Manuel Conthe

Mr. Manuel Conthe
Serrano, 26 – 4º
28001 Madrid
Spain

Opinion on the risk of State-interference (R5) on Huawei as a 5G Vendor[1]

July 4th, 2020

[1] This Expert Report was commissioned and funded by Huawei Technologies España S.L., which has authorized the author to make it public on his professional webpage as arbitrator (www.manuelconthe.com)

4TH July, 2020

Table of Contents

Abbreviations 3
1. Introduction 4
2. Huawei: an overview 4
2.1. Huawei's success story 4
2.2. R&D 5
2.3. Corporate structure and governance 6
2.4. Compliance 8
2.4.1. Huawei's Global Cyber Security and Privacy Protection Office 8
2.4.2. Huawei's third-party security mechanisms 9
2.5. Huawei in Europe 9
2.5.1. Huawei's role in European 4G networks 9
2.5.2. Huawei's Transparency Centres 10
2.5.3. Huawei's compliance with the GDPR 10
2.5.4. The UK's HCSEC and Oversight Board 12
2.6. Huawei in Spain 14
2.6.1. Huawei's business in Spain 14
2.6.2. Relations with public authorities 16
3. Spain´s 5G project 16
3.1. Spain´s current telecoms network 16
3.2. Spain´s 5G roadmap 16
3.3. Huawei as 5G supplier 17
4. Political concerns about Huawei 17
4.1. Western suspicions about Chinese companies 17
4.2. 5G-related geopolitical concerns 18
4.3. US special fears about Huawei 19
4.4. The UK's position on Huawei 21
4.5. EU-China relations and EU "digital sovereignty" aspirations 21
5. The EU's Toolbox 23
5.1. The EU Coordinated Risk Assessment 23
5.2. The Toolbox's main elements 24
5.2.1. Risks 24
5.2.2. Measures 24
5.2.3. Recommendations 26
5.2.4. Legal nature 27
6. The legal framework on 5G networks 28
6.1. The three basic regulatory frameworks 28
6.2. The EU Telecommunications Framework 29
6.3. The NIS Directive 31

6.4. The EU Cybersecurity Act Regulation 31
6.5. Data Protection and privacy rules 32
6.5.1. The General Data Protection Regulation (GDPR) 32
6.5.2. Spain´s regulations on data protection 33
6.5.3. The AEPD's initial position on 5G 33
6.6. The Directive on Critical Infrastructures 33
7. Assessing the risk of PRC interference in Huawei (R5): key legal principles 34
7.1. The Toolbox and the "Preventative State" 34
7.2. The limits of the "public security" or "public policy" exception 35
7.2.1. WTO law and the security exception 36
7.2.2. The EU's "appropriateness" and "proportionality" tests 38
7.2.3. Spain's legal principles 43
7.3. Conclusions 44
8. Assessing the risk of PRC interference in Huawei (R5): key issues 45
8.1. The risk of Chinese political interference in Huawei 45
8.1.1. Is Huawei State-owned? 45
8.1.2. Is Huawei State-controlled? 48
8.1.3. Could Chinese security laws have illegal extraterritorial effects? 53
8.1.4. Why (only) Huawei? 56
8.1.5. Conclusions 57
8.2. Huawei's track-record 58
8.2.1. No past cyber-security incidents 59
8.2.2. Pro-active cyber-security attitude and cooperation with authorities 60
8.3. The costs of declaring Huawei a High-Risk Vendor (HRV) 61
8.4. The existence of more effective and less restrictive alternatives 64
8.5. Conclusions 65
9. General conclusions 66
10. Final considerations 70

Abbreviations

AEPD	Spanish Data Protection Supervisory Authority
BCP	Business Continuity Plan
BIPPA	Bilateral Investment Promotion and Protection Agreement
BSIMM	Building Security in Maturity Model
CEOE	Spanish Confederation of Business Organizations
CERT(s)	Computer Emergency Response Team(s)
CI(s)	Critical Infrastructure(s)
CNMC	Spain's National Commission on Markets and Competition
CSEM	Cyber Security Evaluation Methodology
CSIRT(s)	Computer Security Incident Response Team(s)
DDoS	Denial-of-Service
DPO	Data Protection Officer
DPAs	Data Protection Supervisory Authorities
DPIA(s)	Data Protection Impact Assessment(s)
EC	European Commission
ECI(s)	European Critical Infrastructure(s)
ECJ	European Court of Justice
EECC	European Electronic Communications Code
ENISA	The European Agency for Cybersecurity
FDI	Foreign Direct Investment
GATT	General Agreement on Tariffs and Trade
GCSPC	Global Cyber Security and Privacy Protection Committee
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation [Regulation (EU) 2016/679]
GSPC	Global Cyber Security and Privacy Protection Committee
GSPO	Global Cyber Security & Privacy Officer
GVA	Gross Value Added
HCSEC	Huawei Cyber Security Evaluation Centre
ICT	Information and Communication Technologies
INCIBE	The Spanish National Institute of Cybersecurity
ICSL	Independent Cyber Security Lab
MNO(s)	Mobile Network Operator(s)
MVNO(s)	Mobile Virtual Network Operator(s)
NCC	Spain's National Cryptologic Centre
NCSC	UK's National Cyber Security Centre
NIS	Network & Information Systems
NRA	National Regulatory Authority
PIA	Privacy Impact Assessment
PRC	People's Republic of China
R&D	Research and Development
TFEU	Treaty on the Functioning of the European Union
WTO	World Trade Organization

1. Introduction

1. I have prepared this expert opinion (henceforth, the "Opinion") at the request of Huawei Spain, to give my opinion on the following related questions:

   - Whether there is a risk of interference of Chinese public authorities on Huawei as a supplier of Spain's 5G network; and,

   - Whether, on the basis of its risk-profile, it would be appropriate to apply to Huawei any of the restrictions envisaged in strategic measure 03 (SM 03) of the document "Cybersecurity of 5G networks. EU Toolbox of risk mitigating measures" (henceforth, the "Toolbox") approved by the NIS Operating Group in January 2020[2],

2. This Opinion is based on the information, documents and responses and explanations, both oral and in writing, provided to me by Huawei, together with the information, publications, and relevant legal texts publicly available on this matter.

3. I have assumed that the documents provided to me by Huawei are accurate and complete copies of the originals and, in the case of Chinese laws, that their English translation is also accurate.

4. My CV is publicly available at www.manuelconthe.com. My qualification for writing this Opinion is based on the experience shown therein and particularly on my work as lawyer and international arbitrator since 2009, and my previous experience as senior public official in Spain's Securities & Exchange Commission (CNMV) and Ministry of Economy and Finance and in the World Bank.

5. I want to express my particular gratitude to Carmen Ruiz Lorente, Legal Counsel for Huawei Spain, who most kindly and effectively provided me with all the information, and organized all the interviews, that I requested for the preparation of this Opinion.[3]

6. This Opinion has been prepared under Spanish law and the interpretation or references to the laws of any other jurisdiction have been carried out according to Spanish law.

2. Huawei: an overview

2.1. Huawei's success story

7. Huawei was originally founded in 1987 by Mr. Ren Zhengfei and other five investors as a modest undertaking based in Shenzen, a part of China where private companies could expand because it was a special economic zone. While it initially specialized in reselling telephone switches mostly in rural China, it is today i a leading global provider of Information and Communication Technology ("ICT") solutions, with around 194,000 employees,

[2] Available at https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_127.
[3] Only publicly available documents will be explicitly mentioned in this Report, even if its autor consulted many other non-public ones.

operating in more than 170 countries and regions, and serving more than three billion people around the world.

8. As part of its ICT activities, Huawei carries out in China and around the world not only the research, design, manufacture and marketing of telecom network equipment, but also provides many other services, including cloud technology and services, mobile internet services and the production of smartphones and other devices for enterprises and consumers. However, this Opinion will concentrate exclusively on Huawei's role as vendor of 5G equipment to European and Spanish mobile network operators ("MNOs").

9. In 2019, Huawei's sales revenue reached 858.8 billion Chinese yuan (approximately 123 billion USD), with net profits of 62.7 billion Chinese yuan (approximately 8.97 billion USD) and an operating cash of 91.4 billion Chinese yuan (approximately 13.1 billion USD).

10. Huawei's value chain, while concentrated in China, spans other parts of the world, as it has outside China manufacturing plants in Hungary (Budapest), Munich (Germany), India (Chennai) and, in the immediate future, France.

11. While Huawei has competitors in all of the market segments where it operates (including, for instance, US Apple or the Chinese ZTE), as supplier of 5G equipment to European MNOs it has essentially two main competitors:

    - Ericsson, a global provider of information and communication technology to telecom operators based in Stockholm (Sweden); and

    - Nokia, a global vendor in the network and IP infrastructure, software, and the related services market based in Espoo (Finland).

2.2. R&D

12. In all likelihood, Huawei's remarkable growth and business success has been driven by its huge effort at R&D. For instance, according to Huawei's 2019 Annual Report, in 2019 over 10% of its revenue was invested into R&D (i.e. around 18,9 billion USD). And during the last decade, cumulative R&D expenditures exceeded 86 billion USD. In 2019, it had 96,000 employees (i.e. almost half its total workforce) dedicated to R&D.

13. If we compare R&D expenditures across companies, for the period 2018-2019 he 2019 EU Industrial R& Investment Scoreboard showed Huawei, with an estimated R&D annual expenditure of €12.7 billion, ranked 5th of the world, right ahead of US Apple and Intel, with Nokia (€4 billion, 36th) and Ericsson (€ 3.4 billion, 46th) lagging well behind[4].

