely is it due to
   a. Market failure,
   b. Regulatory failure,
   c. Inequitable outcome, and/or
   d. Behavioral bias.
4. Identify who are the relevant stakeholders.
5. How is the problem likely to evolve with no further action.

In this Report we directly address question 1. We do not address question 2.[7]

the speculative question is whether the government measures could be an example of regulatory failure, namely, when public policy action appeared justified but fails to solve the problem satisfactorily or helps create new problems'.

For question 3 the speculative question is whether the government measures could be an example of regulatory failure, namely, when public policy action appeared justified but fails to solve the problem satisfactorily or helps create new problems. For question 4 the scope of the Report addresses the subject as regards telecommunication 5G network operators and governments. It is recognized there are other stakeholders. Finally, question 5 is addressed in section 4 'Why should the stakeholders act?'.

3.1 Competition law and policy

Competitive markets encourage enterprises to be efficient and innovative, thereby creating more choice for consumers, reducing prices and improving the quality of goods and services. Increased competition contributes to the functioning of the internal market and typically improves a country's economic performance, opens business opportunities to its citizens and reduces the cost of goods and services throughout the economy. When governments intervene in markets to regulate the behavior of businesses, this can restrict competition further than is really necessary to achieve the desired policy objectives.

7. This question has been addressed at least in the following reports:
- Oxford Economics, *Restricting competition in 5G network equipment, An Economic Impact Study,* December 2019, see https://resources.oxfordeconomics.com/hubfs/Huawei_5G_2019_report_V10.pdf;
- Oxford Economics, *Restricting competition in 5G network equipment throughout Europe, An Economic Impact Study,* June 2020, see https://www.oxfordeconomics.com/recent-releases/51856cd0-46d6-409c-bcab-218875f6b510;
- Assembly Research, *Macroeconomic impact of a delayed 5G roll-out in the UK*, September 2020, see https://static1.squarespace.com/static/59ca375d80bd5e1a6eaed324/t/5f58fb7023d5c611028d482e/1599667057207/Macroeconomic+impact+of+a+delayed+5G+roll-out+in+the+UK.pdf;
- StrandConsult, *Understanding the Market for 4G RAN in Europe: Share of Chinese and Non-Chinese Vendors in 102 Mobile Networks - Version 1.2*, 2020, see http://www.strandconsult.dk/sw8772.asp

As the Commission and OECD identify in their methodologies, if there is a positive answer to any of the following questions then a detailed analysis should be undertaken. The questions are 'does the government intervention.

- limit the number or range of suppliers?
- limit the ability of suppliers to compete?
- reduce the incentive of suppliers to compete? and/or
- limit the choices and information available to customers?'

It is self-evident that the government measures limit the number of suppliers by excluding or limiting named suppliers. Therefore, pursuant to the European Commission's and OECD's methodologies a competition analysis should be undertaken of the government measures.

It is self-evident that the government measures limit the number of suppliers by excluding or limiting named suppliers. Therefore, pursuant to the European Commission's and OECD's methodologies a competition analysis should be undertaken of the government measures.

3.1.1. Key concepts

The prequel to addressing these questions is to define key concepts of competition law for this subject, namely, what is the relevant market, do market players have market power, what is the structure of the market and are there barriers to entry?

It is not within the scope of this Report to make a determination of these key concepts. However, given findings by others preliminary conclusions can be proposed. Annex 3 is a table identifying third party findings considered material to the subject and the preliminary conclusions. In summary, the preliminary conclusions are that:

- **Relevant markets:**

Based on the relevant market definition of the existing generations of technology (4G etc.), the product market for 5G network equipment will be divided between three major markets: CNS (Core Network Systems), RAN (Radio Access Network) and Network-related services. Further, each of those markets can be divided by types of equipment, components and/or technology used. With each technology improvement, new subdivisions of those markets may become relevant.

It is generally considered that the market scope is global. However, some players are not active in some areas of the world, the technical requirements are different between regions as are the level of technology developments, and customers are largely different. With increased regulation, security requirements and the exclusion of some players from some regions, it could be relevant to divide the markets by region or even countries.

- **Structure of the market:**

The evidence gathered suggests that the relevant markets are concentrated with three top-tier global companies (Huawei, Ericsson and Nokia). There are a few other players, none of them currently competing on a global basis to the same level with the three leading players.

- **Market players have market power**

The evidence gathered suggests that together the top-tier global players have a degree of market power on the relevant markets. Further analysis would be necessary to determine the level of market power on each and all product and geographic markets, in particular in light of the government measures that may impact significantly the presence of Huawei. However, there is evidence that the network equipment suppliers face a degree of buyer power from the telecom network operators that are acting either in an oligopolistic market on their domestic markets or as global buyers with material buyer power. It is an open question whether there exists a balance of power between the customers and the suppliers and, additionally, how that balance will change as a result of the measures.

It is an open question whether there exists a balance of power between the customers and the suppliers and, additionally, how that balance will change as a result of the measures.

- **Barriers to entry:**

The evidence gathered suggests that the level of investments required, complicated (high-level) R&D, time required to develop competing technology and the conformity cost of the new EU cybersecurity certification scheme create significant barriers to entry on the relevant markets. Moreover, although the developments associated with 5G technology may ease entry of new players over time, the backward compatibility requirement between 5G and existing technologies increases the costs for new players to enter the markets and limits their ability to enter the markets in a timely fashion.

3.1.2. Practical assessment

On the basis of the determination of the key concepts, a practical assessment can be made by addressing the following questions: what is the impact of the government measures on:

- **existing firms?**
- **entry of new firms?**
- **Prices?**
- **non-price elements? and**
- **upstream and downstream (or related) markets?**

It is not within the scope of this report to make a determination of these elements. However, given findings by others, preliminary conclusions can be proposed. Annex 4 is a table identifying third party findings considered material to the subject and the preliminary conclusions. In summary, the preliminary conclusions are that:

Existing firms:

The exclusion of the leader of the industry will likely result, in the short and medium-term, in a significant increase in the market shares of the two other top-tier global players. Moreover, the cybersecurity requirements of diversification of suppliers or limiting the presence of certain suppliers (e.g., NCSC's advice for a 50/50 split between suppliers for any given network) might limit the incentive of the players to compete once they reach their 'maximum allocated' share of the market.

It is also self-evident that, on a market largely supplied by three players that together hold significant market power, excluding one of those players will lead to increasing the individual market power of the two remaining players.

Entry of new firms:

The entry in the market of new competitors on some new segment of the technology is likely to continue to increase regardless of the government measures. However, the government measures will increase the regulatory barriers in the markets. Moreover, given that some of the risks identified in the government measures originates in non-EU State decisions, there is a significant risk that the government measures will in effect result in an exclusionary decision of any and all companies on the basis of the country of origin. This will likely limit the numbers of suppliers able to enter in the market

Will higher sector costs lead to higher customer prices? If it is assumed that telecommunication network operators are active in a market which is not competitive then costs increases are likely to be passed-on to customers downstream (industry and consumers). If the market is assumed to be competitive, then depending upon the level of margin, it is possible only some of those costs increases would be passed-on downstream, but it follows that the market players would then be operating on lower margins, which might impact their ability to engage in capital expenditure programs.

Prices:

The results of the government measures can be expected to lead to a price increase due to (i) the exclusion of one of the largest players in the industry (who has a reputation for being towards the lower end of the price range), (ii) the higher security standard on suppliers, and (iii) the necessity to replace the existing infrastructure equipment or ensuring interoperability between suppliers equipment. Will higher sector costs lead to higher customer prices? If it is assumed that telecommunication network operators are active in a market which is not competitive then costs increases are likely to be passed-on to customers downstream (industry and consumers).

If the market is assumed to be competitive, then depending upon the level of margin, it is possible only some of those costs increases would be passed-on downstream, but it follows that the market players would then be operating on lower margins, which might impact their ability to engage in capital expenditure programs.

- **Non-price elements:**

The government measures are likely to increase the pressures to produce and supply 5G network equipment in a timely manner. This is also true for equipment for existing networks as their equipment will also need replacement. This will lead to significant delay in the implementation of 5G network in the EU.

- **5G market and other related markets:**

The conclusions developed above show that significant supportive government intervention will be required to limit the impact of the government measures. Intervention will be required to help develop interoperable standards, help the entry on the market of new players and compensate the cost increase in the development of 5G network for telecom network operators.

As the development of the existing generations showed, the early deployment of the network is crucial, giving a significant advantage for first movers, in the development of various technologies and services on the existing market and the creation of entirely new markets.

The costs increase and delay due to government measures will significantly impede the development on those markets.

3.2. Cybersecurity law and policy

The objectives of the EU cybersecurity toolbox[8] are to identify a common set of measures which are able to mitigate the main cybersecurity risks of 5G networks and to provide guidance for the selection of measures which should be prioritized in mitigation plans at national and at EU level. Nine risks are identified in the toolbox which are grouped into five risk scenarios. To address those risks the EU toolbox identifies eight possible strategic measures, eleven possible technical measures and ten possible additional supporting actions.

In this Report it is assumed that a government measure is intended to mitigate an identified risk. Rather than question the veracity of the evidence and rationale used to reach the decision to adopt a measure, this Report raises the question of the extent to which there are secondary or unintended effects as regards cybersecurity.

The first step to doing so is to identify the "potential implementation factors" per the EU cybersecurity toolbox.[9] Those three factors are:

(i) resource costs,

(ii) sector-specific economic impacts (for operators or for suppliers) and

(iii) broader economic and/or societal impacts. They can be positive and/or negative.

8 European Commission, *Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures*, see https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

9 We anticipate all governments will in some manner undertake this exercise, even if not using the methodology of the EU Member States pursuant to the EU's toolbox..

The second step is to consider those measures that are characterized as "low" or "medium" as regards their effectiveness.[10] Both those types of measures, to the extent they have secondary or unintended effects, are susceptible to the question of whether they create a problem, on the basis of either proportionality or having a net-negative effect. The EU toolbox identifies no measures the effectiveness of which is low but does identify some as medium. The table in Annex 5 identifies the medium measures and the related risks. All the measures are technical, there being no strategic or supporting measures identified as being of medium effect.

Undertaking both steps in relation to all government measures is beyond the scope of this Report. Consequently, the exercise for the purpose of providing examples addresses the government measures according to the best available public information, which has been found to be the United Kingdom, France and the United States.

Third party findings for each step and the preliminary conclusions are set-out in the tables in Annex-6 (potential implementation factors) and Annex-7 (medium technical measures).

In summary, the preliminary conclusions are that the measures:

- Will raise costs to telecommunication network operators;
- Impose costs on government and society in general;
- Require an active industrial policy, with FDI defensive measures and EU-centered R&D expenditure
- Named suppliers' products will remain in use in the short-to-medium term to avoid what would otherwise be a disproportionate negative impact;
- The 'rule' should be applied to all suppliers that are deemed to be of high risk. It is unclear how many suppliers would be affected, given concerns expressed about non-EU suppliers;
- There is no single standard to address all risks in the toolbox and this will likely create regulatory challenges for all stakeholders; and
- Measures have been adopted without publicly available evidence that the impact has been fully analyzed.

10. Low means the measure is considered hardly effective, as it is expected to mitigate the related risks only marginally. Medium means the measure is considered somewhat effective, meaning that is expected to mitigate the related risks to some extent.

3.3. Conclusion

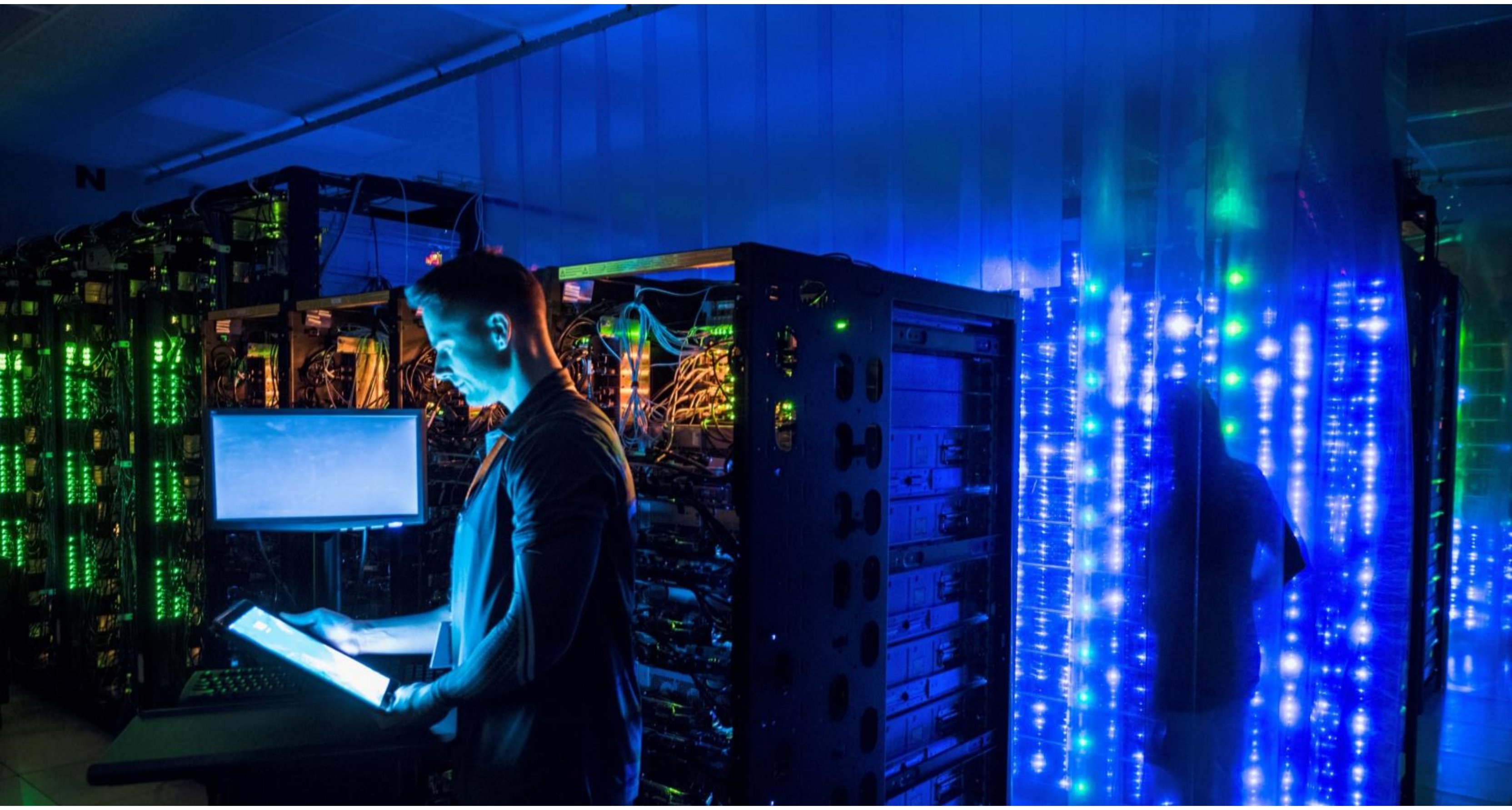
In light of the above, a preliminary conclusion can be made as regards the question of whether there is a problem and why.

Preliminary conclusion - 1

The government measures create a problem

The government measures seek to address a foreseen cybersecurity problem and have created new problems. The measures limit the number of suppliers on the market and the preliminary conclusion using a competition law and policy optic is that this will raise costs for telecommunication operators and delay the roll-out of a fully functioning 5G network. Both those ultimately have negative effects on consumers.

Using a cybersecurity optic, the measures increase the level of cybersecurity risk by placing reliance on the incumbent suppliers for at least the short to medium term. Additionally, cybersecurity regulatory oversight by government and its implementation by telecommunication network operators will be significantly increased to manage the deemed risks of having named suppliers' equipment directly or indirectly an element of the 5G network. However, the tools (standards) for such oversight and implementation might be deficient at this point in time.



4

Why should the stakeholders act?

4. Why should the stakeholders act?[11]

It is appropriate to consider separately the two stakeholders that are within the scope of the Report.

4.1. Telecommunication operators

It is assumed that telecommunication operators, as legal entities, subject to rights and obligations, seek to ensure their interests are protected and promoted. From the economic perspective this is expressed as being autonomous economic actors that are profit maximizing. From the legal perspective, using EU law as an example reference, this is expressed as the freedom of establishment (Title IV, Chapter 2 TFEU) and the fundamental right laid down in Article 16 of the Charter of Fundamental Rights of the European Union, the freedom to conduct a business within the limits of Article 17 of the Charter (right to property). The purpose of EU rules in this area is to enable businesses to be set up anywhere in the EU enjoying the freedom of movement of persons, services and capital, to provide protection for shareholders and other parties with a particular interest in companies, to make businesses more competitive, and to encourage businesses to cooperate over borders.

In light of the above, the assumption is that telecommunication operators have an interest in considering the problems identified in this Report.

Specifically, to the extent the problem negatively impacts their ability to engage in commerce, they should seek to have the problems addressed. This would encompass any aspect of commerce regulated or otherwise affected by government.