14. Huawei argues that by not having external shareholders and not being publicly listed, it can concentrate on investing into mid-to long-term R&D and innovation, rather than focusing on short-term profits or share prices.

[4] See "The 2019 EU Industrial R&D Investment Scoreboard", December 18, 2019, available at https://iri.jrc.ec.europa.eu/scoreboard/2019-eu-industrial-rd-investment-scoreboard

15. Huawei is shifting from an innovation in technology, engineering, products, and solutions to breakthroughs in basic theory and developing new basic technologies.

16. As a consequence of that huge R&D effort, Huawei has more than 85,000 active patents, (including more than 40,000 granted in Europe and the US).

2.3. Corporate structure and governance

17. According to Huawei's documents and official statements, Huawei is a private company owned by its employees.

18. Through the *Union of Huawei Investment & Holding co., Ltd*. ("Huawei's Union", for short) they implement an Employee Stock Ownership Plan (ESOP) involving 104,572 employees. Only Huawei's employees are eligible to participate. No government agency or outside organization holds shares in Huawei. The only other direct or "registered" shareholder is Mr. Ren, the company's founder, who has a 1.01% direct stake in Huawei (and a combined one of nearly 1.14 %, including its indirect participation through the ESOP.

19. Huawei explains that China's Company Law sets a limit of 50 shareholders for all limited liability companies. Thus, to allow for the participation of such huge number of employees in its capital, Huawei, as many other Chinese companies, had to channel its employees' participation through Huawei's Union, a legal entity registered with the Shenzen Federation of Trade Unions. Huawei's Union plays thus a dual role: as a "trade union", as defined by China's Trade Union Law, on the one hand, and as a shareholder, as defined by China's Company Law, on the other, which serves as a collective platform allowing Huawei's employees to own "virtual shares" in Huawei. Those two separate roles are fully independent from each other, with the first one being managed by a "trade union committee" and the second one by the "Representatives' Commission".

20. Huawei prides itself of having a robust corporate governance system[5]. Shareholding employees elect, on a one-vote-per-share basis, 115 representatives, for a 5-year term, to form the Representatives' Commission, Huawei's highest decision-making body. This Commission makes decisions on major company matters, like profit distribution or capital increases.

21. Huawei stresses that even if its employees do not own "direct shares" of Huawei -i.e. they are not "registered" as Huawei's shareholders-, they own "virtual restricted shares" (through Huawei's Union), which have political and economic rights and, thus, are not just a mere profit-sharing plan. According to Huawei, only Chinese employees are currently eligible to participate in the ESOP, because of foreign exchange controls in China, but Huawei is exploring the possibility of allowing non-Chinese employees to participate in the ESOP as well.

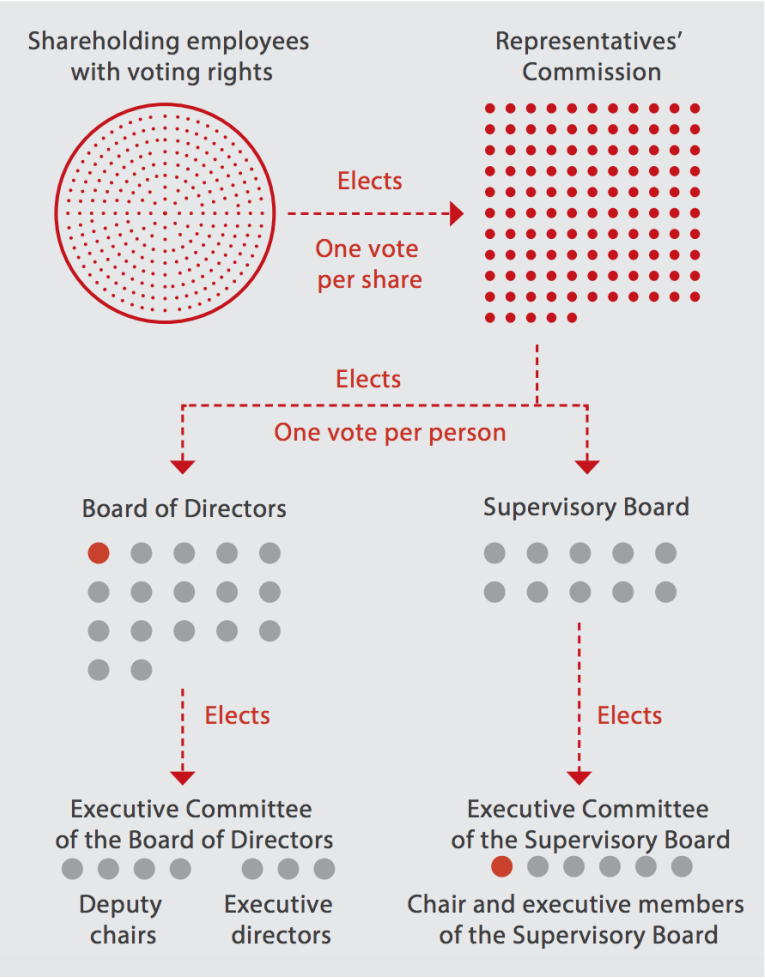
22. The Representatives' Commission also elects the Chairman of the Board of Directors -who also serves as the Commission's chairman- and the remaining 16 Board directors. The Board of Directors, in turn, elects four deputy chairs and three executive directors, who form

[5] https://www.huawei.com/en/about-huawei/corporate-information

together the Executive Committee. Three of these deputy chairs take turns serving as the Executive Committee's chairman (hence, the "rotating chairman" plays a role similar to a Western CEO, even if only for 6-month periods).

23. Each rotating chairman serves for six months. This peculiar rotating system reflects the company's "collective leadership model", which ensures that the company's fate is not tied to any single individual. Huawei explains that this rotating system mimics bird migration patterns, where birds change their position in the formation to take turns leading the flock across the ocean.

24. The following diagram, taken from Huawei's 2019 Annual Report, summarizes the governance system:



25. The rotating chairman leads the Board of Directors and its Executive Committee. The Board exercises decision-making authority for corporate strategy and operations management, and is the highest body responsible for corporate strategy, operations management, and customer satisfaction.

26. As Huawei's founder, Mr. Ren has the right to veto certain matters in order to uphold the company's common values and long-term direction, a right which he has never exercised and does not apply to routine or management decisions.

27. As explained in section 8.1.1 of this Opinion, Huawei's official view on its ownership and governance structure has been challenged by some external analysts.

2.4. Compliance

28. Huawei prides itself of conducting business with integrity, observing international conventions and all applicable laws and regulations in the countries and regions where it operates.

29. According to the reviewed documentation, Huawei has implemented a comprehensive compliance system in line with international best practices and has set up dedicated compliance and oversight teams to further bolster the management and oversight of its global business operations. It has drafted handbooks with the purpose of ensuring compliance with local ICT laws and regulations after analyzing local requirements, as well as requirements raised by industry associations, in more than 100 countries where Huawei has a business presence. Huawei has compliance officers in all its European subsidiaries, including Spain.[6]

2.4.1. Huawei's Global Cyber Security and Privacy Protection Office

30. As part of its effort to comply with the strictest standards for the protection of cyber-security and privacy, and assuage any fears of its overseas customers on that front, Huawei has set up a Global Cyber Security & Privacy Protection Office ("GSPO Office") led by a Global Cyber Security Protection Officer (GSPO), reporting directly to the Rotating Chairman. The current GSPO is Mr. John Suffolk, who is based in the UK.

31. The GSPO Office is responsible for building comprehensive end-to-end cyber security and privacy protection mechanisms for customers, pushing relevant departments to incorporate cyber security and privacy protection requirements into process management and business decision-making systems, and auditing.

32. The functions of the GSPO also include:

- Running the Independent Cyber Security Lab ("ICSL").

  The ICSL is a security verification organization independent of business teams and of the R&D departments that was established in 2012. It has been certified under ISO 17025. It uses the Cyber Security Evaluation Methodology ("CSEM") based on security threats and risks to conduct independent security testing on Huawei's products. The evaluation report released by the ICSL serves as the basis for making product launch and release decisions. If the ICSL test finds that a product has high security risks, the test results will support the GSPO to veto the product launch. The ICSL is transparent to its customers as its test platforms, tools, evaluation methods, and results are open to them as required.

[6] https://www.huawei.com/en/about-huawei/sustainability/win-win-development/develop_honesty

- Carrying out source code verification services. For this purpose, Huawei established several transparency centres so that customers can inspect Huawei's source code in these locations, as discussed below.

2.4.2. Huawei's third-party security mechanisms

33. According to Huawei's documentation, Huawei provides customer security assurance not only through the independent testing and evaluation of its products by Huawei's ICSL, but also through external third-party security testing labs and certification entities.

34. As will be explained in more detail below, Huawei claims that "is the most open, most evaluated, and most transparent ICT company in the world, and is subject to comprehensive verifications by expert teams from governments, customers and third parties. Huawei is also the only company in the telecom sector that is willing to have its source code reviewed".

35. In the specific case of Spain, since 2010 Huawei has got certifications from the National Cryptologic Centre ("NCC") and its accredited laboratories. Currently, 25 Huawei products have passed Common Criteria certifications in Spain, including the 5G RAN solution while 10 products are still undergoing the evaluation process, including the 5G Core solution. Moreover, two Huawei development sites have also been certified as secure development sites since 2013.

2.5. Huawei in Europe

2.5.1. Huawei's role in European 4G networks

36. Huawei won its first mayor contract in Europe with the Dutch mobile operator Telfort in 2004. A year later, Huawei was selected as one of the strategic suppliers for British Telecom's twenty-first century network programme. By the end of 2007, Huawei was able to secure contracts with all major network operators in Europe. In 2014, Vodafone announced that it had awarded Huawei the contract to upgrade its networks in 15 countries in Europe and Africa. Currently, Huawei is part of the deployment of 5G networks in Italy, Monaco, the Netherlands, Finland, the United Kingdom, Switzerland, Spain, etc.