4.2. Governments

It is assumed that governments have full regard to their societal concerns and obligations (e.g. ensuring free and fair competition in the market, ensuring markets function properly and so efficiently allocate society's resources, risk management and security).

If a problem is found and the driver of the problem is regulatory failure, then government has the obligation to review its own actions and their effects and ask itself the following questions:

- Does the measure achieve a socially efficient allocation of resources?
- Has government been unduly influenced by the (partial) information provided by one or more specific interest groups (so-called "regulatory capture")?
- Is the government measure poorly designed (or expressed more positively, is it sub-optimal)?
- Does the measure have unintended negative consequences, such as favoring incumbents, creating barriers to entry and innovation or leading to excessive cumulative regulatory costs for industry?
- Is there a high risk that implementation of the measure may be poorly implemented and/or enforced?

11. The tool refers to why should the EU take action. This Report seeks to raise similar questions but as might be addressed by all stakeholders.

- Finally, is there is high risk the measure may become out of date as the world evolves and problems and drivers change?

The response to these questions, in the first instance, is that responsible governments as a matter of best practice should undertake an impact assessment to determine their best options.

Serious consideration should be given as to whether there would be benefits in replacing (emerging) different national policies and rules with a more homogenous policy approach

4.3. Conclusion

The telecommunication network operators have a right and arguably a duty to protection their commercial interests. As such it is a legitimate action directly to seek to influence government. This includes the role of public policy influencer as well as promoting its interests as regards legislative and similar legal detailed drafting. It is also legitimate to approach independent agencies about actual or foreseen concerns, including therefore the competition agencies as regards anti-competitive outcomes.

Government has the natural obligation to ensure its actions are appropriate. It is also best practice both be able to self-critical and so review measures that have been take or are proposed.

Given the preliminary conclusion that there is a problem and negative knock-on effect, if follows that both telecommunication network operators and governments, as stakeholders, have a right and arguably duty to act.

Consideration of trans-national organizations, such as the United States Federal government and the European Commission, does not alter this fundamental conclusion. Instead, it is recognized that there is added complexity.

However, that merely cautions that measures should be adopted only after achieving a reasonably strong level of assurance that action should be taken, and to review early the reasons for the decision to take action as well as the action (measure).

Compared to other governmental authorities, the European Commission is in a special position, given its obligations in relation to the Single Market and similar obligations or goals pursuant to the EU Treaty and the EU's international obligations under trade and other legal instruments. In this regard, the fundamental of ensuring the Single Market operates effectively might suggest the European Commission needs to seek a stronger role as regards the subject of this Report. The particular example is the contrasting views and so outcomes of some Member States taking measures into relation to named suppliers as regards the 5G domestic network, while others do not. On its face this would seem to lead to fragmentation of the Single Market, in particular given the need and desire for networks in each Member State to be inter-connected. In brief, serious consideration should be given as to whether there would be benefits in replacing (emerging) different national policies and rules with a more homogenous policy approach.

Preliminary conclusion - 2

The stakeholders arguably have a right and a duty to act

Telecommunication network operators should protect their own stakeholders' interests (shareholders, employees, customers) to ensure that government measures are proportionate and that secondary negative effects are mitigated. Governments should review their policies in the light of changing situations and at the trans-national level the EU should give serious consideration as to whether there would be benefits in replacing (emerging) different national policies and rules with a more homogenous policy approach in order to protect the Single Market.

5

What should be achieved by the stakeholders?

5. What should be achieved by the stakeholders?

There should be a logical link between the problem identified, the initiative to effect change and the desired outcome. Any resulting proposed actions should not themselves create side-effects that negatively impact the outcome. Additionally, for any proposed actions there would be defined indicators used to measure progress. In this vein of all possible actions, proposed actions should be S.M.A.R.T.[12]

5.1. Telecommunication operators

Specific to telecommunication operators the identified problem is that the measures raise the telecommunication operators' costs, limit their choice of suppliers and increase materially the regulatory burden. To the extent those problems might arise from anti-competitive outcomes, a competition analysis would seek to determine this and can result in remedies being adopted by government or voluntary changes by the identified market participants. However, as an antitrust analysis can only be undertaken by government, telecommunication operators can and arguably should press government to take action.

To prompt government to initiate an investigation, the following actions could be taken, each of which should be communicated to government authorities:

- Measure the likely costs increase and its impact on prices to consumers,
- Measure the likely delay in time for the roll-out of the 5G network,
- Identify the consequences for consumers as regards services that either will be available but only later or possibly not at all,
- Compare the development of the benefits of 5G in the home country with other countries,
- Propose ex-ante market regulations that could avoid supplier price increases,
- Propose alternative solutions that would mitigate the risk but produce less negative effects,
- Be vigilant for anticompetitive conduct and report any suspicions to the relevant competition authorities.

Such action to encourage the government to initiate an investigation can be done by telecommunication operators directly or via a trade body or similar association of industry representatives.

5.2. Governments

All aspects of the problem should be of interest to government. As identified in section 3 of this Report, the speculative question is whether the government measure could be an example of regulatory failure, namely, when public policy action appeared justified but fails to solve the problem satisfactorily or helps create new problems. Two outlooks could be taken by government. One is that the measure is valid but given recognition of the negative knock-on effects, counter measures should be taken to mitigate them. Second, the measure should be reviewed to determine whether it continues to be valid and to determine whether it can be changed to reduce or negate the negative knock-on effects.[13]

12. Specific, Measurable, Achievable, Relevant and Time-bound.

13. It is assumed the third possibility of regarding the measure as valid and ignoring the existence of the knock-on effect problem is not something that would be accepted as responsible government behavior, not the least as such non-action could lead to other stakeholders seeking legal redress or change.

Between these two outlooks, as of the date of this Report the former outlook has predominated. This can be expected given how recent the decisions are to adopt the measures and that for the most past the measures taken have been political announcements of what measures will be adopted or, in the case of France, application of a law without official motivation:

UK	20 July 2020 political announcement. Formally the measure does not apply until the enactment of the Telecoms Security Bill. The first draft of that Bill has not been presented to Parliament as at the date of this Report.
USA	15 May 2020 announcement re changes to the foreign direct product rules, relating to the prohibition, subject to an application for exemption, of U.S. technology, including software, from being exported from the United States, and thus in practice preventing U.S. companies from supplying Huawei with any products that use U.S. technology (provisions take immediate effect subject to a 120 days transition period). 5 August 2020 political announcement re Clean Network. No information is available on the legal measures that would turn this into law or on the timing for the adoption of such law. 5 August 2020 the FY 2021 NDAA (applying to the U.S. government's annual budget commencing 1 October 2020) re prohibition of Huawei and others from being used on the networks of Federal Agencies was adopted by the House of Representatives. The NDAA has not yet been signed into law but no information suggests it will not be signed.
France	1 August 2019, the law No 2019-810 aiming at safeguarding France's defense and national security interests in connection with the operation of mobile radio networks was enacted giving the Prime Minister the responsibility to authorize the creation or development of any telecommunication infrastructure. July 2020 authorization delivery. On the basis of law No 2019-810, several authorizations have been delivered. Without officially announcing a ban on Huawei's equipment from the French market, projects including Huawei equipment have received authorization for a shorter period than others accompanied by unofficial confirmation that those authorizations will not be renewed. This has been widely understood as an unofficial ban of Huawei from the French market, despite announcement to the contrary by a French official.[14]

14 See https://www.reuters.com/article/us-france-huawei-5g-security-exclusive-idUSKCN24N26R; See also https://www.politico.eu/article/france-introduces-de-facto-ban-on-huawei-5g-equipment-by-2028/

All three of the jurisdictions (UK, USA and France) that have been focused on in this Report have government departments, bodies or agencies that have analyzed the situation. That analysis appears to have recognized the existence of the negative knock-on effects and that counter measures should be taken. Some examples of such counter measures are:

Negative knock-on effect	Example counter measure
Need to avoid an undue delay in 5G rollout	"Given there is only one other appropriate scale vendor for full fiber equipment, we are embarking on a short technical consultation with operators to understand their supply chain alternatives, so that we can avoid unnecessary delays to our gigabit ambitions and prevent significant resilience risks". *UK Secretary of State, oral statement to the Parliament.*
Need to avoid an undue delay in 5G rollout	"The commission thus demanded that the Prime Minister proportionate the effects of his decisions to their potential impact on the deployments already carried out and on future 5G deployments, in terms of pace and cost. The service provided to users may not be degraded as a result of a refusal to grant authorization, except in particularly serious circumstances." *Report on behalf of the Senate Committee on Economic Affairs on the draft law aiming at safeguarding the defense and national security interests of France within the framework of the operation of mobile radio networks, Page 21.*[15]
Need for a supplier diversification strategy	'The strategy will focus on three core elements: First - securing the supply chains of our incumbent, non-high-risk suppliers by putting in place measures and mitigations that will protect supply chains and ensure there is no disruption to our networks. Second - bringing new scale vendors into the UK market by removing barriers to entry, providing commercial incentives and creating large scale opportunities for new vendors to enter the UK market. And third - addressing the existing structure of the supply market by investing in research and development and building partnerships between operators and vendors that will mean operators using multiple vendors in a single network will become the standard across the industry.' *UK Secretary of State, oral statement to the Parliament.*

15. Catherine Procaccia, *Report on behalf of the Senate Committee on Economic Affairs on the draft law aiming at safeguarding the defense and national security interests of France within the framework of the operation of mobile radio networks*, June 2019, *in French*, see http://www.senat.fr/rap/l18-579/l18-5791.pdf.

Negative knock-on effect	Example counter measure
Need for a supplier diversification strategy	"According to the information gathered, the Government intends, through this text, to adopt a balanced approach that aims to address all potential vulnerabilities related to the deployment of 5G, regardless of their source. Thus, the proposed law, on the one hand, does not aim to ban Huawei, on the other hand, does not concern Huawei alone: the modalities for operating the equipment would be checked for the entire network chain, regardless of the operators' service provider - equipment manufacturer or other. The Government also stresses that this initiative is independent on the international context. Consequently, two fears that emerged in the debates, namely a risk of disruption of supply and a risk due to the lack of competitiveness of operators in cases where they would not be able to use Huawei's equipment, should be able to be dispelled."[16] *Report on behalf of the Senate Committee on Economic Affairs on the draft law aiming at safeguarding the defense and national security interests of France within the framework of the operation of mobile radio networks, Page 36.*
Need for higher cyber standards for products	'Congress should resource and direct the Department of Homeland Security to resource a federally funded research and development center to work with state-level regulators in developing certifications for cybersecurity insurance products'. *U.S. Cyberspace Solarium Commission, Final Report, Key recommendation 4.4.*[17]
Need for higher cyber standards for products	'Congress should pass a law establishing that final goods assemblers of software, hardware, and firmware are liable for damages from incidents that exploit known and unpatched vulnerabilities.' *U.S. Cyberspace Solarium Commission, Final Report, Key recommendation 4.2.*
Need to develop domestic based and created technology products	'Commit Significant and Consistent Funding toward Research and Development in Emerging Technologies'. *U.S. Cyberspace Solarium Commission, Final Report, Key recommendation 4.6.2.*

16. It should be noted that at the time the law was discussed in Parliament in France, the government's announced public intention was not to exclude Huawei from the markets. As such, the discussion on counter measures was limited and did not include discussion on the diversity of suppliers or the development of domestic technology and product.

17. Cyberspace Solarium Commission, *Report*, 11 March 2020, see https://www.solarium.gov/#h.p_rK7mL_1MeZw7.

As regards the second point of view, while it is assumed governments will continue to review the situation, changes currently proposed strongly suggest that changing the measure could be difficult. This is particularly so for those governments that have or intend to adopt the measure through primary legislation. For example, the UK government has announced its intention that the measure will be set out in law by the Telecoms Security Bill (no draft is currently available), with the consequence that "By the time of the next election [i.e. 2024], we will have implemented in law an irreversible path for the complete removal of Huawei equipment from our 5G networks".[15] It remains to be seen, however, the procedural mechanism that the legislation would set-out. It is common for such detailed elements as a prohibition of a named legal entity to be set-out by order of a government minister, the order being made pursuant to power granted by legislation. In principle, therefore, the minister can also amend or repeal the order.

Many of the measures that are being proposed have yet to be formally expressed in terms of rules, let alone adopted and applicable. Nevertheless, there appears to be a propensity of intent to legislate, which as identified above can make it difficult, subsequently, to make changes to reflect the new facts. For example, in the Solarium Commission's Final Report, there are 24 key recommendations and 59 enabling recommendations.

The Commission suggests 54 separate legislative proposals to put these recommendations into effect which comprise several House Resolutions, amendments to various Acts (for example, The Homeland Security Act of 2002 and The Cybersecurity Enhancement Act of 2014) and several new Bills addressing specific subjects – in total 255 pages of new legislation.

5.3. Conclusion

The scope of this Report addresses those government measures directly excluding or otherwise limiting named suppliers' products from 5G networks. However, even a cursory review of the many cybersecurity measures that are contemplated reveal both a broad and deep app roach to the subject, particularly so in the United States where analysis and review appears most advanced. It is beyond the scope of this Report to analyze whether the package of measures are S.M.A.R.T.

are the measures directly excluding or otherwise limiting named suppliers' products from 5G networks disproportionate?

However, the apparent comprehensiveness leads to the question whether the measures directly excluding or otherwise limiting named suppliers' products from 5G networks are necessary given the totality of measures proposed or contemplated. Expressed slightly differently, are the measures directly excluding or otherwise limiting named suppliers' products from 5G networks disproportionate

18. Secretary of State Oliver Dowden, oral statement to the House of Commons (Parliament), 14 July 2020

Preliminary conclusion - 3
Further analysis is warranted

Given the scope and impact of the government measures, objective studies can be conducted to assess:

(i) the proportionality of those measures and

(ii) the extent to which counter measures are required to remedy the knock-on effects of those measures.

6

What options exist to achieve the objectives?

6. What options exist to achieve the objectives?

In order to identify the impacts of actions to be taken, a baseline is needed. Typically, the baseline is "no change". Proposals not yet adopted or implemented can be included in the baseline on the assumption that they will come into effect. Formally expressed, the majority of the measures within the scope of this Report have not entered into effect, nor even into law. However, the baseline is deemed to be the scenario that the measures are put into effect. We further assume for this scenario that all other cybersecurity measures expressed as at the date of this Report and which are to a large extent identified in this Report have a reasonable prospect of coming into effect.

6.1. Options

The next step in the methodology is to consider what possible regulatory and non-regulatory options exist for tackling the problem? It is suggested that the policy options are:

1. Competition Analysis:

Undertake a competition analysis of an ex ante nature with the objective of putting in place any measures determined necessary to ensure incumbents do not benefit from the situation to the detriment of consumers and society as a whole:

a. This would require the initiation of action by the relevant competition authorities

b. Such action, in order for the result to be effective should occur in the near term given that a competition analysis can be expected to last six months.

c. Any proposed actions to be taken due to the conclusions and recommendations of the competition analysis are likely to be directed at the incumbent telecommunications equipment suppliers, in order to ensure any temporary market power they hold does not produce outcomes that negatively affect telecommunication operators and ultimately consumers.

2. Cybersecurity Act Early Certification:

Accelerate the implementation of the EU certification for 5G network technologies as anticipated through the EU's Cybersecurity Act[19] (or construct a parallel process that is similar to it, depending upon the jurisdiction) so applying the certification regime to 5G technologies. This would ensure a validated determination of the security of each of 5G suppliers' products, processes and services. This might result in the certified ability to use specific products/processes/services for 5G technologies, on a product-by-product basis, and replace the current blanket ban.

a. This would require the initiation of action by the EU and by NISCG.

b. The sooner this is actioned, the greater and earlier would be any benefits produced.

c. Any outcomes would affect the suppliers directly and the telecommunication operators

19. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 ("Cybersecurity Act") OJL 151/15 of 7.6.2019 see https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN.

3. Comprehensive Review

Change nothing but expend additional resources on reviewing the situation and be open to change should a change in the situation indicate action should be taken.

a. This would require each government to be open to review, something which at least in principle appears already to exist given the various government bodies responsible for reporting and reviewing the situation. Such action would likely combine naturally with broader multilateral initiatives. For example, the Prague Proposals, as they address they need for a framework for analysis, the Chinese government's proposal for a global initiative on data security[20] and the existing UNGGE on cyberspace[21] or the Global Forum on Cyber Expertise.[22]

b. This action is a continual one.

c. All stakeholders would be affected.

4. REFIT Initiative:

Pursue a REFIT initiative - per the EU Regulatory Toolbox, Tool#2.[23] In brief, while retaining the overall objectives of the measures (cybersecurity protection), revise existing measures, including those which are not yet in effect. The key point is to identify opportunities to reduce regulatory costs and to simplify the measures without negatively affecting the achievement of the underlying policy goal.

a. This would require each government to be open to review, something which at least in principle appears already to exist given the various government bodies responsible for reporting and reviewing the situation.

b. This action would need to occur before the measure was adopted. In the UK, for example, this would need to occur in the near term given the government intention for the Telecom Security Bill to be passed by Parliament by the end of 2020.

c. All stakeholders would be affected.