37. In February 2020, Huawei announced the construction of a 4G/5G equipment factory in France. This facility is expected to require an investment of more than 200 million euros.

38. As is also the case in other countries, European countries and MNOs are planning to create their 5G networks not from scratch as "Stand Alone" (SA) 5G networks, but on top of existing 4G networks, i.e. as "Not Stand Alone" (NSA) 5G networks.

39. Hence, in the case of most European countries, including Spain, Huawei has already supplied equipment embedded in existing 4G networks, such that restrictions on Huawei's involvement in the development of European 5G networks might represent a significant setback for operators, as will be indicated below.

2.5.2. Huawei's Transparency Centres

40. As part of its policy of ensuring its customers' trust in the reliability and cyber-security of its products, Huawei has created Transparency Centres in Europe, which are open to customers and independent third-party testing organizations, and facilitate objective and independent security tests and verifications according to industry-recognized cyber security standards and best practice.

41. There are three Transparency Centres:

- The first one was the Huawei Cyber Security Evaluation Centre ("HCSEC") in the UK in November 2010.

  As explained below, the HCSEC opened under a set of arrangements between Huawei and the UK's Government to mitigate any perceived risks arising from the involvement of Huawei in parts of the UK's critical national infrastructure. HCSEC provides security evaluation for a range of products used in the UK telecommunications market. Through HCSEC, the UK's Government is provided with insight into Huawei's UK strategies and product ranges.

- A second one was set up in Bonn (Germany) in November 2018.

  The centre works closely with German customers, partners, research institutions as well as government and supervisory authorities. Within this framework, a close and regular cooperation between the German Federal Office for Information Security and Huawei is planned and focuses on new technologies (especially 5G, artificial intelligence, IoT and Smart Cities, standardization (like 3GPP) as well as the verification of product safety.

  The German centre's objective is to explore and standardize industry security standards and specifications, discuss innovative security concepts for future technologies, and facilitate Huawei's collaboration and dialogue with the German Federal Office for Information Security and industry partners.

- The most recent was established in Brussels, Belgium, in March 2019.

  This Centre provides a technical verification and evaluation platform for Huawei's customers, including source code verification It aims at addressing European objectives and needs, as well as sharing important technical information on Huawei's solutions to cyber security threats and vulnerabilities. In addition, the Centre also collaborates with industry organizations and standard organizations to promote and develop security standards and verification mechanisms. Furthermore, it collaborates and innovates jointly with the EU cyber security verification organizations.

2.5.3. Huawei's compliance with the GDPR

42. One of the relevant existing regulatory frameworks and instruments mapped in the EU Toolbox is Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal

data and on the free movement of such data ("General Data Protection Regulation" or "GDPR").

43. The GDPR is not only the main piece of legislation which governs the European fundamental right of the protection of natural persons in relation to the processing of personal data but it has also become an international standard in terms of compliance with processing activities and the security of processing.

44. The GDPR adopts a so-called "risk-based approach" of compliance according to the "accountability" principle which requires the implementation of appropriate technical and organisational measures according to the risks of varying likelihood and severity to the rights and freedoms of natural persons (article 24 in relation to article 5 of the GPPR).

45. Huawei has implemented a comprehensive GDPR-compliance scheme based on industry standards - encompassing all relevant elements, including the Privacy Impact Assessment ("PIA") methodology set out in article 35 GDPR into all its business processes. Huawei builds privacy protection requirements into the design of each business process through PIAs.

46. Concerning organizational measures, one of these key measures set out in the GDPR and in Spain's Data Protection Act for network operators and communication digital service providers is the appointment of a Data Protection Officer ("DPO") who should be in a position to perform his duties and tasks in an independent manner.

47. During the author's assessment, Huawei confirmed that it has in place the organizational accountability measures required by the GDPR and that the company has appointed an independent EU DPO as defined in article 37 and 38 of the GDPR. Huawei's DPO's Office is located in Düsseldorf (Germany) and lead by Mr. Joerg Thomas as Director of Huawei's DPO Office.

48. Mr. Thomas has confirmed that, as required by the GDPR, the DPO does not receive any instructions regarding the exercise of his tasks, that he cannot be dismissed or penalised for performing his tasks and that he reports to the highest management level (the Rotating Chairman) through the Global Cyber Security and Privacy Protection Committee ("GCSPC").

49. Huawei's DPO's "jurisdiction" extends to the processing of EU personal data at Huawei within the EU and outside the EU where the GDPR is applicable. His tasks, as per article 39 GDPR, include:

    - Being the contact point for the European Data Protection Supervisory Authorities ("DPAs").

    - Approving proactive communication with DPAs.

    - Monitoring and auditing Data Protection Compliance.

    - Monitoring performance of Data Protection Impact Assessments ("DPIAs").

    - Monitoring Data Breach handling and notification.

- Providing Data Protection guidance and advice.
- Maintaining a DPO mailbox and privacy whistleblowing hotline.
- Reporting to leadership.
- Supporting external communication.

2.5.4. The UK's HCSEC and Oversight Board

2.5.4.1. The HCSEC

50. As already explained, the HCSEC opened in November 2010, under a set of arrangements between Huawei and the UK's Government to mitigate any perceived risks arising from the involvement of Huawei in parts of the UK's critical national infrastructure.

51. The HCSEC is a facility in Banbury, Oxfordshire belonging to Huawei Technologies (UK) Co. Ltd. and for the last ten years it has been providing understanding and technical security artefacts to the UK operators and to the UK's National Cyber Security Centre (NCSC)

52. In that regard, the most recent report of the NCSC to the Oversight Board stated that HCSEC continued to "provide unique, world-class cyber security expertise to assist the Government's ongoing risk management programme around the use of Huawei equipment with the UK operators".

53. The NCSC's objective is to require HCSEC to perform a product evaluation on every relevant product in the UK at least every two years.

54. The HCSEC's priorities are set collaboratively by UK operators, NCSC and HCSEC, not allowing that any operator unfairly dominates the program of work due to commercial pressures. The final program is signed off by the NCSC Technical Director for Telecommunications on behalf of the Oversight Board and kept under review during the year by HCSEC.

55. The HCSEC's evaluation process has occasionally uncovered both point vulnerabilities and more strategic architectural and process issues, requiring remediation work by Huawei. However, as indicated below, the HCSEC's Oversight Board has confirmed Huawei's close engagement in the verification process of its equipment and in the remediation work needed to fix the technical glitches discovered. The feedback provided by HCSEC to UK operators, to the NCSC and to Huawei's R&D department has assisted the latter in their remediation efforts.

2.5.4.2. The Oversight Board

56. The HCSEC Oversight Board was established in early 2014. The role of the Oversight Board is to oversee and ensure the independence, competence and overall effectiveness of HCSEC as part of the overall mitigation strategy in place to manage the risks presented by Huawei's presence in the UK and to advise the National Security Adviser on that basis. The National

Security Adviser will then provide assurance to Ministers, Parliament and ultimately the general public as to whether the risks are being well managed.

57. The Oversight Board is chaired by Ciaran Martin, the Chief Executive Officer of the NCSC, and an executive member of GCHQ's Board with responsibility for cyber security. The Oversight Board also includes a senior executive from Huawei as Deputy Chair, as well as senior representatives from across the Government and the UK telecommunications sector.

58. The Oversight Board's scope relates to products that are relevant to UK national security risks. It covers

    i) the HCSEC's assessment of Huawei's products that are deployed or are contracted to be deployed in the UK and are relevant to UK national security risk which is determined at the NCSC's sole and absolute discretion; and

    ii) the independence, competence and therefore overall effectiveness of HCSEC in relation to the discharge of its duties.

59. The Oversight Board is responsible for providing an annual report to the National Security Adviser, who will provide copies to the National Security Council and the Intelligence and Security Committee of Parliament. The Oversight Board's four high-level objectives for HCSEC have remained consistent and are:

    - To provide security evaluation coverage over a range of UK customer deployments as defined in an annual HCSEC evaluation programme.

    - To continue to provide assurance to the UK Government by ensuring openness, transparency and responsiveness to Government and UK customer security concerns.

    - To demonstrate an increase in technical capability, either through improved quality evaluations output or by development of bespoke security related tools, techniques or processes.

    - For HCSEC to support Huawei Research and Development to continue to develop and enhance Huawei's software engineering and cyber security competence.

60. In his most recent Report, the Oversight Board makes several important statements:[7]

    - "3.8 NCSC continues to believe that the UK mitigation strategy, which includes HCSEC performing technical work and the Oversight Board providing assurance as two components, is the best way to manage the risk of Huawei's involvement in the UK telecommunications sector. The discovery of the issues exposed in this report are an

[7] "Huawei Cyber Security Evaluation Center (HCSEC) Oversight Board Annual Report 2019", A report to the National Security Adviser of the United Kingdom , March 2019 available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf

indication of the model working properly. Huawei currently continues to engage with this process".

- "3.10 HCSEC continues to have world-class security researchers who are creating new tools and techniques to provide the UK community understanding of the software engineering and cyber security implications of Huawei's unique software engineering and cyber security processes in the complex sphere of telecommunications".

- "3.13 The significant risk in the UK telecommunications infrastructure brought about by Huawei's equipment will continue to need to be managed by the UK operators and significant work will be required from all parties involved to reduce that risk in existing equipment over time. NCSC and the UK operators will continue to work with Huawei to create a credible and sustainable remediation plan for the equipment in the UK. Huawei has agreed that the remediation of the equipment in the UK is independent of any other work Huawei may do and will occur in a timely manner".