5. No REFIT justification:

Similar to the REFIT initiative but taking the subject from the other end of the telescope, an analysis should be undertaken justifying why it is no opportunities exist to reduce regulatory costs and to simplify the measures without negatively affecting the achievement of the underlying policy goal.

a. This would require each government to be open to review, something which at least in principle appears already to exist given the various government bodies responsible for reporting and reviewing the situation.

b. This action would need to occur before the measure was adopted. In the UK, for example, this would need to occur in the near term given the government intention for the Telecom Security Bill to be passed by Parliament by the end of 2020.

c. All stakeholders would be affected.

20. See https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1812951.shtml
21. United Nations Group of Governmental Experts Advancing responsible State behavior in cyberspace in the context of international security, See https://www.un.org/disarmament/group-of-governmental-experts/.
22. See https://thegfce.org/.
23. EU Regulatory toolbox, Tool #2. The Regulatory fitness Programme and the REFIT Platform, see https://ec.europa.eu/info/sites/info/files/better-regulation-toolbox-2_en_0.pdf.

6.2 Conclusion

In light of the above, a preliminary conclusion can be made as regards the question of what options exist to achieve the objective

Preliminary conclusion - 4
Five options are identified

(i) Competition analyses;

(ii) Cybersecurity Act certification;

(iii) Comprehensive review;

(iv) REFIT initiative; and

(v) No REFIT justification

7

What are the impacts of the different options?

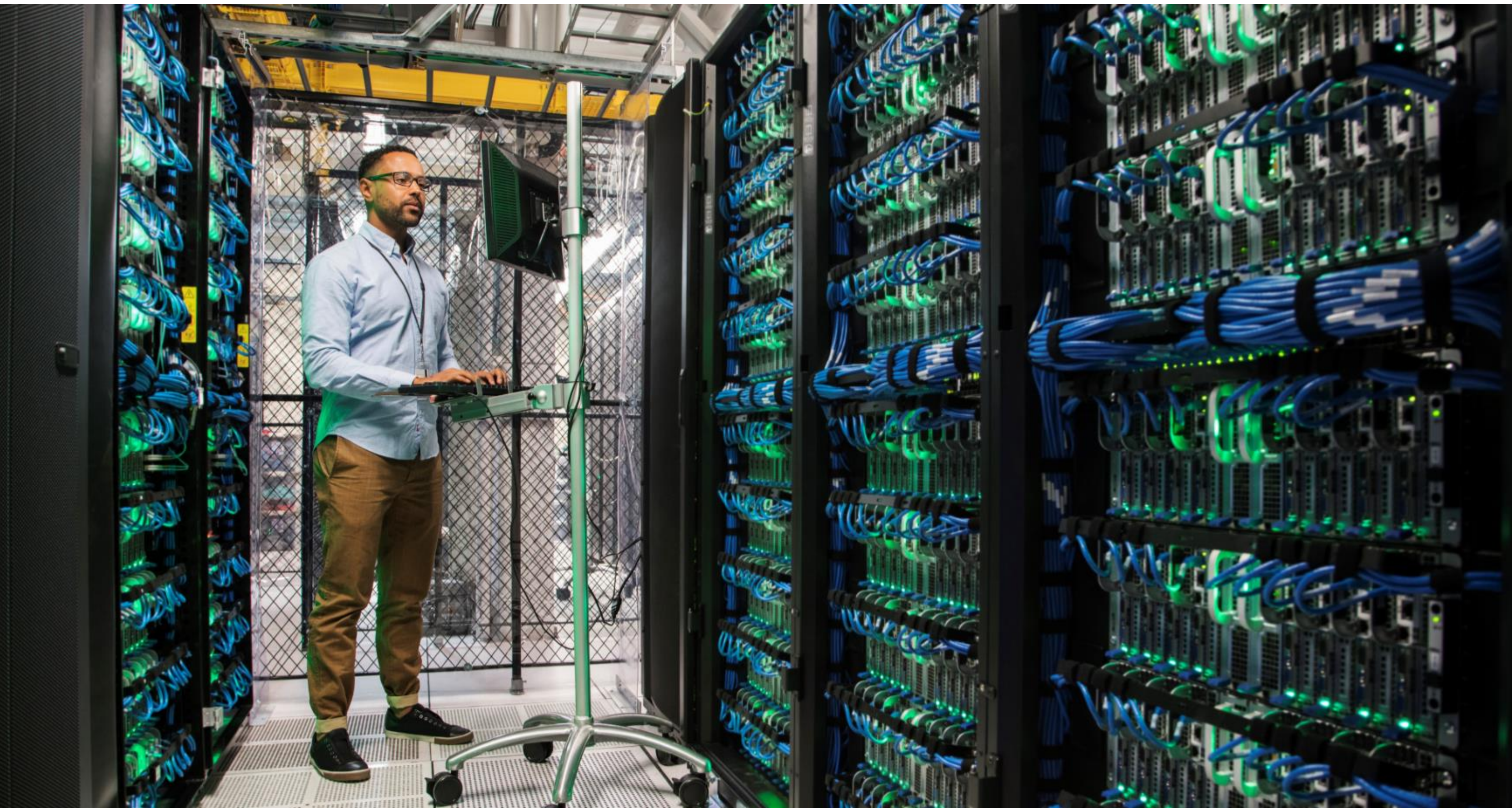
7. What are the impacts of the different options?

It is necessary to consider the likely impacts of each of the listed options. Those impacts will cover economic, legal and other societal elements affected by the options. Those impacts may be positive and/or negative. A typology exists for this costs and benefits exercise (EU Better Regulatory Toolbox, Tool #58) and wherever possible the costs/benefits should be quantified.[24]

It is important to recall that these costs and benefits are measured as to their effect on the baseline, where the baseline is the assumption that the measures (removal of named suppliers' products from the 5G network) would come into effect.

Undertaking this costs and benefits exercise is beyond the scope of this Report. However, it seems reasonable to consider the following in terms of relative likely costs/benefits.

- low (*), namely, costs/benefits to government where typically, at most, for example, the cost of expending government resources is an opportunity cost between committing resources either to (i) investigate X, (ii) investigate Y, or (iii) do not investigate.
- medium (**), namely, costs/ benefits relating to more than one stakeholder, and.
- or high (***), namely, costs/ benefits relating to more than one stakeholder and to society as a whole



24. EU Better Regulation Toolbox, Tool #58. Typology of Costs and Benefits, see https://ec.europa.eu/info/sites/info/files/file_import/better-regulation-toolbox-58_en_0.pdf

The table below identifies them with a brief comment:

Option	Cost/Benefit	Comment	Relative Cost
Competition Analysis	Direct Costs - Direct Compliance Costs - Administrative Burden	These would be both private costs (telecom operators and incumbent 5G network equipment suppliers) that engage in the public consultation aspect of an analysis and public costs (the administration) in terms of resource costs to undertake the analysis.	**
	Enforcement Costs	Could only arise if the results of the option were acted upon. They would be private costs (incumbent suppliers) as well a public cost (the administration).	**
	Direct Benefits - Market Efficiency - Cost savings & Improved Information	Could only arise if the results of the option were acted upon. They would be private benefits (telecommunication operators) through, for example, constraints on equipment prices	*
	Indirect Benefits - Wider Macroeconomic Benefits	Competition benefits are expected to flow through to the consumer.	*
	Direct Costs - Direct Compliance Costs - Charges & Compliance Costs & Administrative Costs	These would be private costs (telecommunication operators and incumbent suppliers). As they would by definition be early results, they are costs that would have occurred in any event.	*

Option	Cost/Benefit	Comment	Relative Cost
Cybersecurity Act Early Certification	Direct Costs - Direct Compliance Costs - Charges & Compliance Costs & Administrative Costs	These would be private costs (telecommunication operators and incumbent suppliers). As they would by definition be early results, they are costs that would have occurred in any event.	*
	Indirect Costs - Indirect Compliance Costs	Certification typically imposes a cost on downstream customers. As they would be definition only be early results, they are costs that would have occurred in any event.	*
	Direct Benefits - Market Efficiency - Improved Information & Wider Range of Products/services	The benefits would be both private and the wider society. As they would by definition only be early results, they are benefits that would have occurred in any event.	***
	Indirect Benefits - Indirect Compliance Benefits & Wider Macroeconomic Benefits & Other, Non-Monetizable Benefits	As they would be definition only be early results, they are benefits that would have occurred in any event.	*

Option	Cost/Benefit	Comment	Relative Cost
REFIT Initiative	Direct Costs - Direct Compliance Costs - Administrative Burden	This is largely a public (government authority) cost.	*
	Direct Benefits - Market Efficiency - Cost Savings & Wider Range of Products/Services	This is a private benefit on the basis that the ability to acquire some named suppliers' products might mean lower costs and/or better services for telecommunication network operators.	*
	Indirect Benefits - Indirect Compliance Benefits	This is a private benefit for telecommunication operators and 5G network equipment suppliers.	**
No REFIT justification	Direct Costs - Direct Compliance Costs - Administrative Burden	A relatively small public cost (for the government authority) is expected in order to undertake the analysis.	*

8 How do the options compare?

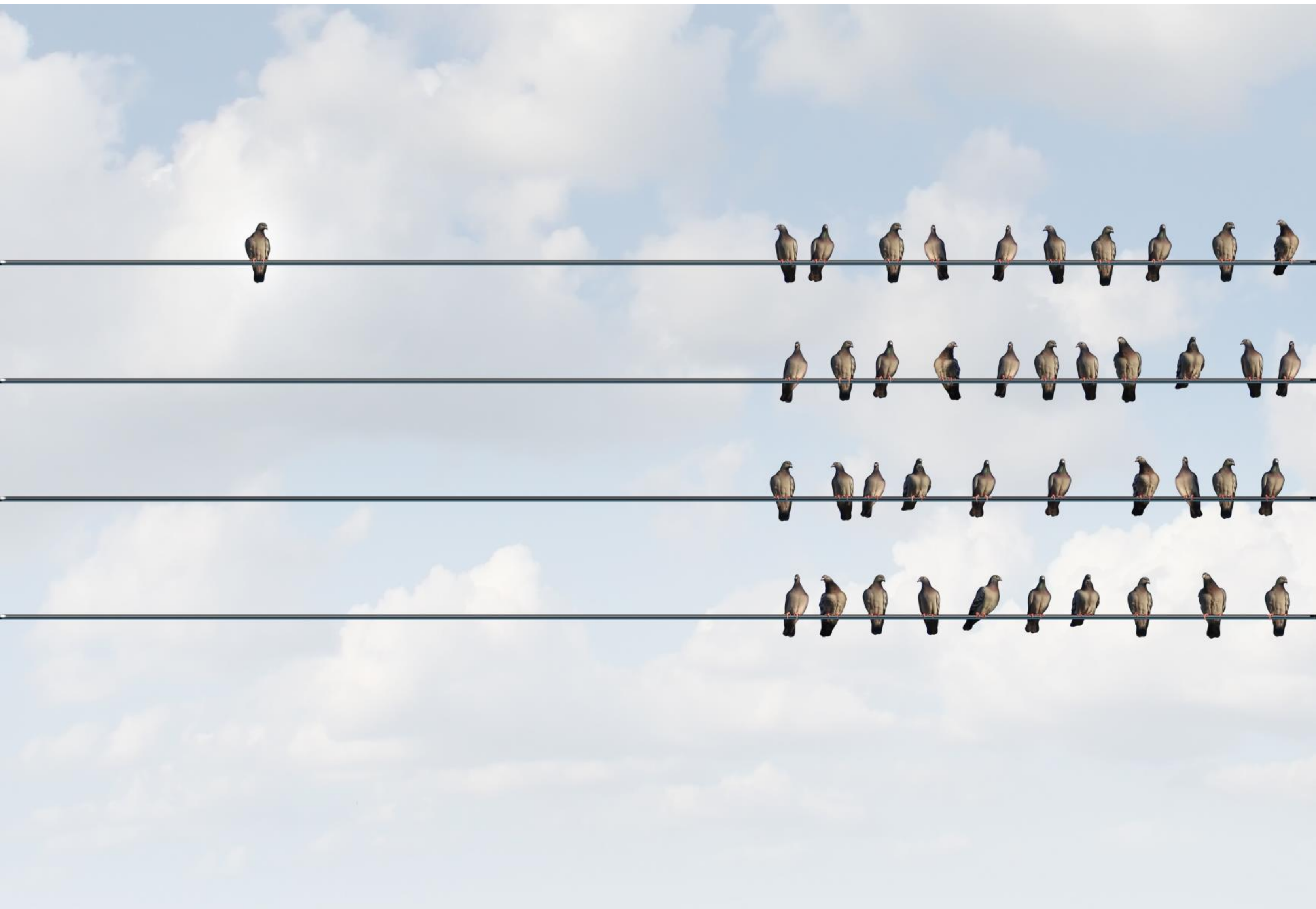
8. How do the options compare?

The comparison of the options relates to their effectiveness (extent of achievement of the objectives), efficiency (costs and benefits) and coherence with the surrounding policy and legal environment.

Undertaking this exercise is both beyond the scope of this Report and not plausible in the absence of quantitative results. Nevertheless, some preferential ranking can be suggested.

This has the benefit of presenting a 'target' for deeper consideration and challenge as to priority. Alternatively, if the ranking is not regarded as contentious, it can stimulate fuller consideration of the lead ranking options.

Having made this caveat, the following table offers insight on the relative strengths of the options with a relative ranking of highest (5/5) to lowest (1/5), with 3/5 being neutral. To pursue this partial exercise to its natural conclusion, the higher the aggregate ranking the better



Comparator	Competition Analysis	Cybersecurity Act Early Certification	Comprehensive Review *	REFIT Initiative *	No REFIT Justification
Option goes beyond what is necessary to address the problem	5	5	5	5	5
Option addresses the issue given its geographic scope (boundary test)	2 - if at State level; 4 - if at the multistate level	2 - if at State level; 4 - if at the multistate level	2 - if at State level; 5 - if at the multistate level	2 - if at State level; 5 - if at the multistate level	1
Option is coherent and as simple as possible?	4	3	4	5	5
Option creates costs? † ‡	2	3	3	4	4
Option creates benefits? ‡	2	4	4	2	0
Aggregate total	**15 (or 17 if multistate)**	**17 (or 19 if multistate)**	18 (or 21 if European / Multilateral)*	18 (or 21 if European / Multilateral)*	15

Note:

* *Assuming adopting this option leads to changes.*

† *Where a high cost, which is regarded as a negative, would be accorded a low ranking of '1'.*

‡ *The costs and benefits allocation is at best indicatory and relative to its own category. There is no intention to suggest that a costs allocation of '2' is similar in absolute to a benefit allocation of '2'. In reality costs may aggregate to far more than the benefits, or vice-versa.*

9

Comment and recommendations

9. Comment and recommendations

Pursuant to the methodology of an impact assessment, the next step would be to identify the preferred option with an explanation as to why it is preferred, or why there is no preferred option (e.g. inconclusiveness comparison of options). Such a definitive conclusion is not appropriate given the scope of this Report. Nevertheless, the following observations can be made about the options.

First, the Comprehensive Review, REFIT Initiative and No REFIT justification are of a similar nature. The thrust of the analysis undertaken strongly supports all government initiatives to continue and to strengthen a review of the situation but also to simplify the actual or proposed measures without negatively affecting the achievement of the underlying policy goal. In that regard, a REFIT-like initiative over-and-above the on-going review of the situation would seem appropriate. In this regard it is noted that the Prague Proposals are consistent with establishing a proper framework for adopting measures given the statement that 'Proper risk assessment [is] essential - Systematic and diligent risk assessment, covering both technical and non-technical aspects of cyber security, is essential to create and maintain a truly resilient infrastructure. A risk based security frameworks [sic] should be developed and deployed, taking into account state of [the] art policies and means to mitigate the security risks.'[25] As a result of continued and strengthened review, speculatively stated, a more focused measure than the blanket prohibition of named suppliers' products from a 5G network might both achieve the desired objectives and mitigate the negative knock-on effects.

Adopting such an action together with trans-national (EU) and international engagement by governments would likely further the benefits of these options because of the global nature of the industry and, therefore, the fact that aspects of the solution are arguably exogenous to any individual country or region.

Second, a Competition Analysis is a stand-alone exercise. It can produce inputs for longer term considerations, such as industrial policy review as well as suggest immediate remedies to actual problems or foreseen problems. At its most simply expressed, it is an exercise that obtains information and analyses the situation in a manner and thoroughness that seems not to date to have been undertaken by governments. This seems a missed opportunity. Competition law and policy is a mature optic with well-rehearsed economic and legal elements that can be brought to bear on the subject. In contrast, the analysis of cybersecurity is an emerging discipline. The advantage, therefore, of using the competition law and policy optic is that it is capable of being undertaken within a well-defined analytical framework. In addition, most mature governments have competition authorities that are independent of government. As such, the authority's analysis can be undertaken largely absent any claim of being materially influenced by the political, industrial policy or trade agenda of the government.