- "3.15 The NCSC believes that HCSEC remains competent in the areas of technical security necessary to advise the operators, NCSC and the Oversight Board as to the product and solution risks admitted by the use of Huawei products in the UK telecoms infrastructure. The NCSC's report to the Oversight Board is that HCSEC continues to provide unique, world-class cyber security expertise to assist the Government's ongoing risk management program around the use of Huawei equipment with the UK operators".

61. Subsequent to that report, in its "Security analysis for the UK telecoms sector", the NCSC highlighted again the importance attached to the role played by the HCSEC:[8]

> "*The existence of HCSEC provides the NCSC and Her Majesty Government with clear and unbiased evidence on the risks posed to the UK through the use of Huawei's products by UK operators. It ensures that it is feasible that embedded malicious functionality could be detected should it exist. HCSEC deploys a range of tools and AI to scan Huawei's UK products, complemented by skilled analysts.*
>
> *Due to the UK's mitigation strategy, which includes HCSEC as an essential component, our assessment is that the risk of trojan functionality in Huawei equipment remains manageable. Placing 'backdoors' in any Huawei equipment supplied into the UK is not the lowest risk, easiest to perform or most effective means for the Chinese state to perform a major cyber- attack on UK telecoms networks today*".

2.6. Huawei in Spain

2.6.1. Huawei's business in Spain

62. Huawei launched its operations in Spain in 2001, through a commercial representative office, to further develop its business as a key ICT supplier. Shortly thereafter, underlining

[8] NCSEC, "Security analysis for the UK telecoms sector. Summary of findings", January 2020, par.8.4.2 at p.22.

its intention to expand in the Spanish market, a full-fledged subsidiary, "Huawei Technologies España" (henceforth, "Huawei Spain"), was created.

63. Huawei Spain has around 1,000 employees, 80% Spanish nationals, 5% Chinese and 15% from all over the globe. Its head office is in Madrid, along with five further offices in Barcelona, Valencia, Sevilla, La Coruña and Bilbao.

64. Huawei works with all of Spain's main network operators and has provided mobile (3G, 4G, etc.), fixed network (fiber access, transport, etc), and ICT equipment or services to, among others, Telefónica, Vodafone, Orange, MásMovil, etc.

65. As part of its retail business, it has opened big flagship stores in Madrid and Barcelona.

66. Huawei also has many private corporate customers in Spain, including leading listed companies Santander Bank, BBVA and Caixa Bank; energy companies Repsol, Cepsa and Naturgy, or Spain's leading department stores El Corte Inglés.

67. Huawei also has various joint innovation centres in Spain with Mobile Network Operators ("MNOs") Telefónica and Vodafone.

68. Huawei participates in several boards and associations commissions related to the ICT sector, such as the Spanish Confederation of Business Organizations[9] ("CEOE" as per its Spanish initials) or DIGITALES.

69. As indicated, Huawei has been actively involved in the construction of Spain´s 4G network, supplying passive and active antennas, base stations, optical and IP transport networks, core network solutions (traditional and virtualized), IT equipment (computing servers, storage, networking switches) for Cloud/virtualized Core and Edge Solutions), Business Support Systems and Operation Support Systems or associated services, among others.

70. Huawei has not only been involved in the established of Spain's 4G networks, but has taken the lead in the development of 5G in Spain, being the only supplier that, until May 2020, has contributed to the two 5G pilot projects selected by Red.es, namely one led by Vodafone[10] in Andalusia for 25.4 million euros, and another led by Telefónica[11] in Galicia for 11.5 million euros. In both projects Huawei provides 5G end-to-end solutions.

71. In June 2019, Vodafone announced the arrival of 5G's commercial deployment in 15 cities in Spain with Huawei's team as the main contributor. Vodafone Spain also markets the Huawei Mate 20X in Spain, the first Huawei device to support 5G.

[9] https://www.ceoe.es/en/contenido/huawei-spain-becomes-a-member-of-the-spanish-confederation-of-business-organizations-ceoe
[10] https://www.red.es/redes/es/actualidad/magazin-en-red/redes-impulsa-la-puesta-en-marcha-del-proyecto-piloto-5g-en-andaluc%C3%ADa
[11] https://www.telefonica.com/es/web/sala-de-prensa/-/se-pone-en-marcha-el-proyecto-piloto-5g-en-galicia-impulsado-por-red-es

2.6.2. Relations with public authorities

72. Huawei Spain and the Spanish National Institute of Cybersecurity ("INCIBE") signed, within the framework of the Mobile World Congress held in Barcelona in 2016, a Memorandum of Understanding for collaboration in which both organizations are committed to promote cybersecurity in Spain. This was the first agreement of that nature that Huawei signed in a European country[12].

73. As part of the joint roadmap set out by that Memorandum, Huawei Spain and INCIBE established the following targets: to create mechanisms for a periodic information exchange on cybersecurity matters; to foster the sharing of methodologies to improve cybersecurity; to share knowledge within this area and to support the training and qualification of the Spanish companies and professionals in this area.

3. Spain´s 5G project

3.1. Spain´s current telecoms network

74. Spain has one of the largest mobile markets in Europe, with effective competition from four MNOs and a good number of resellers and Mobile Virtual Network Operators ("MVNOs"). This competition has driven down the cost of mobile services for end users while the investment in network infrastructure has also been able to cope with the continuous increase in mobile data traffic year on year. Vodafone Spain was the first operator to launch a 5G network, in June 2019.

75. Spain has four main MNOs: Telefónica, Vodafone, Orange and MásMovil. According to publicly available information of the CNMC, during the first trimester of 2019, the three main telecommunications operators accounted for 77.1% of the sector's retail revenues.[13]

3.2. Spain´s 5G roadmap

76. On the basis of the input gathered from the public consultation held in July 2017, the Ministry of Energy, Tourism and Digital Agenda developed Spain's 5G National Plan for the 2018-2020 period (the "5G National Plan"). The 5G National Plan aims at placing Spain amongst the most advanced countries in developing this technology.

77. A total of 31 5G pilot tests are being carried out, more than in any European country, with 40 use cases in the first call, with the pilot tests of Telefónica in Galicia and Vodafone and Huawei in Andalusia. Both pilot tests started in May 2019 and are scheduled to end in December 2020.

78. While, in preparation for the launch of the 5G networks, the auction of the 3.6-3.8 GHz spectrum took place in July 2018 -it raised 438 million euros-, the 700 MHz auction -particularly interesting, given its wide coverage, to cover sparsely populated territories-, initially scheduled for the first half of 2020, was subsequently postponed to 2021, due in part to the Covid-19.

[12] https://www.huawei.com/en/press-events/news/2016/2/Huawei-Spain-and-INCIBE-sign-a-MoU
[13] Movistar accounted for 42.6%, Orange for 17.7% and Vodafone for 16.8%.

79. The 470 to 790 MHz frequency band was to be released in EU member countries by June 30, 2020 at the latest for wireless broadband electronic communications services. However, due to the exceptional situation derived from the Covid-19 pandemic, Spain communicated to the European Commission the need to postpone the date of June 30 to complete the release of the second digital dividend.

3.3. Huawei as 5G supplier

80. Huawei has the technology and the ability to supply 5G base stations (antennas –both active and passive–), radio units, base bands, energy equipment cabinets, optical transports, IP routers, core networks NFV, core networks IT infra (computing, storage, switching), edge computing platforms (MEC), indoor coverage solutions, small cell solutions, data centre infrastructures (cooling, energy, UPS…), customer premise equipment user devices, etc.

81. Huawei also has the manpower to supply

- post-sales support services (i.e., incident resolution and hardware and software upgrades);
- operation and maintenance services (both on hardware and software): and
- deployment services (installation, integration or optimization, among others).

4. Political concerns about Huawei

4.1. Western suspicions about Chinese companies

82. The general apprehension that the economic ascendancy of Chinese companies has spontaneously raised in Western countries has been traced by one American Scholar, Sophie Meunier, to two main factors: [14]

- The central role of the Chinese state in the economy.

  "*Even in the case of transactions conducted by private investors, doubt persists as to the actual influence of the Chinese government and Communist Party. This has been an issue, for instance, with efforts to invest in the U.S. by Huawei, a private company, whose owner is rumored to entertain very close links with the Chinese government*".

- China is not a security ally.

  "*The United States and European countries are not used to receiving investment from countries which are not their security allies. The Soviet Union did not invest in*

[14] Sophie Meunier, "Beware of Chinese Bearing Gifts: "Why China's Direct Investment Poses Political Challenges in Europe and the United States", in "China's Three-Prong Investment Strategy: Bilateral, Regional, and Global Tracks", Julien Chaisse ed. Oxford University Press, February 2019.

the West during the Cold War. To be sure, China is not an enemy but rather a superpower with avowed geopolitical ambitions and foreign policy goals often at odds with those of the U.S. and some European countries. This raises several causes for concern about the ultimate motive of investment, including issues of dual-use technology and strategic leverage".

4.2. 5G-related geopolitical concerns

83. In the specific case of Huawei, political fears in Western countries have been compounded by its leading role in the development of 5G technology, coupled with the enormous potential of 5G.

84. 5G may indeed be a critical enabler that could bring with it new applications and opportunities that cannot yet be imagined. The main advantages of the 5G are a greater speed in the transmissions, a lower latency and therefore greater capacity of remote execution, a greater number of connected devices and the possibility of implementing virtual networks, providing more adjusted connectivity to concrete needs.

85. Even if there is no evidence that 5G is generally less secure than the current 4G networks, the complexity of 5G networks poses a security challenge. From a political perspective, two main potential cybersecurity risks have been described:

- The malicious planting in 5G equipment and software programs of spyware, hardware trojans or "backdoors" for political espionage purposes.

  Spyware is unwanted software that infiltrates your device, stealing internet usage data and sensitive information. Spyware is used for many purposes. Usually, it aims to track and sell your internet usage data, capture your credit card or bank account information, or steal your personal identity.

  Hardware Trojans, also known as Trojan circuits, are modifications of integrated circuits in computer chips that can give third parties access to data.

  A backdoor, in cybersecurity terms, is a method of bypassing security controls to access a computer system or encrypted data. While backdoors can be common in some network equipment and software because developers create them to manage the gear, they can be exploited by attackers.

- The malicious planting of sabotage devices (occasionally described with the popular, colourful term of "kill switches") to produce wilful disruptions or outages of 5G networks, including massive Distributed Denial of Services (DDoS).

86. The political concerns extend not only to the initial manufacturing and design of equipment and programs, but also to their subsequent maintenance, updates and patches.

87. The fact that Huawei is a Chinese company with headquarters in China, not listed in international capital markets and owned by Chinese nationals -Huawei's employees- has raised in the US and in other Western countries -particularly in those belonging to the so-

called Five Eyes intelligence alliance (i.e. Australia, New Zealand, Canada and the UK), concerns as to who controls Huawei and whether it is, or could become, a tool which could be controlled or used by the Chinese political authorities or the Chinese Communist Party (CCP) and become an instrument of China's foreign policy.

4.3. US special fears about Huawei

88. In the case of Huawei and the US, irrespective of any fears about new cybersecurity risks in 5G networks, there is probably a much deeper concern about its technological prowess and leadership, due to the fact that "Huawei has taken an early lead in developing the next generation of wireless technology, 5G, with its promise of quantum leaps in connectivity. Should Huawei maintain and extend that lead while also advancing on other fronts, it and, by extension, China could be first to produce a new generation of sensitive military systems, smart grids, autonomous transportation vehicles and other crucial products and processes. The U.S. worries that such a shift in the balance of power between it and China threatens its national security".[15]

89. In other words, US political concerns about Huawei are not related exclusively to 5G risks: they are probably a reflection of China's technological edge over Western countries, and the challenge that this may pose, over the medium term, to US international dominance.

90. Probably as a consequence of those fears, the Trump Administration´s reaction has been mostly directed to crippling the Chinese company's international ambitions, in one episode of what scholars have come to describe as a modern US-China version of the so-called "Thucydides trap", i.e. the century conflict among the two leading Greek city-states of Sparta and Athens that historian Thucydides explained in these terms: "It was the rise of Athens and the fear that this instilled in Sparta that made war inevitable".[16]

91. Measures launched by the Trump Administration against Huawei include:

- Charging Huawei's chief financial officer, Mrs. Meng Wanzhou, Ren's daughter, with fraud and sanctions violations, and seeking her extradition from Canada.

- Forbidding not only US companies, but also companies located in other countries but with US suppliers, to conduct certain types of business with Huawei.

- Demanding that governments and companies around the world stop buying or using Huawei products and equipment and threatening Western allies which fail to do so with adverse consequences, like stopping sharing intelligence information or withdrawing military forces.

[15] Norman Pearlstine, David Pierson Robyn Dixon, David S. Cloud, Alice Su &Max Hao Lu, "The Man Behind Huawei", Los Angeles Times, April 10, 2019 available at https://www.latimes.com/projects/la-fi-tn-huawei-5g-trade-war/

[16] Graham Allison, "Destined for War. Can America and China escape Thucydides's trap?", Scribe, 2017.

92. By way of illustration of these political pressures brought to bear by US on its allies, US Senator Tom Cotton expressed himself in these terms in his recent testimony to the UK Parliament:[17]

> "*I understand that the UK Government has been advised that the threat from Huawei can be contained if it is kept away from sensitive facilities in the so-called core of your network. I will not wade too deeply into that technical debate, but I will note that our own technical experts disagree, as do the experts in allied democracies like Australia and Japan. These same experts also warn that Huawei could help China obtain a host of damaging information, from details about how our aircrews fight to intrusive personal information about our airmen themselves. They warn of scenarios where the Chinese Communist party could acquire compromising details about American forces stationed in your country.*
>
> *[…]*
>
> *China is a graver long-term threat to international peace and stability than Russia is, so, in the coming years, the United States plans to increase our defense posture in the Pacific. That build-up may require us to ship assets from other commands. The case for a heavy lay-down of air force assets in England rather than, say, Alaska, Hawaii, Guam or Japan was already contested in our debates in Washington. Now, senior US officials are realizing our troops will face an operational security risk in the United Kingdom, that they would not otherwise face in the Pacific*".

93. When UK's MP Mr. Kevan Jones retorted that " It is very clear from GCHQ and our security agencies that there is no way that Huawei equipment will come anywhere near anything in terms of our signals intelligence, or impact on yours", Senator Cotton's replied:

> "*5G technology is such a technological leap beyond 3G and 4G technology. It is so central to the way economies will function in the future and the way our countries will secure themselves that I believe using Huawei technology, using ZTE technology or using any technology from a company that is beholden to the Chinese Communist party would be as if we had relied on adversarial nations in the cold war to build our submarines or our tanks—it is just not something that we would have ever considered. There are certain technologies that are so sensitive and so integral and vital to our prosperity and security; we would never use an adversarial nation for such technology*".

94. US economist Jeffrey D. Sachs has criticized the approach of the Trump Administration towards Huawei and dub it a new illustration of what he calls the "Cheney doctrine":[18]

---

[17] House of Commons, Defense Sub-Committee, "The security of 5 G", witness testimony of US Senator Mr. Tom Cotton, June 2, 2020, available at Available at https://committees.parliament.uk/oralevidence/448/html/.

[18] Jeffrey D. Sachs, "America's War on Chinese Technology", Project Syndicate, November 7, 2019, available at https://leaders.economicblogs.org/project-syndicate/2019/d-sachs-america-war-chinese-technology-2/.

"*In the run up to the Iraq War, the US-Vicepresident Richard Cheney declared that even if the risk of weapons of mass destruction falling into terrorist hands was tiny, say 1%, we should act as if it were certain by invading. The US is at it again, creating a panic over Chinese technologies by exaggerating tiny risks.*

The problem with the Cheney Doctrine is not only that it dictates taking actions predicated on small risks without considering the potentially very high costs. Politicians are tempted to whip up fears for ulterior purposes.

That is what US leaders are doing again: creating a panic over Chinese technology companies by raising, and exaggerating, tiny risks. The most pertinent case (but not the only one) is the US Government attack on the wireless broadband company Huawei. The US is closing its markets to the company and trying hard to shut down its business around the world. As with Iraq, the US could end up creating a geopolitical disaster for nor reason".

4.4. The UK's position on Huawei

95. In January 2020, the UK's government announced that Huawei would be permitted to supply equipment for "non-core" parts of the 5G network and that its presence would be capped at 35% of the market share in the radio access.

96. However, on May 26, 20202 the CNBC[19] informed that the UK's NCSC had launched an emergency review of Huawei's role in the U.K. after the U.S. introduced new sanctions on the company.

97. According to the Financial Times, Vodafone has warned that the UK's hopes of leading the world in 5G technology would be dealt a terminal blow if the government removes Huawei from the country's telecoms infrastructure. In addition, the Financial Times also informs that, even though Huawei's equipment in the UK is central to delivering 5G, Boris Johnson is facing mounting pressure from Washington and from within his own government to exclude Huawei. [20]

98. It is beyond this Legal Opinion to take a view on these political developments. But they are mentioned just to indicate the high-political stakes in the US reaction against Huawei and to help explain their impact on the EU approach towards Huawei.

4.5. EU-China relations and EU "digital sovereignty" aspirations

99. While EU political relations with China had traditionally not been adversarial, in March 2019 the growing political concern about China was illustrated by the Communication to the Parliament and the Council on the strategic review of the relations between the EU and

[19] https://www.cnbc.com/2020/05/26/huawei-5g-ncsc.html
[20] https://www.ft.com/content/c2fd1c70-3eaa-4e80-8ad3-e88e7bec7d12

China presented by the High Representative of the Union for Foreign Affairs and Security Policy, Mrs. Federica Mogherini.[21]

100. Specifically, in Chapter IV ("Achieving a more balanced and reciprocal trade and investment relationship"), the Communication said:[22]

> "*China's proactive and state-driven industrial and economic policies such as 'Made in China 2025' aim at developing domestic champions and helping them to become global leaders in strategic high-tech sectors. China preserves its domestic markets for its champions, shielding them from competition through selective market opening, licensing and other investment restrictions; heavy subsidies to both state-owned and private sector companies; closure of its procurement market; localisation requirements, including for data; the favoring of domestic operators in the protection and enforcement of intellectual property rights and other domestic laws; and limiting access to government-funded programs for foreign companies. EU operators have to submit to onerous requirements as a precondition to access the Chinese market, such as creating joint ventures with local companies or transfer of key technologies to Chinese counterparts*".

101. In that spirit, the Communication called for "strengthening the Union's competitiveness and ensuring a level playing field" and argued that "the EU should foster industrial cross border cooperation, with strong European players, around strategic value chains that are key to EU industrial competitiveness and strategic autonomy".