25. See Annex 1.

Third, the Cybersecurity Act and its underlying processes are complex. Whether an *ad hoc* process, analogous to a test case could credibly be instituted is a matter beyond the scope of this Report. However, if it could be an example case it would appear also to be able to test the validity of the Cybersecurity Act, given its stated scope is to .

> 'ensuring the proper functioning of the internal market while aiming to achieve a high level of cybersecurity, cyber resilience and trust within the Union (...) and a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services and ICT processes in the Union, as well as for the purpose of avoiding the fragmentation of the internal market with regard to cybersecurity certification schemes in the Union'. [26]

As the situation exists at the date of this Report, there is a lack of cohesion on the subject between governments, including within the EU, as to whether or not to accept the use of named suppliers products in the domestic 5G network. The Prague Proposals represent an announcement from an *ad hoc* meeting and not, therefore, an official government position. From an EU perspective that is an internal market fragmentation which the Cybersecurity Act is intended to address. In the ordinary course, when the Cybersecurity Act is in full operation, it is plausible to speculate the possibility that one, some or many products *et al.* of named suppliers receive certification. In that speculative scenario, those governments that have decided not to allow named suppliers' products on its domestic 5G network may find the situation going forward difficult to justify. With that possible negative prospect in mind, encouraging stakeholders in the near future to undertake a Cybersecurity Early Certification action could avoid this possible negative.

In light of the above, the following recommendations are made

Recommendation - 1

Encourage a deeper review of the situation

It is proper for all governments to review the situation and to strengthen the review where the subject is important. It is also proper to simplify the actual or proposed measures without negatively affecting the achievement of the underlying policy goal. To achieve this objective a REFIT-like review would allow a comprehensive and transparent review. Speculatively stated, a more focused measure than the blanket prohibition of named suppliers' products from a 5G network might both achieve the desired objectives and mitigate the negative knock-on effects

26. Cybersecurity Act, Article 1(1).

Recommendation - 2

Encourage an antitrust investigation

A competition investigation could be undertaken to determine the consequences of the government measures. This would be a prequel to and might lead to ex-ante actions intended to negate or reduce anticompetitive outcomes foreseen by such analysis.

Recommendation - 3

Encourage using 5G network technologies as a test case in relation to the Cybersecurity Act

A competition investigation could be undertaken to determine the consequences of the government measures. This would be a prequel to and might lead to ex-ante actions intended to negate or reduce anticompetitive outcomes foreseen by such analysis.

EY Law

Annexes

1. Governmental Measures
2. Parts of a 5G Network
3. Competition Key Concepts
4. Competition Practical Assessment
5. Cybersecurity medium measures and the related risks
6. Cybersecurity Potential Implementation Factors
7. Cybersecurity Medium Technical Measures

Annex - 1: Governmental Measures

United States

Negative knock-on effect	Example counter measure
H.R.5515 - John S. McCain National Defense Authorization Act for Fiscal Year 2019. [1]	Section 889 of the FY 2019 NDAA provides for a general ban for the US government on Huawei equipment.
Executive Order 13873 of May 15, 2019 on Securing the Information and Communications Technology and Services Supply Chain.[2] Text of a Notice on the Continuation of the National Emergency on Securing the Information and Communications Technology and Services Supply Chain for one year (until 15 May 2021).[3]	This executive order authorize the Commerce Secretary to prohibit or condition the acquisition, importation, transfer, installation, dealing in, or use by persons subject to U.S. jurisdiction of information and communications technology or services "designed, developed, manufactured, or supplied" by persons owned, controlled or directed by a "foreign adversary" where the Secretary believes there is an "unacceptable risk" to U.S. national security.
Department of Commerce, Bureau of Industry and Security, Addition of Entities to the Entity List, 21 May 2019, Rule 84 FR 22961 Department of Commerce, Bureau of Industry and Security, Addition of Certain Entities to the Entity List and Revision of Entries on the Entity List, 21 August 2019, Rule 84 FR 43493	These decisions bans US suppliers from selling chips made using U.S. technology to Huawei without obtaining a special license from the Department of Commerce.
Department of Commerce, Bureau of Industry and Security, Export Administration Regulations: Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule) and the Entity List, 19 May 2020, Rule 85 FR 29849.[4]	This decision bans non-US suppliers from selling chips made using U.S. technology to Huawei without obtaining a special license from the Department of Commerce.

:1. See https://www.congress.gov/bill/115th-congress/house-bill/5515/text.

2. See https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

3. See https://www.whitehouse.gov/briefings-statements/text-notice-continuation-national-emergency-securing-information-communications-technology-services-supply-chain/

4. See https://www.federalregister.gov/documents/2020/05/19/2020-10856/export-administration-regulations-amendments-to-general-prohibition-three-foreign-produced-direct.

United States

Regulation	Summary
The Clean Network program [5]	On 29 April 2020, Secretary of State Michael R. Pompeo announced the launch of the 'Clean Path', a program where the U.S. Department of State will begin requiring that all 5G network traffic entering and exiting U.S. diplomatic facilities would not use any equipment or services from untrusted vendors such as Huawei. On 5 August 2020, Secretary of State Michael R. Pompeo announced the expansion of the Clean Path to the 'Clean Network' program, to include carriers, app store, apps, cloud services, cable infrastructure.
National Defense Authorization Act for Fiscal Year 2021 (To Be Adopted)	Under the project of FY 2021 NDAA, section 828 recalls Section 889 of FY2019 NDAA and calls for the timely implementation of the government ban on Huawei equipment. Moreover, Section 1046 provides that the Department of Defense would have to take into account security risks of 5G telecommunication networks, including equipment provided by 'at-risks vendors' such as Huawei when deciding where to base US military personnel and activities.

5. See https://www.state.gov/the-clean-network/.

European Union

Regulation	Summary
The EU Cybersecurity Act [6]	The EU Cybersecurity Act establishes an EU-wide cybersecurity certification framework for digital products, services and processes to create tailored and risk-based EU certification schemes. The EU certification schemes will specify: a) the categories of products and services covered; b) the cybersecurity requirements, for example by reference to standards or technical specifications; c) the type of evaluation (e.g. self-assessment or third-party evaluation); and d) the intended level of assurance (e.g. basic, substantial and/or high).
The European Electronic Communications Code [7]	No provisions are directly applicable to network equipment manufacturers. Nevertheless, Member States can imposes various obligations on telecommunication operators, are required to ensure that the integrity and security of public communications networks are maintained and have to ensure that undertakings providing public communications networks or publicly available electronic communications services take technical and organizational measures to appropriately manage the risks posed to security of networks and services.

6. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) OJL 151/15 of 7.6.2019 see https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN.
7. Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) OJ L 321, see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2018.321.01.0036.01.ENG.

   This directive repeals from 31 December 2020:

> Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive) OJ L 108;

> Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services (Authorisation Directive) OJ L 108;

> Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) OJ L 108 ;

> Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) OJ L 108. ;

The provisions referred to in the present document are applicable under the existing and the future framework.

European Union

Regulation	Summary
The European Electronic Communications Code [7]	The framework also provides that competent national regulatory authorities have powers to issue binding instructions and ensure compliance. In addition, under Directive 2002/20/EC10 Member States are allowed to attach to a general authorization conditions concerning the security of public networks against unauthorized access, for the purpose of protecting the confidentiality of communications, in accordance with Directive 2002/58/EC. [8]
EU Toolbox of risk mitigating measures [9]	The EU Toolbox recommends that: ▸ Member States should assess the risk profile of suppliers; as a consequence, apply relevant restrictions for suppliers considered to be high risk - including necessary exclusions to effectively mitigate risks - for key assets defined as critical and sensitive in the EU coordinated risk assessment (e.g. core network functions, network management and orchestration functions, and access network functions); ▸ the European Commission screen potential foreign direct investments (FDIs) affecting 5G key assets and by avoiding distortions in the 5G supply market stemming from potential dumping or subsidies.

8. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201, see https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=celex:32002L0058.
9. See https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

The Prague proposals

Regulation	Summary
Prague Proposals, The Chairman Statement on cyber security of communication networks in a globally digitalized world, Prague 5G Security Conference, 3 May 2019 [10]	The Prague Proposals establishes four categories of proposals to be followed when rolling out 5G networks to ensure the security of the networks. The Prague Proposals present four Policies, six recommendations in the Technology and Economy sector and four classified as Security, Privacy and Resilience propositions:
	Policy: The Prague Proposals recommend that communication network and services should be designed from the onset with resilience and security in mind using international, open, consensus-based standards and risk-informed cybersecurity best practices. To do so, the overall risk of influence on a supplier by a third country should be taken into account, notably in relation to its model of governance, the absence of cooperation, multilateral or international agreements on security, data protection, cybersecurity and crime. The Prague Proposals also call for global interoperable cyber security guidance with transparent and equitable law and policies governing networks and connectivity services while recalling that every country is free to set its own national security and law enforcement requirements.
	Technology: The Prague Proposals call for regular vulnerably assessments and risks mitigation of all components and network systems, taking into account all relevant factors including applicable legal environment and other aspects of supplier's ecosystem, that malicious cyber activities do not always require the exploitation of a technical vulnerability and the technological changes accompanying 5G networks roll out. The Prague Proposals recommend that States adopt policies to enable efficient and secure network data flows and that customer must be able to be informed the origin and pedigree of components and software that affect the security level of the product or service according to state of art and relevant commercial and technical practices.

10. See https://www.vlada.cz/assets/media-centrum/aktualne/PRG_proposals_SP_1.pdf.

The Prague proposals

Regulation	Summary
Prague Proposals, The Chairman Statement on cyber security of communication networks in a globally digitalized world, Prague 5G Security Conference, 3 May 2019 [10]	**Economy** The Prague Proposals put forward the principle of diverse communications equipment market and supply chain as a tool for security and resilience of networks, calls for robust investment in R&D, for the transparency and oversight of the financing and governance of communication network and services and for transparent, fair, reasonable state incentives and subsidies respectful of open competition.
	Security The Prague Proposals call for collective work between stakeholders to promote security and resilience, including by sharing experience and best-practice, for the implementation of risk assessment of vendors and technologies taking into account the rule of law, security environment, vendor malfeasance, and compliance with open, interoperable, secure standards, and industry best practices as well as for the implementation of risk management frameworks that take into account data protection principle and rights to privacy.

15. Catherine Procaccia, *Report on behalf of the Senate Committee on Economic Affairs on the draft law aiming at safeguarding the defense and national security interests of France within the framework of the operation of mobile radio networks*, June 2019, *in French*, see http://www.senat.fr/rap/l18-579/l18-5791.pdf.

Joint-declarations and Memorandum of Understanding

Regulation	Summary
Joint declarations between the United States and: ▸ Poland, 5 September 2019;[11] ▸ Estonia, 1 November 2019;[12] ▸ Latvia, 27 February 2020;[13] ▸ Czech Republic, 6 May 2020;[14] ▸ Slovenia, 13 August 2020. [15] Memorandum of Understanding between the United States and Romania, 20 August 2020.[16]	In those Joint Declarations and Memorandum of Understanding, the United States and, respectively, Poland, Estonia, Latvia, Czech Republic, Slovenia and Romania either endorse or welcome the Prague Proposals and call for an evaluation of suppliers of networks equipment that would include: a) suppliers should not be subject to control by a foreign government without independent judicial review (all countries); b) transparent ownership structures (all countries (all countries); c) record of ethical corporate behavior and is subject to local regime that enforces transparent corporate practices (all countries); d) commitment to innovation and respect for intellectual property rights (US and: Estonia; Czech Republic; and Slovenia); and e) transparent, commercially-based and following standard best practices financing (US and Estonia).

11. See https://www.whitehouse.gov/briefings-statements/u-s-poland-joint-declaration-5g/.
12. See https://www.whitehouse.gov/briefings-statements/united-states-estonia-joint-declaration-5g-security/.
13. See https://www.state.gov/joint-statement-on-united-states-latvia-joint-declaration-on-5g-security/.
14. See https://www.state.gov/joint-statement-on-united-states-czech-republic-joint-declaration-on-5g-security/.
15. See https://www.state.gov/joint-statement-on-united-states-slovenia-joint-declaration-on-5g-security/.
16. See https://www.comunicatii.gov.ro/wp-content/uploads/2019/11/memorandum-5g.pdf.

United Kingdom

Regulation	Summary
NCSC advice on the use of equipment from high risk vendors in UK telecoms networks, published 28 January 2020, Reviewed 14 July 2020.	The NCSC is a non-binding technical advice to operators in respect of their use of equipment from high risk vendors ("HRVs"). The UK Government has announced its intention put this framework into law. The effect of the revised guidelines is that UK telecommunications providers are prohibited from purchasing new Huawei 5G equipment after 31 December 2020; and must remove and replace all existing Huawei 5G equipment from their networks by 2027. Moreover, this framework provides for: ▸ a complete ban on the use of HRVs in certain "core" network functions; ▸ a ban on HRVs equipment near sites that are significant to national security or sensitive networks; ▸ different hard caps on the use of HRVs in FTTP and 5G networks; ▸ for 4G and legacy fixed access networks, two vendors should be used with an approximate 50/50 split between them; ▸ no more than one HRV in any given network; ▸ the use of HRV is only possible with specific risk mitigation strategy.

17. See: https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks.

France

Regulation	Summary
Law No 2019-810 of 1 August 2019 aiming at safeguarding France's defense and national security interests in connection with the operation of mobile radio networks. [18] Decree no. 2019-1300 of 6 December 2019 relating to the terms and conditions for the prior authorization of the operation of radio network equipment provided for in Article L. 34-11 of the French Post and Electronic Communications Code. [19] Order of 6 December 2019 establishing the list of equipment provided for in Article L. 34-11 of the French Post and Electronic Communications Code. [20]	Under this law, the creation or development of any telecommunication infrastructure requires a pre-authorization from the Prime Minister. This authorization can be refused on the basis of a serious risks to defense and national security interest. In particular, the fact that a supplier is under the control of or subject to acts of interference by a State which is not a member of the European Union must be taken into consideration. The refusal can be implicit and/or do not need to be motivated if the communication of the motivation would jeopardize defense and national security interest.

18. See https://www.legifrance.gouv.fr/eli/loi/2019/8/1/ECOX1907688L/jo/texte.

19. See https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=EDDF5E9E052F4EF0DC1752714C233407.tplgfr27s_2?cidTexte=JORFTEXT000039455649&dateTexte=20191207

20. See https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=EDDF5E9E052F4EF0DC1752714C233407.tplgfr27s_2?cidTexte=JORFTEXT000039455672&dateTexte=20191207

Poland

Regulation	Summary
Draft act amending the act on the national cybersecurity system and the act - Public Procurement Law published on September 2020.	This draft law introduces provisions closes to those provided for in the EU Cybersecurity Act and is also largely inspired by the Prague Proposals. In addition, under this draft law, the Cyber Security College would be empowered to assess the risk of a supplier on the basis of the threats and vulnerabilities to national security as well as regarding Poland's international, and European and allied obligations. The assessment should take into consideration: a) the likelihood the supplier is under the influence of a non-EU or a non-NATO country; b) the legislation of that country regarding civil and human rights and regarding the protection of personal data; c) the capacity of influence of that country on the supplier; d) the ownership of the supplier; e) the degree of supervision of the supplier on the products and risks of delivery. The consequences of that risk assessment can go from the mandatory modification to the product to the complete exclusion and removal of the products from Poland's networks.

21. See https://legislacja.gov.pl/projekt/12337950/katalog/12716608#12716608.

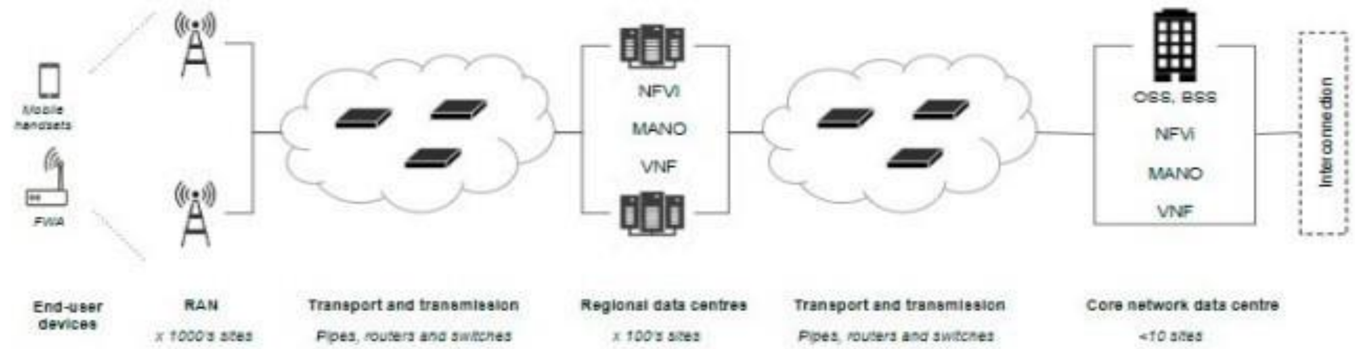
Romania

Regulation	Summary
Draft Law on the adoption of measures relating to information and communication infrastructures of national interest and the conditions for the implementation of 5G networks published in August 2020.[22]	Under this draft law, the use of technologies, equipment and software in information and communication infrastructures of national interest and 5G networks would require a pre-authorization from the Prime Minister. This authorization would be given on the basis of the assent by the Supreme Council of National Defense (CSAT). The approval should be based on the assessments of risks, threats and vulnerabilities to national security and/or national defense as well as international obligations of Romania within international organizations and for strategic bilateral partnerships and should take into account: a) the control of a supplier by a foreign government; b) the absence of a transparent shareholding structure of a supplier; c) a history of absence of ethical corporate conduct; d) the absence of mandatory transparent corporate practice by the supplier's legal system.