102. In the same vein, Chapter V ("Strengthening the Union's competitiveness and ensuring a level playing field") argued that "In the context of the renewed industrial policy strategy, the EU should foster industrial cross border cooperation, with strong European players, around strategic value chains that are key to EU industrial competitiveness and strategic autonomy (…) To ensure the long-term competitiveness of EU operators, including in fields where EU enterprises do not enjoy reciprocal market access, the EU needs an ambitious Horizon Europe program open to third countries and international organisations to stay at the forefront of global research and innovation. It should also include clear rules on exploitation of results and allow for effective reciprocal access to research and development funding".

103. Right after these two chapters, final Chapter VI turns its focus to "strengthening the security of critical infrastructure and the technological base" and claims that "any vulnerability in 5G networks could be exploited in order to compromise such systems and digital infrastructure -potentially causing very serious damage. A range of EU instruments, including the Network and Information Security Directive, the recently approved Cybersecurity Act, and the European Electronic Communications Code will allow reinforcing cooperation in addressing cyber-attacks and enable the EU to act collectively in protecting its economy and society".

104. The Chapter ends by recommending as Action 9 that "to safeguard against potential serious security implications for critical digital infrastructure, a common EU approach to the security

[21] https://ec.europa.eu/commission/publications/eu-china-strategic-outlook-commission-contribution-european-council-21-22-march-2019_en

[22] European Commission, High Representative of the Union for Foreign Affairs and Security Policy, "Joint Communication on EU-China-A Strategic Outlook", Strasbourg, 12.3.2019, JOIN(2019) 5 final, pg. 5

of 5G networks is needed. To kickstart this, the European Commission will issue a Recommendation following the European Council".

105. This last announcement was the harbinger of the Commission's Recommendation on Cybersecurity in 5G Networks, to which we now turn.

5. The EU's Toolbox

5.1. The EU Coordinated Risk Assessment

106. A few days after the presentation of its Communication on the strategic review of the EU-China relations, on 26 March 2019 the Commission adopted a Recommendation on cybersecurity threats for 5G networks[23]. The Recommendation requested Member States to carry out national risk assessments that would form the basis of a common set of measures to mitigate 5G security risks, drawing on the strong EU legislative framework already in place to protect electronic communications networks. Recital 24 of the Recommendation calls for establishing a "toolbox" to "serve to advise the Commission on developing minimum common requirements to further ensure a high level of cybersecurity of 5G networks across the Union".

107. Based on these national risk assessments, on 9 October 2019, the NIS Cooperation Group, formed by representatives of Member States, the Commission and ENISA, published a report on the EU Coordinated Risk Assessment on Cybersecurity in 5G Networks (the "EU Coordinated Risk Assessment")[24] that identifies the main threats and threat actors, the most sensitive assets, the main vulnerabilities (including technical ones and other types of vulnerabilities) affecting 5G networks. On this basis, the EU Coordinated Risk Assessment also identified a number of categories of risks of strategic importance from an EU perspective illustrated by concrete risk scenarios, which reflect relevant combinations of the different parameters (vulnerabilities, threats and threat actors) with respect to the different assets.

108. To complement it and as a further input for the toolbox, ENISA carried out a dedicated threat landscape mapping[25], consisting of a detailed analysis of certain technical aspects, in particular the identification of network assets and of threats affecting them.

109. The EU Coordinated Risk Assessment provided the basis to identify mitigation measures that can be applied at national and European level.

[23] Recommendation (EU) 2019/534 on the cybersecurity of 5G networks, OJ L 88, 29.3.2019. This recommendation followed the mandate of European Council conclusions of 21 March 2019 calling upon the Commission to adopt a recommendation on a concerted approach to the security of 5G networks.
[24] https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security
[25] https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

5.2. The Toolbox's main elements

110. On 29 January 2020, the NIS Cooperation Group published the EU toolbox of risk mitigating measures[26].

111. The Toolbox starts by recalling that, as a major enabler for future digital services, 5G will play a key role in the development of our digital economy and society in the years to come. From personalised medicine to precision agriculture, from smart energy grids to connected mobility, 5G will potentially affect almost every aspect of EU citizens' lives. At the same time, due to its less centralised architecture, smart computing power at the edge, the need for more antennas and increased dependency on software, 5G networks offer more potential entry points for attackers. Therefore, ensuring the security of the EU's future 5G networks is of utmost importance.

112. While operators are largely responsible for the secure rollout of 5G, and Member States are responsible for national security, network security is an issue of strategic importance for the entire EU. A coordinated approach based on robust security measures at national and EU level will help Europe to remain one of the leading regions in the deployment of 5G.

5.2.1. Risks

113. The Toolbox identifies nine categories of risk ("R", for short) identified in the EU Coordinated Risk Assessment, including one specific category which is the focus of this Opinion:

- **R5** State interference through 5G supply chain.

5.2.2. Measures

114. After a long description of the EU legal instruments available to address these risks -to be discussed below-, the Toolbox describes a set of strategic and technical measures which EU Governments could use to address them. In Annex 1, it drills down on the description of such measures, drawing in some cases on criteria previously set out in the EU Coordinated Risk Assessment.

115. The most relevant "strategic measures" ("SM", for short) for the purposes of this Opinion are the following:

- SM01 Strengthening the role of national authorities.

- SM02 Performing audits on operators and requiring information.

- **SM03** Assessing the risk profile of suppliers and applying restrictions for suppliers considered to be high risk -including necessary exclusions to effectively mitigate risks - for key assets.

[26] https://ec.europa.eu/digital-single-market/en/nis-cooperation-group

- Establish a framework with clear criteria, taking into account the risk factors identified in paragraph 2.37 of the EU coordinated risk assessment and adding country-specific information (e.g. threat assessment from national security services, etc.), for national competent authorities and MNOs to:

    - Perform rigorous assessments of the risk profile of all relevant suppliers at national level and/or EU level (for example jointly with other Member States or other MNOs).

    - Based on the risk profile assessment, apply restrictions -including necessary exclusions to effectively mitigate risks- for key assets defined as critical or sensitive in the EU coordinated risk assessment report (e.g. core network functions, network management and orchestration functions, and access network functions).

- Take steps to ensure that MNOs have adequate controls and processes in place to manage potential residual risks, such as regular supply chain audits and risk assessments, robust risk management, and/or specific requirements for suppliers based on their risk profile.

According to paragraph 2.37 of the EU Coordinated Risk Assessment, the risk profiles of individual suppliers can be assessed on the basis of several factors, notably:

- The likelihood of the supplier being subject to interference from a non-EU country. This is one of the key aspects in the assessment of non-technical vulnerabilities related to 5G networks. Such interference may be facilitated by, but not limited to, the presence of the following factors:

    - A strong link between the supplier and a government of a given third country;

    - The third country's legislation, especially where there are no legislative or democratic checks and balances in place, or in the absence of security or data protection agreements between the EU and the given third country (in this context, several Member States attribute a higher risk profile to suppliers that are under the jurisdiction of third countries conducting an offensive cyber policy);

    - The characteristics of the supplier's corporate ownership;

    - The ability for the third country to exercise any form of pressure, including in relation to the place of the manufacture of the equipment.

- The overall quality of products and cybersecurity practices of the supplier, including the degree of control over its own supply chain and whether adequate prioritisation is given to security practices.

- SM05 Ensuring the diversity of suppliers for individual MNOs through appropriate multi-vendor strategies.

Ensure that each MNO has an appropriate multi-vendor strategy taking into account the technical constraints and interoperability requirements of the different parts of a 5G network:

- To avoid or limit any major dependency on a single supplier (or suppliers with a similar risk profile);

- To avoid dependency on suppliers considered to be high risk within the meaning of SM03.

116. As indicated at the beginning, this Opinion will concentrate exclusively on strategic measure 5 (SM05), without addressing the issue of diversity of suppliers (SM 05).

117. Among the "technical measures" ("TM", for short) recommended, there is also one relevant for this Opinion:

- TM09 Using EU certification for 5G network components, customer equipment and/or suppliers' processes.

  Under the EU cybersecurity certification framework, the Commission should publish the Union Rolling Work Programme for the development of the EU-wide certification schemes by July 2020. The Commission should consider including into the Union Rolling Work Programme relevant EU-wide scheme(s) for critical network components used in the 5G networks and/or for 5G customer equipment (for example, for eSIMs and related cryptographic material) under the EU certification framework.

  It should also be examined at a later stage whether the certification of supplier's process could also be added to the Union Rolling Work Programme.

5.2.3. Recommendations

118. The key recommendations of the Toolbox are the following:

I. All Member States should ensure that they have measures in place (including powers for national authorities) to respond appropriately and proportionately to the presently identified and future risks, and in particular ensure that they are able to restrict, prohibit, and/or impose specific requirements or conditions, following a risk-based approach, for the supply, deployment, and operation of 5G network equipment on the basis of a range of security-related grounds.

   They should, in particular:

   - Strengthen security requirements for mobile network operators (e.g. strict access controls, rules on secure operation and monitoring, limitations on outsourcing of specific functions, etc.);

   - 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);

- Ensure that each operator has an appropriate multi-vendor strategy to avoid or limit any major dependency on a single supplier (or suppliers with a similar risk profile), ensure an adequate balance of suppliers at national level and avoid dependency on suppliers considered to be high risk; this also requires avoiding any situations of *lock-in* with a single supplier, including by promoting greater interoperability of equipment;

II. The European Commission, jointly with Member states, should contribute to:

- Maintaining a diverse and sustainable 5G supply chain in order to avoid long-term dependency, including by:
    - Making full use of the existing EU tools and instruments, in particular through the screening of potential foreign direct investments (FDIs) affecting 5G key assets and by avoiding distortions in the 5G supply market stemming from potential dumping or subsidies; and
    - Further strengthening EU capacities in the 5G and post-5G technologies, by using relevant EU programmes and funding.
- Facilitating coordination between Member states regarding standardisation to achieve specific security objectives and developing relevant EU-wide certification scheme(s) in order to promote more secure products and processes.