22. See http://www.mt.ro/web14/transparenta-decizionala/consultare-publica/acte-normative-in-avizare/3059-l04082020dcom.

Annex -2: Parts of a 5G Network

Figure 2: Parts of a 5G network



Glossary:

NFVI Network Function Virtualisation infrastructure; **MANO** Management & Network Orchestration; **VNF** Virtual Network Function; **OSS** operational support systems; **BSS** business support systems

- **Mobile Core.** The core includes critical functionality, e.g. user authentication and call routing. The functions within the core network are increasingly moving to software-based architecture (as discussed later in this section).
- **Radio Access Network.** The radio access network (RAN) connects customer devices (e.g. handsets) and mobile phone masts using radio spectrum.
- **Transport and Transmission.** These functions aggregate traffic from the mast sites and carry it to the core network. The transmission layer includes the 'pipes' and the transport layer comprises switches and routers that direct traffic.
- **Interconnect.** Mobile operators connect to the wider internet via Internet Exchanges. These are large data centres into which ISPs and major tech companies (e.g. Netflix, Amazon and Google) have high speed connectivity and connect to each other via switches and routers operated by the internet exchange.
- **Operational and Business Support Systems.** These are intelligent software that are critical for managing service provisioning, billing, customer services, and monitoring network performance. As with the core, these applications are increasingly being deployed as software-based virtualised functions.

Department for Digital, Culture, Media & Sport, UK Telecoms Supply Chain Review Report, Page 17, July 2019, see https://assetsCCS0719559014-001.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819469/CCS001__Telecoms_Security_and_Resilience_Accessible.pdf.

Annex -3: Competition Key Concepts

Third party findings	Preliminary conclusions
"In Nokia/Alcatel-Lucent, Ericsson/Nortel Group, and Nokia Siemens Networks/Motorola Network Business, the Commission distinguished between (i) RAN equipment, (ii) Core Network Systems ("CNS") and (iii) network-related services". *ERICSSON/KATHREIN ANTENNA AND FILTER ASSETS, §12* [1]	**Relevant product market** On the mobile telecommunication equipment, three markets can be distinguished: Core Network Systems ("CNS"), "Radio Access Network" ("RAN") and network-related services.
"The Commission considers that the RAN equipment market may be segmented by technology standards and/or between macro-cells and small-cells equipment. Moreover, it cannot be excluded that SRAN equipment may constitute a separate market segment." *NOKIA/ALCATEL-LUCENT, §24* [2]	**Relevant product market** The RAN equipment market should be sub-divided by: ▶ Generation: 2-2.5G, 3G, 4G and 5G; and ▶ Technology: macro-cells and small-cells.
"Since Nokia/Siemens the industry has transitioned to the newer 4G technology, whose network functionalities revolve around an Evolved Packet Core, which no longer distinguishes between circuit-core and packet-core, but treats all voice and data as packets. The Commission has not yet analysed the exact scope of the relevant product market/s in relation to either Evolved Packet Core equipment or Carrier IP telephony products." "In any event, for the purpose of this decision, the Commission considers that the exact product market definition, and in particular whether a distinction should be made between (i) wireless packet core, including a possible segmentation into Traditional Packet Core and Evolved Packet	**Relevant product market** The relevant product market for CNS may be subdivided between: ▶ Wireless packet core; ▶ Carrier IP telephony products that may be further divided between Softswitch products, Media Gateway products, SBC, VAS, IMS Core; ▶ OSS/BSS that may be further divided between decentralized and centralized SON solutions. However, with each generation, new subdivision of the CNS market may be relevant.

1. ERICSSON/KATHREIN ANTENNA AND FILTER ASSETS (Case No COMP/M. 9332) Commission Decision C(2019) 6196 final [2019] OJ C 56/1, see https://ec.europa.eu/competition/mergers/cases/decisions/m9332_422_4.pdf.

2. NOKIA/ALCATEL-LUCENT (Case No COMP/M.7632) Commission Decision C(2015) 5315 final [2015] OJ C 329/1, see https://ec.europa.eu/competition/mergers/cases/decisions/m7632_788_2.pdf.

Third party findings	Preliminary conclusions
Core and Evolved Packet Core and a further sub-segmentation of these two products into SGSN and GGSN and into MME and PGW respectively; (ii) Carrier IP telephony products, including a possible segmentation of these products into Softswitch products (and their further segmentation into wireless and wireline), Media Gateway products (and their further segmentation into wireless and wireline), SBC, VAS, IMS Core (including further segmentation into CSCF and HSS); and (iii) OSS/BSS including whether decentralised and centralized SON solutions constitute separate markets or market segments, can be left open" *NOKIA/ALCATEL-LUCENT, §50, 59*	
"RAN equipment establishes a connection between individual mobile devices and the core network through radio connections. Notable components of the RAN equipment are antennas, filters, radio units, baseband, and cabling. Ericsson manufactures baseband and radio units which are the key components of the RAN equipment that it supplies to mobile network operators." "The results of the market investigation indicate that passive antennas, antenna modules and filters should be considered to belong to markets distinct from the market for other RAN equipment components and that the same finding may potentially apply to active antennas." "The Commission concludes that passive antennas belong to a separate product market distinct from other RAN equipment components. In addition, the Commission concludes that passive and active antennas belong to separate product markets.	**Relevant product market** The RAN equipment market can at least be divided between: ▸ RAN components, ▸ Passive antennas; ▸ Active antennas; ▸ Antenna modules, ▸ Filters.

Annex -3: Competition Key Concepts

Third party findings	Preliminary conclusions
The question whether passive antennas and antenna modules as well as single-band and multi-band antennas belong to distinct product markets can be left open. Likewise, the question whether the potential product market for active antennas would have to be segmented between semi-active and AAS active antennas and whether antenna modules used for semi-active antennas and AAS antennas belong to distinct product markets can be left open." "Therefore, the Commission concludes that filters constitute a separate product market distinct from other RAN equipment components." *ERICSSON/KATHREIN ANTENNA AND FILTER ASSETS, §10, 23, §75-76, 88*	
"The Notifying Party submits that the relevant geographic market for mobile network equipment, including RAN, is global in scope due to several factors including: (i) international standardization of mobile telecommunications network equipment; (ii) vendor and industry interoperability initiatives through Interoperability Testing Centers ("IOTs"); (iii) contracts that are competed on a global basis – there is no longer a concept of 'home' market or region; (iv) worldwide shipping and limited transport costs; (v) limited regional variations in cost and price; and (vi) liberalized downstream service markets leading to open upstream equipment markets." "(…) The majority of competitors who replied to the market investigation confirm that they are active in the supply of RAN equipment worldwide. There are, however, certain regions of the world where some vendors do not actively compete:	**Relevant geographic market** The relevant geographic market for the different mobile network equipment is traditionally understood as "global". However, with increasing regulation and legal requirements and the exclusion of certain competitors from some markets, it might be possible that the structure of the markets change substantially and that those markets may be geographically divided according to the exclusion of certain competitors.

Annex -3: Competition Key Concepts

Third party findings	Preliminary conclusions
Chinese vendors, despite their global presence, are not active in the United States, given the latter's security concerns. As regards prices, the majority of competitors also state that their prices are not homogeneous worldwide due to the different requirements of mobile operators. As regards technology, half of the competitors state that the technology and standards are global and that, as products are developed supporting telecommunication standards, no difference among regions exists. The other half of the competitors, however, considers that differences in terms of technological development exist between regions. In particular, one competitor submits, that although the products are based on global telecommunication standards, customers have very specific requirements for the products to be included in their networks. The large majority of competitors also confirm the existence of differences in terms of applicable regulation and legal requirements between the EEA and other regions of the world (for example US operators require security certificates)." *NOKIA/ALCATEL-LUCENT, §26, 32-34.*	
"A majority of respondents to the market investigation indicate that they supply and/or procure RAN equipment on a global basis, with the main RAN equipment suppliers based in Europe, USA and Asia." ERICSSON/KATHREIN ANTENNA AND FILTER ASSETS, §28	**The relevant geographic market** The relevant geographic market for the different mobile network equipment is traditionally understood as "global".

Annex -3: Competition Key Concepts

Third party findings	Preliminary conclusions
"The global telecoms equipment market for network operators is dominated by three global players – Huawei, Ericsson and Nokia. Other players include Samsung, CISCO, Juniper, Ciena and ZTE – however, their participation varies across different parts of the network." *UK Telecoms Supply Chain Review Report, page 29* [3]	**Market structure** Market for telecoms equipment for network operators is concentrated
"Increased consolidation is consistent with a market which is characterised by high levels of R&D investment, economies of scale, buyer power and intense competition keeping prices (and therefore profits) low. (...) These factors suggest that the current market conditions are not particularly favourable to new entrants. New entry entails significant long term commitments in terms of time and R&D investments, and recovery of costs is not immediate. However, technology developments associated with 5G (e.g software-defined networks – see Section 2) may create greater opportunities for market entry and diversification over time. There is also the scope for policy interventions to support this trend (see Section 5)." *UK Telecoms Supply Chain Review Report, page 32.*	**Market structure** The concentrated structure of the market is consistent with the high barriers to entry. If developments associated with 5G technology may ease market entry over time, backward compatibility and legacy advantage (see below) will limit this new entry on the short term

3. Department for Digital, Culture, Media & Sport, UK Telecoms Supply Chain Review Report, July 2019, see https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819469/CCS001_CCS0719559014-001_Telecoms_Security_and_Resilience_Accessible.pdf.

Annex -3: Competition Key Concepts

Third party findings	Preliminary conclusions
"In the race to 5G contracts for equipment manufacturers, it is difficult to say who is really winning so far because of not all the figures being released and made public. Ericsson for instance states that it currently has 78 5G commercial agreements or contracts with unique operators out of which 31 have been publicly announced and out of which 24 are live 5G networks. While the American ban on Huawei has been seen as an opportunity for its competitors it has not prevented the Chinese infrastructure vendor to claim the leadership in the past but this is something that is difficult to follow over the time. Recently, Huawei claimed at last 60 5G contract of which with 28 European operators. As for Nokia, it secured 50 commercial contracts for 5G at the end of October, making it potentially the last of the 3 equipment vendor in the 5G race. But figures do not tell the whole story. Behind the figure, indeed, Nokia has claimed in the past to be leading in terms of the comprehensiveness of the 5G solution sold to operator. In an article to Fiercewireless, Sandro Tavares, Nokia's head of global mobile networks marketing said that "More than half of the deals that we have signed actually include more than just radio". It should be noted here also that most of the MNOs usually contract with several network vendors." *IDATE Digiworld report produced for the European Commission, 5G Observatory Quarterly Report 8, up to June 2020, page 67.* [4]	**Market structure** This supports the other evidence of a concentrated market with three top-tier companies.

4. IDATE Digiworld report produced for the European Commission, 5G Observatory Quarterly Report 8 Up to June 2020, July 2020, see http://5gobservatory.eu/wp-content/uploads/2020/07/90013-5G-Observatory-Quarterly-report-8_1507.pdf.

Annex -3: Competition Key Concepts

Third party findings	Preliminary conclusions
"Passive antennas and other RAN equipment components are generally manufactured by a different set of suppliers, with the exception of Huawei which produces both passive antennas (as well as antenna modules) and other RAN equipment components." "Passive antennas are produced by dedicated antenna manufacturers and supplied to MNOs on a standalone basis or as part of a turnkey solution. The only exception is Huawei which has end-to-end in-house capabilities. By contrast, active antennas are manufactured by RAN equipment suppliers and antenna manufacturers only supply the antenna module as they generally lack radio capabilities. MNOs procure active antennas as integrated solutions only from RAN equipment suppliers." *ERICSSON/KATHREIN ANTENNA AND FILTER ASSETS, §50, §72. See also §50, 100-136, 152, 159, 161, 163, 164-166, 174, 178, 186, 208, 210, 239, 243.*	**Market power** On the RAN equipment markets, most components are manufactured by a different set of suppliers. Huawei is an exception, being the only player with end-to-end in-house capabilities. Huawei acts as an independent supplier on certain occasion and markets. Huawei is listed on each RAN equipment markets as a top-tier player with large market shares.
"...by early 2019, Huawei led the world with 1,529 of these "standards essential patents" for 5G technology." *Cyberspace Solarium Commission report, page 18* [5]	**Market power** The implication is that this level of SEPs means Huawei has a high level of market power.
"...Huawei spends the most in absolute terms on R&D but has mostly been the lowest spender across the three main vendors as a proportion of sales." *UK Telecoms Supply Chain Review Report, page 31*	**Market power** The suggests that (i) Huawei is the first worldwide investor in R&D and that (ii) Huawei has larger sales than its main competitors (Ericsson & Nokia).

5. Cyberspace Solarium Commission, Report, 11 March 2020, see https://www.solarium.gov/#h.p_rK7mL_1MeZw7.

Annex -3: Competition Key Concepts

Third party findings	Preliminary conclusions
"Network equipment providers are global players, and operators make purchasing decisions in global collaborations. For example, Telenor / Telefonica make purchases together across a number of counties. In 2019 single country has limited impact on infrastructure prices. (...) Mobile operators have exerted tremendous pressure on network suppliers by holding back on their purchases. European mobile operators spent €110 billion for frequencies in the 3G auctions around year 2000. However, their business models to monetize the spectrum by increasing subscriber fees did not pan out. Many mobile operators folded or were acquired." *Understanding the Market for 4G RAN in Europe: Share of Chinese and Non-Chinese Vendors in 102 Mobile Networks – Version 1.2, pages 10-11* [6]	**Market power** This suggests that telecom operators hold significant buyer power that seems capable of countervailing the market power of the top-tier suppliers of network equipment.
"European cybersecurity certification scheme' means a comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific ICT products, ICT services or ICT processes." *Cybersecurity Act, Article 2(9)* [7]	Barriers to entry The EU cybersecurity certification scheme will likely raise the regulatory bar for telecommunication products and services, at least through a conformity cost.

6. StrandConsult, Understanding the Market for 4G RAN in Europe: Share of Chinese and Non-Chinese Vendors in 102 Mobile Networks - Version 1.2, 2020.

7. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) OJL 151/15 of 7.6.2019 see https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN.

Annex -3: Competition Key Concepts

Third party findings	Preliminary conclusions
"(…) 5G networks can be deployed in two ways: standalone (SA) and non-standalone (NSA). (…) NSA deployments will be the first phase of 5G in the UK over the next few years and will rely on existing 4G infrastructure. For NSA deployments, 5G network equipment will need to be compatible with legacy network (i.e. 3G/4G) equipment. For this reason, UK operators will tend to use their current 4G vendors for 5G rollout." "Switching costs. In mobile and fixed access, switching costs are high once the equipment of a particular vendor is deployed in the network. This is most notable in the mobile access network, where switching may involve replacing costly legacy equipment, due to the non-standalone nature of 5G deployment in the next few years" *UK Telecoms Supply Chain Review Report, page 18 & 32*	**Barriers to entry** The requirement for backward compatibility between 5G and 4G equipment increase the cost for new players to enter the market as choosing new suppliers for 5G equipment means that 4G equipment needs to be replaced.
"This compatibility with past infrastructure investments is very important for telecom operators – in Europe as well as in other world regions – it is essential that 5G deployment follows an evolutionary approach. Such an approach will allow for a gradual shift of infrastructure from 4G to 5G, thus allowing appropriate returns of investment from 4G deployments and upgrades but also to address operational considerations: deploying equipment over a large territory takes time and starting from a zero footprint might decrease the appeal of 5G, especially for some vertical industries that need a wider coverage in rural areas or indoor." *5G empowering vertical industries White Paper, page 9* [8]	**Barriers to entry** This is consistent with other analysis on the importance of backward compatibility and legacy cost.

8. 5GPPP, 5G empowering vertical industries White Paper, 2016, see https://5g-ppp.eu/wp-content/uploads/2016/02/BROCHURE_5PPP_BAT2_PL.pdf.

Annex -3: Competition Key Concepts

Third party findings	Preliminary conclusions
"R&D investment is a key barrier to entry. The high levels of R&D and time taken to develop technically capable products act as a barrier to entry and expansion. There is intense competition across vendors and R&D plays a significant role." *UK Telecoms Supply Chain Review Report, page 31*	**Barriers to entry** 5G equipment requires high level of R&D and time to develop which is a significant barrier to entry and limits the ability of new competitors to enter the market in a timely manner.
"Economies of scale. High R&D requirements mean that vendors need to undertake significant investments, some of which involve fixed and irrecoverable costs. In such markets, economies of scale can drive firms to chase volumes in order to reduce average costs and offer lower prices than smaller rivals. The investment risks involved can act as a barrier to the entry and expansion for smaller players." *UK Telecoms Supply Chain Review Report, page 31*	**Barriers to entry** The high level of investments limits the ability of new player to enter and compete on the markets in a timely manner.

Annex -4: Competition Practical Assessment

Third party findings	Preliminary conclusions
"…in upcoming 5G networks, mobile data traffic entering American diplomatic systems will be subject to new, stringent requirements if it has transited Huawei equipment. The objective is that untrusted IT vendors will have no access to U.S. State Department systems." *United States' Secretary of State Michael R. Pompeo, announcement, 29 April 2020* [1]	**Existing firms** The quantum effect of this announcement is unclear, but presumably limited in the sense that diplomatic systems constitute a small part of the total US government and private telco network. As such the other major players can expect a small increase in business, but otherwise no material impact. A broader impact is expected to occur following implementation of sec.828 NDAA for FY 2021, which would prevent all Federal agencies from contracting with Huawei, pursuant to a determination by Congress under sec.899 NDAA for FY2019. The effect of the broader Clean Network Program announced by the White House is not capable of determination given there are no details and questions as to its legality.
"By the time of the next election, we will have implemented in law an irreversible path for the complete removal of Huawei equipment from our 5G networks." *UK Digital Secretary Oliver Dowden, statement to the House of Commons, 14 July 2020* [2]	**Existing firms** By May 2024 the impact of the measure is expected to be irreversible.[3] This can be expected to be taken into account by the two remaining major players in terms of their strategy and actions on the market.

1. United States' Secretary of State Michael R. Pompeo, announcement, 29 April 2020, See https://www.state.gov/secretary-michael-r-pompeo-at-a-press-availability-4/. Legal basis for the announced action is the National Défense Authorization Act for Fiscal Year 2020 (the '2019 NDAA') – no official final text is currently publicly available on-line – that requires a strategy for secure 5G networks for the Department of defense (and by implication all of U.S. government) – commonly referred to as the 5G Clean Path strategy – and part of a broader White House strategy announced on 5 August 2020 referred to as the Clean Network Program, see https://www.state.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets/.

2. UK Digital Secretary Oliver Dowden, statement to the House of Commons, 14 July 2020, See https://www.gov.uk/government/speeches/digital-culture-media-and-sport-secretarys-statement-on-telecoms.

3. This appears inconsistent with a general test of whether or not an entity should have its products removed from the network, as enunciated, for example, by the UK's NCSC and as also appears from the Prague Proposals. The statement on its face means there is nothing Huawei could do to change its classification as an HRV.

Annex -4: Competition Practical Assessment

Third party findings	Preliminary conclusions
"In order to minimise the additional cyber security risk caused by HRVs, NCSC believe it is necessary and proportionate to limit their presence in networks. This has been NCSC's consistent advice to operators (when they have sought our guidance) and is most operators' existing common practice." *NCSC advice on the use of equipment from high risk vendors in UK telecoms networks, para. 11.*[4]	**Existing firms** Either HRV was not sufficiently robust or Telco operators nevertheless found Huawei price/quality offering very attractive.
"Huawei has always been considered higher risk by the UK government and a risk mitigation strategy has been in place since they first began to supply the UK." *NCSC advice on the use of equipment from high risk vendors in UK telecoms networks, para. 13.*	**Existing firms** Given the government recognized data that Huawei holds a market share of the mobile access market of approximately one third, this suggests the measures had limited effect. Other firms' existing competition (market) strategy likely includes the fact that Huawei is already restricted due to security reasons.
"Any use of an HRV in other 5G or FTTP network functions should be limited and we consider that a hard cap of 35% of a network equipment type allows for effective cyber security risk management. This cap properly balances two different security and resilience risks; the first being the risk associated with HRVs, the second being the need for a diversity of supply in the market." *NCSC advice on the use of equipment from high risk vendors in UK telecoms networks, para. 11(b).*	**Existing firms** An HRV can provide up to 35% of certain aspects of 5G and Fibre to the Premises (FTTP) network. This partially open door rather than total exclusion is recognition of the need for diversity of supply in the market. This bifurcation might affect market definition given that some market players are not able to compete in certain activities.

4. UK's National Cyber Security Centre (NCSC), NCSC advice on the use of equipment from high risk vendors in UK telecoms networks, 30 August 2020 (updated), see https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks.

Annex -4: Competition Practical Assessment

Third party findings	Preliminary conclusions
"For 4G and legacy fixed access networks, the NCSC's advice to operators remains unchanged. Two vendors should always be used in the access network. While no specific volume cap has been recommended, the NCSC has always expected approximately 50/50 split between vendors in a given network." *NCSC advice on the use of equipment from high risk vendors in UK telecoms networks, para. 11(c)*	**Existing firms** Implication is that competition in the market may decrease as established players reach their nominal 50% share of a network, which may result in higher prices as incumbent's become less keen to compete for the final market tranche.
"These factors suggest that the current market conditions are not particularly favourable to new entrants. New entry entails significant long term commitments in terms of time and R&D investments, and recovery of costs is not immediate. However, technology developments associated with 5G (e.g software-defined networks – see Section 2) may create greater opportunities for market entry and diversification over time. There is also the scope for policy interventions to support this trend" *UK Telecoms Supply Chain Review Report, page 32* [5]	**Existing firms** It is not certain nor even likely that new entrants will replace excluded suppliers without supportive government intervention. On the assumption that any new entrants would not occur in the short term, this suggests the two other major players will increase their market share.
"Operators should never use more than one HRV in any given network; the NCSC believes it is not possible to perform effective cyber security risk management where two HRVs are present in a network." *NCSC advice on the use of equipment from high risk vendors in UK telecoms networks, para. 11(d)*	**Existing firms** Implication is that competition in the market may become (i) asymmetric, which some players active in all markets, while others are active in only some markets, leading potentially to cross-price subsidization by participants in their tendering strategies, and/or (ii) lock-in whereby once an HRV's products are used by a network operator for a network, that HRV might always consistently be able to reach the 35% threshold if it is naturally providing lower-priced/better products.

5. Department for Digital, Culture, Media & Sport, UK Telecoms Supply Chain Review Report, July 2019, see https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819469/CCS001_CCS071 9559014-001_Telecoms_Security_and_Resilience_Accessible.pdf

Annex -4: Competition Practical Assessment

Third party findings	Preliminary conclusions
"On the 15th May 2020, the US placed an additional sanction on Huawei. These are such that Huawei is very unlikely to be able to continue to use US technology and software in the design and production of its products. We believe that will force significant changes to the products that Huawei supply into the UK, which will make oversight of the products significantly more challenging, and potentially impossible. In addition to the products themselves, HCSEC will also now need to analyse these new tools, which are totally unknown to us and which will need to be created without access to the established technology used today." *NCSC advice on the use of equipment from high risk vendors in UK telecoms networks, para. 16.*	**Entry of new firms** Combined with statements concerning the new for interoperability and standards, there is the implication that many new entrants risk being marginalized or even facing being qualified as an HRV if their technology is novel and not substantially based on existing US technology.
"Initially pushed by MNOs to end their dependency on one or two single equipment provider it [Radio Access Network] has been seen as an opportunity for new players to enter the RAN market with software solution while traditional equipment suppliers other than Huawei have been forced to more or less timidly support the movement to continue working with some Tier 1 mobile operators." *5G Observatory Quarterly Report 8, up to June 2020, page 64 .*[6]	**Entry of new firms** Measure will have no direct impact in relation to new technologies, such as RAN, which is creating new vendors (e.g. Altiostar, Mavenir, JMA, Parallel Wireless, Acelleran, Airspan, Radisys) that will continue to progress on the market.

6. IDATE Digiworld report produced for the European Commission, 5G Observatory Quarterly Report 8 Up to June 2020, July 2020, see http://5gobservatory.eu/wp-content/uploads/2020/07/90013-5G-Observatory-Quarterly-report-8_1507.pdf.

EY Law

Annex -4: Competition Practical Assessment

Third party findings	Preliminary conclusions
"The overall risk of influence on a supplier by a third country should be taken into account, notably in relation to its model of governance, the absence of cooperation agreements on security, or similar arrangements, such as adequacy decisions, as regards data protection, or whether this country is a party to multilateral, international or bilateral agreements on cybersecurity, the fight against cybercrime, or data protection." *The Prague Proposals, page 3* [7]	**Entry of new firms** The implication is that new entrants will need to satisfy criteria, some of which they can address (endogenous criteria) and some which can only be addressed by the country where they are based (exogenous criteria). As a general statement, this raises regulatory barriers to entry.
"The Rapporteur recalls, however, that Huawei is not the only one equipment manufacturer on which suspicions may arise as to the nature of its links with a foreign State. It has been publicly established - contrary to what has happened so far in Huawei - that the United States has voluntarily implanted "back doors" in the equipment of the American company Cisco so that its intelligence services could undermine the secrecy of correspondence, as revealed by the "Snowden affair". Similarly, the US authorities can rely on the Cloud Act, which allows law enforcement agencies to compel US service providers to provide data stored on servers, which are located in the United States or in foreign countries." *Report on behalf of the Senate Committee on Economic Affairs on the draft law aiming at safeguarding the defense and national security interests of France within the framework of the operation of mobile radio networks, Page 21* [8]	**Entry of new firms** Any non-EU firm wishing to enter the market would be submitted to the same approval process. [9] This report suggests that US companies would or should be subject to the same regime than Huawei. This will further limit the access to the market of new entrants.

7. Prague 5G Security Conference, The Prague Proposals, The Chairman Statement on cyber security of communication networks in a globally digitalised world, 3 May 2019 see https://www.vlada.cz/assets/media-centrum/aktualne/PRG_proposals_SP_1.pdf.
8. Catherine Procaccia, Report on behalf of the Senate Committee on Economic Affairs on the draft law aiming at safeguarding the defense and national security interests of France within the framework of the operation of mobile radio networks, June 2019, in French, see http://www.senat.fr/rap/l18-579/l18-5791.pdf.
9. Law No 2019-810 of 1 August 2019 aiming at safeguarding France's defense and national security interests in connection with the operation of mobile radio networks, see https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=EDDF5E9E052F4EF0DC1752714C233407.tplgfr27s_2?cidTexte=JORFTEXT000039455672&dateTexte=20191207

Annex -4: Competition Practical Assessment

Third party findings	Preliminary conclusions
"…the Government will develop a targeted diversification strategy, supporting the growth of players in those parts of the network that pose security and resilience risks. The strategy will support industrial strategy policies to incentivise entry and growth, including market design and R&D support; promoting interoperability and demand stimulation; and attracting established players to the UK market. It will also be underpinned by wider policies set out in the Future Telecoms Infrastructure Review (FTIR). The Government is willing to discuss opportunities for market diversification with like-minded countries." *UK Telecoms Supply Chain Review Report, page 41*	**Entry of new firms** Implication is that the greater concentration likely to be created by the limitation or removal of a network equipment supplier will have to be counterbalanced by government action to encourage new entrants.
"Greater interoperability and more open interfaces will be required to facilitate new entrants. It is not sufficient that interoperability is included in technical standards" *UK Telecoms Supply Chain Review Report, page 41*	**Entry of new firms** A significant technical element (standard) needs to be created, something that might have been desirable in any event but probably becomes a priority as a result of the government measure.
"Impose additional controls on the presence of certain types of vendors which pose significantly greater security and resilience risks to UK telecoms. In considering what those controls should be, it is necessary to address the identified security risks, whilst seeking to minimise the costs to industry and the wider economy" *UK Telecoms Supply Chain Review Report, page 39*	**Prices** The implication is that the government measure will raise costs for network operators, presumably because (a) network equipment costs will rise due to fewer meaningful equipment suppliers and (b) higher security standards will raise the costs for equipment suppliers who in turn will pass-on those costs through higher prices.

Annex - 4: Competition Practical Assessment

Third party findings	Preliminary conclusions
"In this context, the A.R.C.E.P. stresses that, in a number of cases, a refusal of authorization could lead directly or indirectly to the withdrawal of equipment already deployed. This is typically the case when operators have chosen to operate only equipment from the same equipment manufacturer on each site. If, for example, an operator has chosen to operate 2G, 3G and 4G equipment from manufacturer A on a given site, a refusal to grant an operating license for 5G equipment from manufacturer A on that site could lead the operator to completely replace the 2G, 3G and 4G equipment already deployed (or alternatively could impose significant additional costs on it to be able to operate equipment from different manufacturers on the same site). *ARCEP, Opinion No 2019-0161, Section 2.3*[10]	**Prices** The exclusion of named suppliers for 5G equipment would lead to significant price increase to either make 5G equipment of other manufacturer interoperable with pre-existing named suppliers' equipment or to replace the pre-existing named suppliers' equipment. This will also lead to limit the ability of operator to develop the 5G infrastructure and could lead to put pressure on the other manufacturers for the supply of equipment for 2G, 3G and 4G.
"To reflect the uncertainty inherent in such a process, we modelled three alternative scenarios termed "low cost", "central cost", and "high cost". All give results relative to our (post-coronavirus) baseline scenario, in which no competition restrictions are imposed on the 5G infrastructure market. Under the central cost scenario, our modelling suggests that restricting a key supplier of 5G infrastructure in our 31 European countries would increase total 5G investment costs by almost €3 billion per year on average over the next decade, in 2020 prices. This represents an annual cost increase of 19%, which translates to €3 million per year in Iceland but as much as €479 million per year in Germany.	**Prices** This study evaluates a significant price increase of 5G infrastructure as a consequences of Huawei eviction from the market.

10. ARCEP, Opinion no. 2019-0161 of the Autorité de régulation des communications électroniques et des postes (French regulatory authority for electronic communications and postal services) on a draft text aimed at introducing a system of prior authorization for the operation of radio network equipment, 4 February 2019, in French, see https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000039792749&categorieLien=id.

Third party findings	Preliminary conclusions
(...) Increase in average annual investment costs for 5G infrastructure over the next decade: Low cost scenario €1.4 billion (9%); Central Cost scenario €3.0 billion (19%); High cost scenario €4.5 billion (29%). (...) When interpreting these results, it is important to note that we have not made allowance for costs that network operators would face if they were to need to replace existing equipment built by the restricted provider. Such additional costs would further delay rollout and technological innovation resulting in higher productivity losses." *Restricting competition in 5G network equipment throughout Europe, An Economic Impact Study, page 3* [11]	
"To evaluate the impact of restricting Huawei equipment from networks, one must include the fact that operators must upgrade their networks if they want 5G, regardless of whether they use Huawei. That is to say that there is a sunk cost to network upgrades which must be subtracted from the total cost of using Huawei and ZTE. Most of Europe's networks are already 3-10 years old and are ready to be replaced. In any case, 70–80 percent of the existing RAN equipment must be replaced, regardless of the political decision or the choice of 5G vendor." *Understanding the Market for 4G RAN in Europe: Share of Chinese and Non-Chinese Vendors in 102 Mobile Networks – Version 1.2, page 24* [12]	**Prices** This suggest that the cost of replacing existing Huawei equipment might not be as severe as suggested above considering that Telecommunication Operators would still have to replace existing equipment under normal circumstances.

11. Oxford Economics, Restricting competition in 5G network equipment throughout Europe, An Economic Impact Study, June 2020, see https://www.oxfordeconomics.com/recent-releases/51856cd0-46d6-409c-bcab-218875f6b510.
12. StrandConsult, Understanding the Market for 4G RAN in Europe: Share of Chinese and Non-Chinese Vendors in 102 Mobile Networks - Version 1.2, 2020.

Annex - 4: Competition Practical Assessment

Third party findings	Preliminary conclusions
"Customer - whether the government, operator, or manufacturer - must be able to be informed about the origin and pedigree of components and software that affect the security level of the product or service, according to state of art and relevant commercial and technical practices, including transparency of maintenance, updates, and remediation of the products and service." *The Prague Proposals, page 4*	**Non-price elements** Implication is that an open and transparent 'test' could be created which if passed would allow a supplier to become a market player. This is an example of the steep increase regulation of the markets.
"The associated restriction in competition for 5G infrastructure would lead to delays in the network rollout. Under the central cost scenario, we estimate that around 56 million fewer people across Europe would be covered by the 5G network in 2023. (...) Absolute number of people who will delayed access to 5G by 2023: Low cost scenario 29 million (6%); Central Cost scenario 56 million (11%); High cost scenario 78 million (15%)." *Restricting competition in 5G network equipment throughout Europe, An Economic Impact Study, page 3*	**Non-price elements** This study suggests that the exclusion of Huawei of the market would significantly increase the delay to develop a 5G infrastructure in Europe.
"Communication networks and network services should be financed openly and transparently using standard best practices in procurement, investment, and contracting. "State-sponsored incentives, subsidies, or financing of 5G communication networks and service providers should respect principles of fairness, be commercially reasonable, conducted openly and transparently, based on open market competitive principles, while taking into account trade obligations." *The Prague Proposals, page 4*	**Markets generally** The implication is there is a risk government measures might create a directed/managed outcome rather than a competitive outcome so norms should be observed by government to avoid 'balkanization' of the markets.