5.2.4. Legal nature

119. The EU Toolbox could be broadly be described as a "soft law" instrument on cyber-security risks, meant to guide EU Member States, through recommendations, in the application of the extensive EU "hard law" regulating the telecommunications sector.

120. The Toolbox recognizes that it will be up to Governments to decide which measures they consider appropriate:

> "*In selecting which measures are necessary to pursue, individual Member States will decide on the suitability of the measure*".[27]
>
> "*How to use the toolbox. Step 3: Member State studies the corresponding recommended measures and mitigation plans and selects the measure(s) that will have the most effect and considers potential implementation factors, alone or with aligned Member State(s)*".[28]

[27] Toolbox, paragraph 5.2.
[28] Toolbox, Table 4, How to use the Toolbox.

121. The response of the European Commission to the question "are the Toolbox measures mandatory?", while not particularly illuminating and somewhat asymmetrical, confirms that the Toolbox does not contain mandatory rules:[29]

> "*The EU toolbox on 5G cybersecurity is a document prepared and agreed by the NIS Cooperation Group, which consists of representatives of all Member States authorities, the Commission and the EU Cybersecurity Agency. The development of a coordinated EU approach on 5G cybersecurity relies on the strong commitment by both Member States and the Commission to use and fully implement a key set of recommended measures. The toolbox sets out a precise and objective methodology to address the risks identified in the European risk assessment published in October 2019, while respecting national competences in this area.*
>
> *At the same time, the roll-out and operation of 5G networks is a matter of national security. Member States can go <u>further</u> than what is proposed in the toolbox where they identify a need to do so*".

122. The Toolbox, as the documents on which it draws, is a document basically agreed by national cyber-security authorities, describing extensively the 5G risks that have been identified and the potential strategic and technical measures for addressing them, but without any attempt to elucidate or discuss the potential legal and constitutional constraints that Member States, like Spain, might have to respect when considering some of the recommended strategic measures (including, specifically, when carrying out the assessment of suppliers described as SM03).

6. The legal framework on 5G networks

123. In this Section a legal analysis will be made of the mandatory rules, both European and domestic, applicable to Spain's telecommunication networks.

124. The key take-away of the analysis will be that Spain has a robust legal and regulatory framework, which endows Spanish authorities with all the powers suggested by the EU Toolbox. Their rigorous enforcement powers -which allow them to impose heavy fines and corrective measures- can operate as a highly effective risk mitigator.

6.1. The three basic regulatory frameworks

125. As indicated in the EU-wide Coordinated Risk Assessment of 5G Networks and in the EU Toolbox, mandatory rules on security requirements relevant for the 5G networks ecosystem and related critical systems are set out in three main EU regulatory frameworks:

- The EU Telecommunication framework.
- The NIS Directive.
- The Cybersecurity Act (Regulation on ENISA).

[29] See https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_127

126. To support the implementation of these obligations and instruments, the Union has set up a number of cooperation bodies:

- The NIS Cooperation Group established by the NIS Directive which brings together competent authorities in order to support and facilitate cooperation, in particular by providing strategic guidance.

- The Computer Security Incident Response Teams (CSIRTs) Network, a network of national CSIRTs from EU Member States which facilitates operational information exchange.

  ENISA, the Commission, Member States and national regulatory authorities (NRAs) (in Spain, mainly the CNMC and AEPD) have developed technical guidelines for national regulatory authorities on incident reporting, security measures, threats and assets.

127. Even if the EU Toolbox does not qualify data protection and privacy regulations as one of the "main" frameworks but just as a "relevant" or "potentially relevant" regulatory framework, we will analyse it below, particularly bearing in mind that the statutory and enforcement powers of the AEPD already in place constitute an important risk mitigator. In fact, the Commission Recommendation on the Cybersecurity of 5G networks[30] stresses that a high level of data protection and privacy is an important element in ensuring the security of 5G networks.

6.2. The EU Telecommunications Framework

128. Under the EU telecommunications framework, obligations can be imposed on telecommunication operators by the respective Member State(s) in which they are providing service.

129. Member States 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 organisational measures to appropriately manage the risks posed to the security of networks and services as per Article 13a of the Framework Directive[3132].

130. The framework also provides that competent national authorities have powers to issue binding instructions and ensure their compliance. In addition, under Directive 2002/20/EC10 Member States are allowed to attach to a general authorisation conditions concerning the security of public networks against unauthorised access. The Toolbox also reminds the

[30] Whereas (16) of Commission Recommendation on Cybersecurity of 5G Networks - C(2019) 2335 final.
[31] Article 13a on the security and integrity of networks and services of Directive 2002/21/EC as last amended by Directive 2009/140/EC; and Articles 40 and 41 of Directive 2018/1972.
[32] More info and resources on Article 13a ENISA working group at: https://resilience.enisa.europa.eu/article-13

existing obligations for the purpose of protecting the confidentiality of communications, under Article 4 of Directive 2002/58/EC11 (ePrivacy Directive)[33] which we will review below.

131. The future European Electronic Communications Code (EECC), which will replace the current framework as of 21 December 2020, maintains the security provisions of the current framework (in Title V, Articles 40 and 41) and also introduces definitions on the security of networks and services.[34]

132. For the purposes of this Opinion, it is important to highlight that, as stated in the EU Toolbox, neither the current framework nor the EECC include any provisions directly applicable to the network equipment manufacturers and other service providers, since these providers do not fall under their scope.

133. In Spain, as in most European countries, existing legislation grant authorities the powers envisaged in the EU Toolbox. This is so because Law 9/2014, of 9 May ("the Spanish General Telecommunications Law") transposed Directive 2009/140/EC, of 25 November, on a common regulatory framework for electronic communications networks and services.

134. Thus, Article 44 of the Spanish General Telecommunications Law sets out the obligations on integrity and security of public communications networks, giving the Spanish Telecommunication authority (currently, the Secretary of State for Telecommunications and Digital Infrastructures) the power to issue binding instructions to operators, requiring them:

- To provide information to assess the integrity and security of their networks, including their security policies.

- To allow security audits by independent bodies or relevant authorities, with their results being notified to the Ministry (and with the audit costs being born by the operator).

135. Having said that, the establishment of a vendor screening mechanism or the imposition of market share caps are not foreseen as part of those powers.

136. When exercising the powers described, Spain´s Telecommunication Authority will act in consultation with ENISA, the Secretary of State of the Ministry of Inland Security (vis-à-vis critical infrastructures) and the CNMC (with respect to its regulatory and competition powers in the communications market).

137. Aside from purely regulatory aspects, Law 9/2014 enshrines the principle of free competition in the provision of electronic communications' services on several occasion, for instance:

[33] Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

[34] Specifically under Article 2, (21), 'security of networks and services' is defined as 'the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of those networks and services, of stored or transmitted or processed data, or of the related services offered by, or accessible via, those electronic communications networks or services.

- As an objective and general principle (Article 3.a);
- As a guiding principle for market operators (Article 5.1);
- As a guiding principle for the Public Administration (Article 9.2);
- As a guiding principle for ex-ante market regulation (Articles 13 to 18), the definition of public and universal service obligations (Articles 23 and 25), the occupation of public and private property or the conditions to be met by installations and installers (Article 59).

6.3. The NIS Directive[35]

138. The NIS Directive establishes security and incident notification requirements for operators of essential services in digital infrastructure and other sectors (energy, finance, healthcare, transport) and for digital service providers (cloud computing services and online marketplaces and search engines).

139. The NIS Directive was implemented in Spain through Royal-Decree Law 12/2018, of 7 September and, as the Directive, does not apply to undertakings providing public communication networks or publicly available electronic communication services except when they are designated "critical operators" under the regulations on Critical Infrastructures (Spanish Law 8/2011 of 28 April on Protection of Critical Infrastructures). This exclusion is due the fact that security provisions for operators of public communication networks or publicly available electronic communication services are regulated under the Telecoms Framework.

140. Spain's implementation of the NIS Directive set out Spain's CSIRT/CERTs (Computer Security Incident Response Team/Computer Emergency Response Teams) namely, the CCN-CERT of the National Cryptology centre-*Centro Criptológico Nacional* for public sector and main coordinator, the INCIBE-CERT, of the National Institute of Cybersecurity INCIBE for non-public sector entities and private individuals and the ESPDEF-CERT of Spain's Ministry of Defence for essential services or national defence together with the other CERTs. The Spanish law also reinforces coordination between Member States in case of cross-border incidents affecting operators.

6.4. The EU Cybersecurity Act Regulation[36]

141. The so-called EU "Cybersecurity Act" is a European Union Regulation which entered into force in June 2019 but with a number of relevant sections only applicable as from 28 June 2021. As an EU Regulation, it has direct effect in Spain. It creates a framework for European cybersecurity certification schemes and EU statements of conformity for ICT products, ICT processes and ICT services.

[35] Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

[36] Regulation (EU) 2019/881 of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification

142. The Regulation specifically addresses the so-called risk of “IT dependency”, understood as the reliance and integration of modern ICT products and systems with one or more third-party technologies and components such as software modules, libraries or application programming interfaces. The Regulation acknowledges that this ‘dependency’ could pose additional cybersecurity risks, since vulnerabilities found in third-party components could also affect the security of the ICT products, ICT services and ICT processes.

143. Once the Regulation is fully implemented, certification schemes will also enable manufacturers or providers to demonstrate that they have included specific security features in the early stages of products' design and users to ascertain the level of security assurance, on an EU-wide basis. As recognized by the EU Toolbox, the framework provides an essential supporting tool to promote consistent levels of security.