Annex - 4: Competition Practical Assessment

Third party findings	Preliminary conclusions
"If Qualcomm, Huawei and Samsung are the top three 5G baseband players, two other vendors (excluding Intel that dropped the 5G baseband market) have announced 5G solutions, Mediatek and UniSoC. Mediatek, after announcing the Helio M70 back in June 2018 announced its integrated 5G SoC in May 2019 and has seen its first OEM commercial product launched at the end of December 2019 with the Oppo Reno 3 that is now sold in China. With this mid-end solution, Mediatek is well geared too to increase its position in the 5G device market and it also announced its lower tier 5G solution at CES in January 2020 with first commercial devices with this solution to be launched during the 1st half of 2020 (but that may very well slip in H2 due to COVID-19 epidemic)." *5G Observatory Quarterly Report 8, up to June 2020, page 56*	**Baseband chip manufacturers** Measure will have no direct impact as the measures are not affecting baseband chip production. However, the US trade sanction as regards the in practice prohibition of US-technology to Huawei will likely have an impact. It seems from commentators that this would be further impacted if the UK based chip producer ARM is acquired by the US based chip producer Nvidia. [13]
"As an indication of 5G smartphone ecosystem evolution, while the average selling price of 5G smartphone was around 650 EUR in China in 2019, low-end 5G smartphone around 130 EUR could see the light of the day by the end of 2020 according to Huawei." *5G Observatory Quarterly Report 8, up to June 2020, page 57*	**Smartphone market** The government measures are not currently directly targeting the smartphone market. However, the most recent US measure[14] may limit the ability of Huawei to compete efficiently on the smartphone market where Huawei is recognized as a technological leader.
"This time, with 5G, Fixed Wireless Access was one of the first use cases, rather than mobile usage and first commercial devices announced have been 5G home routers, such as the one announced by Huawei at MWC 2018 in Barcelona, or the one by Samsung. Between Q3 2019 and Q4 2019, the number of such devices listed more than doubled.	**Fixed wire access consumer products market** Measure will have no direct impact as the measures would not appear to affect Huawei Fixed Wireless Access devices. However, the US trade sanction as regards the in practice prohibition of US-technology to Huawei will likely have an impact.

13. Financial Times, Nvidia sends shockwaves through chip industry with Arm deal, 15 September 2020.

14. Department of Commerce, Bureau of Industry and Security, Export Administration Regulations: Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule) and the Entity List, 19 May 2020, Rule 85 FR 29849, see https://www.federalregister.gov/documents/2020/05/19/2020-10856/export-administration-regulations-amendments-to-general-prohibition-three-foreign-produced-direct.

Annex -4: Competition Practical Assessment

Third party findings	Preliminary conclusions
According to Gsacom, as of the end of May 2020, 33 operators had launched 5G FWA services in the world." *5G Observatory Quarterly Report 8, up to June 2020, page 58*	
"Because of the limited margin in the industry and the pressure on price that Chinese vendor Huawei has been able to impose, every point of margin is key, either to reinvest in Research and Development, either to more aggressively compete on prices. Meanwhile, Huawei launched its 1st generation of own 5G base station processor called Tiangang in 2019, while Samsung launched its 2nd generation of base station chipset the same year. While other vendor Ericsson and ZTE are also said to design their own processors, they also ended up partnering with silicon specialist Broadcom and Intel." *5G Observatory Quarterly Report 8, up to June 2020, page 67*	Infrastructure chipset market This changes the bargaining power between chipset suppliers and chipset customers. Possibly, with chipset suppliers gaining some negotiating power.
"Transitions between wireless technology generations before 5G also had substantial commercial, competitive, and security implications for first-movers. Europe, led by Germany, gained first competitive advantage in 2G, and as a result companies like Nokia and Ericsson were able to roll out more advanced devices earlier and were already transitioning to 3G in the 2000s when the United States was still trying to implement 2G. The European wireless tech industry boomed during this period while U.S. companies struggled to keep pace. Europe lost this edge during the 3G transition, when they were hampered by regulations that required time consuming auctions of 3G	**Related markets** The previous examples of the 2G, 3G and 4G show that early deployment of 5G technology will be crucial for the development of various technologies and services based on that technology and gain a significant technological advantage as first movers. The price increase and delay in rolling out 5G that would be the consequence of government measures will limit the development of existing and new technology and services markets in the EU able to set global standard and compete on the global market.

Annex -4: Competition Practical Assessment

Third party findings	Preliminary conclusions
spectrum, rather than simply repurposing existing 2G spectrum bandwidth. Japan took the lead on 3G, and while the United States ultimately caught up to Japan, it took years to roll out 3G networks, which came at a huge cost to U.S. businesses as Japan sprinted forward with its 3G business model. The United States lost thousands of jobs and considerable revenue during this transition, during which multiple wireless technology companies failed or were absorbed into foreign companies." "(...) In the early 2010s, AT&T and Verizon rapidly deployed LTE across the United States in the 700 MHz spectrum they won at auction in 2008. The United States became the first country (after Finland) to see a comprehensive LTE network that delivered approximately 10x the consumer network performance of existing 3G networks. This step-change in performance drove rapid adoption of new handsets with new semiconductors that not only could move much more data, but were computationally much faster as well. U.S. companies like Apple, Google, Facebook, Amazon, Netflix, and countless others built new applications and services that took advantage of that bandwidth and those new handset capabilities. As LTE was deployed in other countries, those same handsets and applications spread across the world, driving U.S. dominance in global wireless and internet services. The United States has benefited significantly from this lead. Recon Analytics published a report in April 20181 estimating that the introduction of 4G contributed to 70% growth in the wireless industry between 2011 and 2014, bolstering GDP while	

Annex -4: Competition Practical Assessment

Third party findings	Preliminary conclusions
increasing jobs in the wireless industry by over 80%. By leading the charge on 4G, the United States was able to build a global ecosystem of network providers, device manufacturers, and app developers that shaped the future of 4G and the experience of all other countries implementing it. First-mover advantage is particularly pronounced in wireless generation transitions because the leader can set the foundational infrastructure and specifications for all future products. (...) The shift to 5G will carry the same potential risks and rewards as previous generational transitions, but at an even larger scale. The leader of 5G stands to gain hundreds of billions of dollars in revenue over the next decade, with widespread job creation across the wireless technology sector. 5G has the potential to revolutionize other industries as well, as technologies like autonomous vehicles will gain huge benefits from the faster, larger data transfer. 5G will also enhance the Internet of Things (IoT) by increasing the amount and speed of data flowing between multiple devices, and may even replace the fiber-optic backbone relied upon by so many households. The country that owns 5G will own many of these innovations and set the standards for the rest of the world." *The 5G Ecosystem: Risks & Opportunities for DoD, Page 6* [15]	

15. Defense Innovation Board, The 5G Ecosystem: Risks & Opportunities for DoD, 3 April 2019, see https://media.defense.gov/2019/Apr/04/2002109654/-1/-1/0/DIB_5G_STUDY_04.04.19.PDF.

Annex - 4: Competition Practical Assessment

Third party findings	Preliminary conclusions
"A delay in the rollout of 5G would also result in slower technological innovation and reduced economic growth. In our central cost scenario, this would result in reductions to national GDP in 2035 ranging from €13 million in Iceland to €7.3 billion in France. The total GDP in 2035 lost in the 31 countries in our study is estimated to be €40 billion in 2020 prices. (...) Estimated permanent loss in Gross Domestic Product (GDP) due to delay in 5G rollout in 2035: Low cost scenario €12 billion; Central cost scenario €40 billion; High cost scenario €85 billion." *Restricting competition in 5G network equipment throughout Europe, An Economic Impact Study, page 3*	**Related markets** This study evaluates a significant growth impact on GDP of slowing down the rolling out of 5G.

Annex -5: Cybersecurity medium measures and the related risks

ID	Measure	Related risks
TM01	Ensuring the application of baseline security requirements (secure network design and architecture)	R1 - Misconfiguration of networks R2 - Lack of access controls R3 - Low product quality R5 - State interference through 5G supply chain R6 - Exploitation of 5G networks by organized crime or organized crime group targeting end-users R7 - Significant disruption of critical infrastructures or services R9 - Exploitation of IoT (Internet of Things), handsets or smart devices
TM02	Ensuring and evaluating the implementation of security measures in existing 5G standards	R1 R2 R3 R6 R7 R9
TM03	Ensuring strict access controls	R1 R2 R3 R5 R6 R7
TM05	Ensuring secure 5G, network management, operation and monitoring	R1 R2 R3 R5 R6 R7 R9
TM07	Reinforcing software integrity, update and patch management	R1 R3 R5 R6 R7
TM08	Raising the security standards in suppliers' processes through robust procurement conditions	R3 R6 R7
TM09	Using EU certification for 5G network components, customer equipment and/or suppliers' processes	R3 R6 R7

Annex -6: Cybersecurity Potential Implementation Factors

Third party findings	Preliminary conclusions
'Since 2010, several measures have been taken to raise the level of security of State information systems. A State Information Systems Security Policy (PSSIE) was developed, an inter-ministerial electronic communications network is in rapid growth and the roll-out of secured mobile terminals has been initiated. These measures, like those aimed at producing the security equipment to protect sovereign information, mobilize human and budgetary resources.' French National Digital Security Strategy, page 15 [1]	**Costs** The government measures create costs for society which are borne by governments.
'Impose additional controls on the presence of certain types of vendors which pose significantly greater security and resilience risks to UK telecoms. In considering what those controls should be, it is necessary to address the identified security risks, whilst seeking to minimise the costs to industry and the wider economy.' UK Telecoms Supply Chain Review Report, page 7 [2]	**Costs** Implication is that the measure is expected to raise costs both to market participants and the wider economy.
"In mobile and fixed access, switching costs are high once the equipment of a particular vendor is deployed in the network. This is most notable in the mobile access network, where switching may involve replacing costly legacy equipment, due to the non-standalone nature of 5G deployment in the next few years." *UK Telecoms Supply Chain Review Report, July 2019, page 32*	**Costs** The measures will raise costs.

1. Office of the Prime Minister of France Manual Valls, French National Digital Security Strategy, October 2015, see https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf.

2. Department for Digital, Culture, Media & Sport, UK Telecoms Supply Chain Review Report, July 2019, see https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819469/CCS001_CCS0719559014-001_Telecoms_Security_and_Resilience_Accessible.pdf.

Annex -6: Cybersecurity Potential Implementation Factors

Third party findings	Preliminary conclusions
"The answer to this issue of sovereignty requires first and foremost the maintenance of a strong and competitive national and European industry in the specialized field of cybersecurity products and services. In general, it requires the development, in France and Europe, of a digital equipment and service offer that provides clients with the guarantees of security and trust adapted to the issues and uses." *French National Digital Security Strategy, page 30*	**Sector-specific impacts** Government led industrial policy would reshape the sector, with a focus on EU self-reliance.
"Limited opportunities and incentives for innovation of large enterprises. There are various mechanisms at the European and national level supporting innovation for SMEs as well as emerging innovative entrepreneurships such as start-ups. Unfortunately, there are limited opportunities and incentives for innovation of large enterprises. Besides some Public-Private Partnerships (PPPs), large enterprises have to face most of the cost and investment in innovation. However, they may have a critical role in order to accelerate innovation as well as to provide access to markets for innovation at scale. Unfortunately, there is a lack of initiatives and incentives in order to support innovation collaboration between SMEs and large enterprises, besides normal market dynamics." *Good practices in innovation on cybersecurity under the NCSS, Page 39* [3]	**Sector-specific impacts** Implication is that elsewhere expressed desire of the need/desire to encourage new entrants and EU-sourced innovation may be harder to achieve than hoped. This implies greater reliance on existing firms than new entrants.

3. European Union Agency for Cybersecurity (ENISA), Good Practices in Innovation on Cybersecurity Under the National Cyber Security Strategies, November 2019, see https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1.

Annex -6: Cybersecurity Potential Implementation Factors

Third party findings	Preliminary conclusions
"In terms of the global market, the key threat to EU is that better funded overseas NIS players succeed in entirely dominating the EU market. They could exploit the EU's fragmentation by acquiring the best local companies in each Member State, then expanding sales as a common brand across the EU, with major inward investment underpinned by their home markets' revenues (in the USA and China). Similarly, it is conceivable that intellectual property funded and developed in the EU could be bought and exploited by overseas NIS suppliers, from China and the USA, so that EU investments in R&D may be lost to the EU. In this regard, promising EU suppliers may have little alternative because of the limited EU investment available to enable them to develop the more advanced tools required and bring them to market. Not only is EU funding for R&D and industrialisation too limited, given the scale of AI and large-scale data analytics required, but it is spread too thinly, making the creation of a major EU player less likely. Moreover, EU and national funding may be too burdensome to access in terms of costs and bureaucracy for start-ups and SMEs. Thus, any promising innovative or existing EU NIS supplier is often acquired by a global player, especially if major equity holders are anxious to realise their investments." *Good practices in innovation on cybersecurity under the NCSS, Page 41*	**Sector specific impacts** Implication is that government measures in order to be effective would need to include FDI investment provisions.

3. European Union Agency for Cybersecurity (ENISA), Good Practices in Innovation on Cybersecurity Under the National Cyber Security Strategies, November 2019, see https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1.

Third party findings	Preliminary conclusions
"This will delay our 5G rollout. Our decisions in January had already set back that rollout by a year and cost up to a billion pounds." "Today's decision to ban the procurement of new Huawei 5G equipment from the end of this year will delay rollout by a further year and will add up to half a billion to the costs. Requiring operators, in addition, to remove Huawei equipment from their 5G networks by 2027 will add hundreds of millions to the cost and further delay roll out. This means a cumulative delay to 5G rollout of two to three years and costs of up to two billion pounds." *UK's Digital, Culture, Media and Sport Secretary of State, oral statement to Parliament.* [4]	**Costs** Broader economic and/or societal impacts Recognition by the UK government of the significant impacts of the government measures.
"To go further and faster beyond a 2027 target would add considerable - and unnecessary - further costs and delays. And the shorter we make the timetable for removal, the greater the risk of actual disruption to mobile telecoms networks." *UK's Digital, Culture, Media and Sport Secretary of State, oral statement to Parliament.*	**Costs** Broader economic and/or societal impacts Implication potentially of broader geographic relevance is that until 2027 Huawei should continue to be an element of the markets (5G, 4G…), to avoid unnecessary negative impacts.
"…we will need to take a different approach to full fibre and older networks - one that recognises that they are different to 5G in terms of their technology, their security, and the vendors supporting them. Given there is only one other appropriate scale vendor for full fibre equipment, we are embarking on a short technical consultation with operators to understand their supply chain alternatives, so that we can avoid unnecessary delays to our gigabit ambitions and prevent significant resilience risks.	**Impacts generally** Per the EU toolbox the effectiveness on cybersecurity of ensuring the diversity of suppliers through appropriate multi-vendor strategies is identified as very high within a time frame of zero to 5 years, depending upon the 5G deployment calendar. Although measures outside of 5G are outside the scope of this Report, applying the EU toolbox rationale to older networks applies consistency of thinking at one level

4. UK's Digital, Culture, Media and Sport Secretary of State, oral statement to the House of Commons on 14 July 2020, see https://www.gov.uk/government/speeches/digital-culture-media-and-sport-secretarys-statement-on-telecoms.

Third party findings	Preliminary conclusions
The technical consultation will determine the nature of our rigorous approach to Huawei outside our 5G networks." *UK's Digital, Culture, Media and Sport Secretary of State, oral statement to Parliament.*	but may not be consistent with the historical record given the acceptance of Huawei products to date within a regulated regime, such as the UK.
"Reinforcement of the protection of operators of vital importance (OIV): Reinforcement of the level of requirements of safety rules which apply to IMSs in the communications sectors electronics and energy supply electric. Short term with financial and legal impact study." *Cyber defense strategic review, Recommendations, Page 138* [5]	**Costs** The assumption is that those measures will have some cost and that those cost needs to be assessed.
"According to the information gathered, the Government intends, through this text, to adopt a balanced approach and to address all potential vulnerabilities related to the deployment of 5G, whatever their source. Thus, the proposed law, on the one hand, does not aim to ban Huawei, on the other hand, does not concern Huawei alone: the modalities for operating the equipment would be checked for the entire network chain, regardless of the operators' service provider - equipment manufacturer or other. The Government also stresses that this initiative is independent on the international context. Consequently, two fears that emerged in the debates, namely a risk of disruption of supply and a risk due to the lack of competitiveness of operators in cases where they would not be able to use Huawei's equipment, should be able to be dispelled. Moreover, these fears seem, in themselves, to be unfounded."	**Impacts generally** This statement is to be compared to the practical effect of the measures and the statement above. At the time where the legal basis for the French government measures was discussed and adopted by the French Parliament, the exclusion of Huawei or any specific supplier was not envisaged, at least publicly. However, the practical effect of the French government measures is in the short/medium-term, in effect, to ban Huawei from the 5G network equipment in France. 6 As such, the discussion in front of the parliament, as well as the financial and legal impact studies conducted could not envisaged properly the impact of the French government measures at the time.

5. General Secretariat for Defense and National Security (SGDSN), Cyber defense strategic review, Recommendations, February 2018, in French, see http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf.

6. See https://www.reuters.com/article/us-france-huawei-5g-security-exclusive-idUSKCN24N26R; See also https://www.politico.eu/article/france-introduces-de-facto-ban-on-huawei-5g-equipment-by-2028/.

Annex -6: Cybersecurity Potential Implementation Factors

Third party findings	Preliminary conclusions
Report on behalf of the Senate Committee on Economic Affairs on the draft law aiming at safeguarding the defense and national security interests of France within the framework of the operation of mobile radio networks, Page 36 [7]	
"Controlling essential digital infrastructures on European territory The decisive nature of digital activities in European societies makes it necessary to control essential infrastructures. The current dependency in this area would constitute a great vulnerability for all Member States and institutions. Consideration must be given to the infrastructures essential to the operation of digital activities in order to identify those whose control constitutes the condition of national sovereignty and European autonomy. Maintaining a sufficient right to regulate (in particular in the context of international trade negotiations) is essential in a context where the speed of digital development creates constant uncertainty about the very level of regulation that we must be able to implement." *France's international digital strategy, Page 24* [8]	
"Since its creation, ANSSI has gradually strengthened its role with the OIV [Operators of Vital Importance]. Until 2013, with the exception of the electronic communications sector, the ANSSI's missions were limited to the dissemination of technical advice by drawing up guides and recommendations or carrying out security audits,	**Broader impacts** The National Cybersecurity Agency of France has seen its power progressively increase from providing advice to setting up requirements. However, even with these powers, the level of security is not considered as satisfactory.

7. Catherine Procaccia, *Report on behalf of the Senate Committee on Economic Affairs on the draft law aiming at safeguarding the defense and national security interests of France within the framework of the operation of mobile radio networks*, June 2019, in French, see http://www.senat.fr/rap/l18-579/l18-5791.pdf

8. France's international digital strategy, December 2017, in French, See https://www.diplomatie.gouv.fr/IMG/pdf/strategie_numerique_a4_02_interactif_cle445a6a.pdf..

Third party findings	Preliminary conclusions
solely at their request. Faced with a growing computer threat and an ever-increasing risk of computer sabotage, the level of security of these players remained insufficient, exposing them, and the nation as a whole, to a major cyber risk. In 2013, France therefore decided to impose computer security requirements on IMSs by law, thus becoming one of the first countries to legislate in the field of cybersecurity of critical infrastructures. The cyber provisions of the military programming law of 2013 have entrusted the ANSSI with new missions in this area: they provide that these operators apply the computer security measures set by the ANSSI and notify it of security incidents affecting their information systems. (...) It is therefore necessary to develop the model to adapt it more to the constraints of the sectors and to the evolution of cyberthreat in five directions: adapting computer security rules to the professions; strengthening the cybersecurity of "supercritical" operators; extending the regulatory mechanism to the treatment of incidents; taking into account the specificities of digital service companies; and developing the private offer of technical assistance in cybersecurity." *Cyber defense strategic review, Recommendations, Page 59*	
"Similar to steps taken in the United Kingdom, the Australian Government will co-design supply chain principles for decision makers and suppliers, to encourage security-by-design; transparency; and autonomy and integrity in investment, procurement and security.	**Costs** Similar to the UK, such measures will create significant costs for the Australian government in the short/medium term.

Annex -6: Cybersecurity Potential Implementation Factors

Third party findings	Preliminary conclusions
The Australian Government will build these principles into decision-making practices, supporting competition and diversity in the market. To keep guidance up to date as technology and threats continue to evolve, the Australian Government will continue to monitor and build on existing government initiatives that promote innovation in sovereign cyber security research and development. AustCyber is well placed to assure continued commercialisation and scaling of cyber security capabilities that support our nation's needs." *Australian Cybersecurity Strategy 2020, Page 32* [9]	

9. Australian Cybersecurity Strategy 2020, August 2020, See https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf.

Annex -7: Cybersecurity Medium Technical Measures

Third party findings	Preliminary conclusions
"For 5G access networks, at most 35% of expected network traffic volume on any particular network passes through HRV equipment and at most 35% of base station sites nationally on any particular network should be served by equipment from an HRV" NCSC guidance 2020, page 7 [1]	**TM03** There is no justification for the 35% threshold in the UK. It is noted this threshold is similar to the current national threshold of Huawei in the UK. Given the effectiveness of access limitation is considered moderate, some justification would seem appropriate.
"…there can be tensions between commercial priorities and security concerns, particularly when these impact on costs and investment decisions. Equally, the business models of vendors have not always prioritised cyber security sufficiently. An extreme example of this can be seen in the conclusions of the 2019 Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board report. The flaws identified in the report are the result of practices that may have achieved good commercial outcomes but have resulted in poor cyber security." UK Telecoms Supply Chain Review Report, page 7 [2]	TM08 Raising the security standards of suppliers impliedly raises costs and so prices, but the UK has concluded this is counterbalanced given its finding of below satisfactory assurance levels of cybersecurity in Huawei's products. Huawei has co-operated materially with the UK through the HCSEC. It is an open question the extent to which other suppliers, in particular for whom concerns have been raised as to their levels of security, will also be subject to an HCSEC-like arrangement. Guidance in the UK is that 'Operators should only use an HRV if that HRV has in place a specific risk mitigation strategy, designed and overseen by the NCSC' .[3]
"The German authorities are currently conducting a consultation with the industry. Possible binding measures are not expected to be adopted before the autumn. On 7 March this year [in 2019], the German telecoms regulator published a list of new security requirements that it wants to make applicable to 5G networks, with the help of its German counterpart ANSSI. It focuses in particular on certification procedures for telecommunications equipment.	

1. UK's National Cyber Security Centre (NCSC), NCSC advice on the use of equipment from high risk vendors in UK telecoms networks, 30 August 2020 (updated), see https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks.
2. Department for Digital, Culture, Media & Sport, UK Telecoms Supply Chain Review Report, July 2019, see https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819469/CCS001_CCS0719559014-001_Telecoms_Security_and_Resilience_Accessible.pdf.
3. UK Telecoms Supply Chain Review Report, Page 7

Annex -7: Cybersecurity Medium Technical Measures

Third party findings	Preliminary conclusions
It recommends that operators avoid exclusive dependence on a single supplier and rely on trusted suppliers. According to ANSSI, there is a divergence of approach between Germany and France: the former wishes to make the process more objective, by listing all the elements required for authorization, without any room for interpretation. This is not the approach adopted by the French Government, which considers it impossible to include everything in a list of questions with boxes to be ticked." Report on behalf of the Senate Committee on Economic Affairs on the draft law aiming at safeguarding the defence and national security interests of France within the framework of the operation of mobile radio networks, Page 27 .[4]	**TM09** The difference in approach between EU governments regarding the certification may significantly raise the regulatory standard and associated cost if, after the implementation of an EU certification, some EU governments require additional security test and protocol.
"Virtualization and the fact that the network architecture will depend in part on its use mean that an analysis focused solely on the specific technical characteristics of the equipment, as supplied by the equipment manufacturers, is no longer sufficient to cover all the security issues, and that a complementary analysis of the operating methods (network configuration and supervision operations, recourse to subcontracting) adopted by each operator becomes essential. ANSSI's managing director believes that "it is possible to deploy very poor telecom networks in terms of security with perfectly secure equipment. On the other hand, a well-secured network architecture makes it possible to use equipment with a less demanding level of security".	**TM01/TM09** The technical certification of the equipment used in the network will not be sufficient to ensure proper security of the network but a more detailed analysis of each network and operating methods on a case-by-case basis will be required.

4. Catherine Procaccia, *Report on behalf of the Senate Committee on Economic Affairs on the draft law aiming at safeguarding the defense and national security interests of France within the framework of the operation of mobile radio networks*, June 2019, in French, see http://www.senat.fr/rap/l18-579/l18-5791.pdf.

Third party findings	Preliminary conclusions
According to the government, the greater freedom given to operators in their choice of deployment and operation of their equipment makes it necessary for them to play a greater role in securing it. The Prime Minister will thus be able to provide support on a case-by-case basis to each operator and its subcontractors in the definition of the modalities of operation of their network. According to ANSSI's Director General, this system would ensure that operators remain, in the long term, the "masters of the game" on their networks." *Report on behalf of the Senate Committee on Economic Affairs on the draft law aiming at safeguarding the defense and national security interests of France within the framework of the operation of mobile radio networks, Page 34.*	
"Is an authorization required in case of an update? The regime of article 226-3 of the penal code concerns both hardware and software. In previous generations of radio networks, upgrades were the result of changes in equipment. Today, networks are modified by simple software updates, which raises the question of when it is a question of new equipment subject to authorization. All equipment manufacturers in the telecommunications field distinguish, in their versioning conventions: ▸ minor evolutions (generally correcting vulnerabilities or malfunctions, without adding new functionalities); ▸ and major changes (changes in the functional scope, for example support for new protocols or new revisions of standards).	TM07 A common definition of the updates and evolutions requiring new authorizations and/or certification would be necessary to improve transparency, objective analysis and confidence in the security of networks and technical requirements on the different actors.

Annex -7: Cybersecurity Medium Technical Measures

Third party findings	Preliminary conclusions
This distinction is generally reflected in the deployment procedures of operators, who deploy minor updates after a relatively small set of tests but provide for extended testing campaigns prior to any major updates. As minor updates do not change the security analysis, they do not give rise to a new request for authorization. On the other hand, in the absence of unified version agreements, the precise definition of what constitutes a major or minor version is specific to each equipment manufacturer, or even to each range of equipment. Ericsson, for example, has adopted a so-called "one track" model, i.e. without a version, which no longer makes it possible to distinguish between major and minor upgrades. The terms and conditions for managing these "versions" are then decided on a case-by-case basis in the conditions associated with each authorization." *Report on behalf of the Senate Committee on Economic Affairs on the draft law aiming at safeguarding the defense and national security interests of France within the framework of the operation of mobile radio networks, Page 48*	**TM07** A common definition of the updates and evolutions requiring new authorizations and/or certification would be necessary to improve transparency, objective analysis and confidence in the security of networks and technical requirements on the different actors.
"Communication networks and services should be designed with resilience and security in mind. They should be built and maintained using international, open, consensus-based standards and risk-informed cybersecurity best practices. Clear globally interoperable cyber security guidance that would support cyber security products and services in increasing resilience of all stakeholders should be promoted." *The Prague Proposals, page 3* [5]	**TM09** The Prague Proposals recognize the importance of open and consensus-bases security standard. However, there is a clear lack of data publicly available and there is no uniformity or consistency between States approach and measures, even within the EU.

5. Prague 5G Security Conference, The Prague Proposals, The Chairman Statement on cyber security of communication networks in a globally digitalised world, 3 May 2019 see https://www.vlada.cz/assets/media-centrum/aktualne/PRG_proposals_SP_1.pdf

Annex -7: Cybersecurity Medium Technical Measures

Third party findings	Preliminary conclusions
"Security visas The ANSSI has for many years, on the basis of in-depth evaluations launched at the initiative of the providers concerned, issued security visas for a wide range of security products: hardware or software, performing encryption, electronic signature, interconnection between secure networks, authentication, etc. These visas are essentially of three distinct types: ▸ the certification attests to the robustness of a security product with regard to the requirements (nature of the security functions, level of the attacker) set by a sponsor, which is not necessarily the State. It is therefore a toolbox enabling various parties (governments, private operators - banks, for example - and independent authorities) to define security criteria and to have these criteria verified by a third party; ▸ qualification by the State is equivalent to a recommendation for use in a given context; it implies certification of the product, supplemented by verification of the safety and updating requirements demanded of suppliers over time. Qualification applies both to the needs of government administrations and services and to those of the OIVs; ▸ Authorization is a regulatory decision authorizing the use of a solution that has been qualified beforehand for the processing of classified information.	TM09 The usage of certification is not new in the area of cybersecurity. Although the current "ad-hoc" certification is limited to high level certification and not suitable for more commonly used products. This report calls for the implementation of a reform close to what has been created with the EU Cybersecurity act and its EU Certification scheme. However, regarding the cybersecurity of 5G network this raises two questions: (i) If the EU certifications scheme is more appropriate to commonly used goods, the EU certification scheme might not be applicable or suitable for 5G network equipment that would require more in-depth review and/or certification; (ii) Given the 'disseminated' nature of 5G network and the importance of equipment on the edge of the network for its security, would the EU certification scheme be enough to ensure the security of 5G network?

Annex -7: Cybersecurity Medium Technical Measures

Third party findings	Preliminary conclusions
(…) The existing certification framework, although modulating the level of requirements according to safety needs, is still very much focused on high level certification. It is ill-suited to the evaluation of commonly used products (such as connected objects), for which it is prohibitively expensive and time-consuming. For this reason, the present review proposes the introduction of a basic cybersecurity certification, in addition to the existing certification framework, which is reserved for products and services at the top of the spectrum. This could be based on existing schemes in other contexts than cybersecurity, such as the CE marking required for the marketing of certain goods or services within the European area. This basic cybersecurity certification would essentially be based on a conformity analysis, on the basis of predefined specifications. This conformity check could be delegated to a private body, with the involvement of public authorities limited to indirect actions (accreditation of private assessment centres). This approach appears to be suitable for certifications for which certain obligations of the current system, such as the carrying out of a "free" vulnerability analysis outside the specifications, and the issuing of certificates by the ANSSI, seem less justified. By reducing certification costs and timescales, this reform is likely to encourage the emergence of a range of products consistent with the requirements. The implementation of a basic certification mechanism could rely on certain compliance monitoring service providers with the help of ANSSI.	

Annex -7: Cybersecurity Medium Technical Measures

Third party findings	Preliminary conclusions
The national cybersecurity authority could contribute to the definition of basic certification protocols, accredit centres of expertise and evaluation, and animate the network, notably through training courses." *Cyber defense strategic review, Recommendations, Page 110* [6]	
"The interoperability of Internet networks, services and digital applications is a prerequisite for its openness. It is based on international standards (e.g. GSM, 4G, 5G for mobile Internet) and protocols (e.g. IPv4, IPv6) defined in various forums (e.g. Internet Engineering Task Force, World Wide Web Consortium, 3 Generation Partnership Project, ITU, GSMA, ETSI International Telecommunication Union). The definition of these standards is of strategic interest in industrial, security and personal data protection terms. It is therefore necessary to better federate the efforts of French and European players, both public and private, within these bodies, in order to influence the development of standards and protocols, but also to define a European approach to standardization, particularly with regard to the emergence of new structuring technologies (such as the Internet of Things). (...) Strengthening Europeans' cybersecurity capabilities The cybersecurity standards applicable to "essential service operators" defined by the Member States in the framework of the implementation of the NIS (Network and Information Security) Directive must constitute a minimum level for all Member States. Capacity development within the EU is a priority for France, which contributes to this through its bilateral partnerships and its active involvement in ENISA, the European Cybersecurity Agency. Capacity	TM02 Several international standards of interoperability remain to be set, and EU cooperation is required in this domain.

6. General Secretariat for Defense and National Security (SGDSN), Cyber defense strategic review, Recommendations, February 2018, in French, see http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf.

Annex - 7: Cybersecurity Medium Technical Measures

Third party findings	Preliminary conclusions
building within the European institutions (CERT-EU) is also a priority." *France's international digital strategy,* [7] *Page 8, 25*	

6. France's international digital strategy, December 2017, in French, See https://www.diplomatie.gouv.fr/IMG/pdf/strategie_numerique_a4_02_interactif_cle445a6a.pdf.

Our offices

Diegem
De Kleetlaan 2
1831 Diegem
Tel: +32 (0) 2 774 64 40

Antwerp
Borsbeeksebrug 26
2600 Antwerpen (Berchem)
Tel: +32 (0) 2 774 64 40

Diegem
Belliardstraat 40
1040 Brussels
Tel: Tel: +32 (0) 2 774 64 40

Gent
Pauline Van Pottelsberghelaan 12
9051 Gent
Tel: Tel: +32 (0) 2 774 64 40

EY LAW BV/SRL

EY LAW

About EY Law
EY Law is a company having the legal form of a limited company (BV/SRL) organised and existing under the laws of Belgium, having its registered office at De Kleetlaan 2, 1831 Diegem, Belgium and registered with the Crossroads Bank of Enterprises (Brussels) with registration number BTW/TVA BE0536.360.510.
EY Law has branch offices in Belgium at rue Belliard 40, 1040 Brussels, at Borsbeeksebrug 26, 2600 Antwerpen and at Pauline Van Pottelsberghelaan 12, 9051 Gent.
EY Law is an independent law firm which has access to the international EY Law network of legal practices affiliated to EY. The EY Law network currently consists of 3,500 highly qualified legal professionals providing legal services in 86 jurisdictions across the globe.
EY Law has a privileged cooperation with EY Tax Consultants.

www.eylaw.be