144. The Regulations allows for the development of cybersecurity certification schemes to respond to the needs of users of 5G-related equipment and software and it also foresees that Member States are able to adopt national technical regulations providing for mandatory certification under a European cybersecurity certification scheme and to have recourse to those schemes in the context of public procurement.

6.5. Data Protection and privacy rules

6.5.1. The General Data Protection Regulation (GDPR) [37]

145. The GDPR is not only the main piece of legislation which governs the European fundamental right of the protection of natural persons in relation to the processing of personal data, but it has also become the international standard for compliance with data processing activities and security of processing

146. Even if 5G equipment suppliers and other service providers may not carry out data processing activities subject to the GDPR, a vast majority of cyber threats will and in a number of situations 5G equipment suppliers may fall under its scope.

147. For suppliers of 5G equipment, like Huawei, risk mitigators would include:

- The need to carry out data protection impact assessments (DPIAs), as required under Article 35 of the GDPR and Article 28 of the Spanish DP Act;

- The adoption of appropriate technical and organisational measures to ensure a level of security appropriate to the risks (article 32 GDPR), particularly as failing to do so may be considered a serious infringement under article 73 d) of the Spanish Data Protection Act;

- The adherence to certification mechanisms and compliance with the principles of data protection by design and by default set out in article 25 of the GDPR.

[37] Regulation (EU) 2016/679 on protection of natural persons with regard to the processing of personal data and on the free movement of such data.

6.5.2. Spain´s regulations on data protection

148. Spain was since 1992, prior to the approval of the EU GDPR, one of the EU countries with the most stringent and comprehensive regulations on data protection (including IT Security of processing).

149. Subsequently, from 1999 on, Spain required all companies to have security protocols in place and appoint a security officer, and carry out biannual security audits, encrypt sensible data when transmitted through communications networks or map security incidents. Those security measures where further reinforced in 2007 when new regulations required software manufacturers to use "privacy by design measures", with the AEPD imposing hefty fines for non-compliance.

150. For those all historic reasons, the Spanish AEPD has played a very significant role in ensuring the integrity and security of communications network, going well beyond the enforcement of obligations on data processing and e-Privacy (traffic data retention period, cookies, etc.).

151. Therefore, the GDPR's direct effect in Spain and its strict enforcement regime and administrative fines are important risk mitigators already in place.

6.5.3. The AEPD's initial position on 5G

152. Not surprisingly, given the proactive role of the Spanish Data Protection (AEPD) on IT security, it released on May 13th May 2020 the public note "Introduction to the 5G technologies and its risks to privacy"[38].

153. In its note the AEPD calls for

- Uniform IT security criteria for all the players in 5G networks, based on PIA risk analysis as required by GDPR.
- Independent audit of services and infrastructures certification mechanisms.
- The establishment of end-to-end encryption in the edge computing model.

6.6. The Directive on Critical Infrastructures

154. Spain implemented the Directive on Critical Infrastructures[39] through Law 8/2011, of 28 April, on the protection measures of critical infrastructures.

155. Identification and designation of a critical infrastructure ("CIs") or European Critical Infrastructures ("ECIs") and inclusion in the Catalogue of CI and ECIs run by Spain's Inland Ministry is classified information (level "SECRET").

[38] https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-publica-recomendaciones-5G
[39] Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

156. As stated in the EU Toolbox, the requirements set out in this piece of legislation to identify critical infrastructure can operate as an effective mitigation measure.

7. Assessing the risk of PRC interference in Huawei (R5): key legal principles

157. The EU Toolbox can be regarded as a set of commonly agreed recommendations to EU Member States on how they should discharge a specific preventive function: the protection of their national 5G networks against the significant cybersecurity risks to which they will be exposed, given the complex technical features of the new 5G technology and the critical functions and services which will be based on the 5G and, particularly, the "internet of things" (IoT).

158. Thus, the Toolbox is essentially a technical document prepared by national experts and authorities dealing with an specific category of critical risks -the cyber-security risks of future 5G networks- and could thus be compared with other potential sets of risk-related recommendations, like those prepared, hypothetically, by cooperation groups of:

- Health authorities on the prevention of pandemics;
- Energy authorities on ensuring the security of energy supplies; or
- Police, intelligence and national security authorities on preventing terrorist attacks.

7.1. The Toolbox and the "Preventative State"

159. As those comparisons show, the Toolbox can be regarded as an illustration of what American lawyer Allan Dershowitz has described as the shift towards the "preventative State", i.e. the adoption by public authorities of *ex ante* measures meant to prevent likely harmful conduct, particularly those with potentially devastating effects. In 2006 he wrote:[40]

> "*The democratic world is experiencing a fundamental shift in its approach to controlling harmful conduct. We are moving away from our traditional reliance on deterrent and reactive approaches and toward more preventive and proactive approaches. This shift has enormous implications for civil liberties, human rights, criminal justice, national security, foreign policy, and international law -implications that are not being sufficiently considered. It is a conceptual shift in emphasis from a theory of deterrence to a theory of prevention, a shift that carries enormous implications for the actions a society may take to control dangerous human behavior, ranging from targeted killings of terrorists, to preemptive attacks against nuclear and other weapons of mass destruction, to preventing warfare, to proactive crime prevention techniques (stings, informers, wiretaps), to psychiatric or chemical methods of preventing sexual predation, to racial, ethnic, or other forms of profiling, to inoculation or quarantine for infectious diseases (whether transmitted 'naturally' or by 'weaponization'), to prior restraints on dangerous or offensive speech, to the*

[40] Alan M. Dershowitz, "Preemption. A Knife that cuts both ways", Norton, 2006, pg.2-3.

use of torture (or other extraordinary measures) as a means of gathering intelligence deemed necessary to prevent imminent acts of terrorism".

160. He ended his 2006 book with a desperate plea:[41]

> "*There is a desperate need in the world for a coherent and widely accepted jurisprudence of preemption and prevention, in the context of both self-defense and defense of others. There is also a pressing need for a neutral body or other fair mechanism to apply any such jurisprudence. Today both needs are lacking. In the absence of a jurisprudence and jurismechanism, ad hoc decisions become de facto rules*".

7.2. The limits of the "public security" or "public policy" exception

161. As indicated before, the EU Toolbox does not contain a single reference to the legal implications of using some of the strategic measures which it recommends, even if in some cases they amount to "profiling" techniques, in which the risk is assessed on the basis of some external features of the vendor, with scant consideration to their particular circumstances.

162. There is not denying that the integrity of 5G networks is likely to be considered a public security concern, involving the national interest, particularly in light of the fundamental role that they will play in the future development of many key services. But that doesn´t mean that, as it will be expressed shortly, a reference to non-technical cybersecurity risks could be used by public authorities as a magical "incantation" or "wild card" allowing them to adopt arbitrary measures not adequate or proportional to address the actual cybersecurity goals.

163. There is indeed a risk that the High Risk Vendor (HRV) screening mechanism can lead to the potential exclusion of certain non-EU vendors (in particular Chinese suppliers). This would run against core legal principles of EU law, including the free movement of goods and services, freedom to conduct business, and the prohibition of discriminatory treatment based on nationality or technology. The HRV mechanism may also violates WTO law and obligations set out in bilateral investment treaties.

164. It should be recalled that opening markets to competition was the primary objective of the liberalization of communications networks and services launched in 1988, which led the EU to abolish special and exclusive rights for the use and provision of telecommunications equipment and services and to ensure the right of private sector operators to use, import, market, connect, bring into service, and maintain telecom equipment of their choice.

165. Hence, in the following paragraphs I will attempt to sketch part of the "jurisprudence" which European Governments, like Spain´s, might likely be keen to observe, when carrying out the assessment of 5G Vendors for the non-technical risks described in the EU Toolbox (more specifically, R5).

[41] *Ibidem*, p.237.

166. Such assessment requires evaluating a very diffuse risk, of political nature, which can be deemed to be related to "national security". This raises the legal issue of how much discretion should authorities be allowed when making such assessment, lest they hide protectionist commercial interests or narrow political interests under the noble mantle of "national security" or apply a "precautionary" approach devoid of any sense of proportionality.

167. In order to explore what existing jurisprudence could apply *mutatis mutandis* to the Toolbox novel exercise in risk assessment, I will draw on precedents in three different legal areas:

- The adoption of restrictive trade measures by WTO members on the basis of GATT's Article XXI.

- The adoption of restrictive measures in the EU on the basis of the so-called "precautionary principle", or in applying the essential internal market freedoms enshrined in the Treaties.

- Legal criteria in Spain on the exercise of discretionary decision power by public authorities.

168. As it will be shown below, one common tenet of existing jurisprudence on all three areas indicate is that the fight against risks does not provide authorities with a "wild card" allowing them to apply restrictions without limitation or which fail the proportionality test.

7.2.1. WTO law and the security exception

169. As indicated by two leading specialists in WTO regulations, measures which limit the use of components from a certain foreign supplier or country (like Huawei or China), let alone forbid altogether its use, would run against the GATT principles of non-discrimination (art. I:1) and national treatment (III:4), unless the exceptions envisaged in articles XX (a) ("public morals") or XXI ("national security") GATT applied. But in their view, it is doubtful that they do. [42]

170. I fully agree with their conclusion and, since the applicability of the exception of article XX seems to me out of the question, I will concentrate on the "national security" exception of article XXI.

171. Under Article XXI of the 1947 General Agreement on Trade and Taxes (GATT), "nothing in this Agreement shall be construed (b) to prevent any member country from taking any action which it considers necessary for the protection of its essential security interests" relating to several categories of goods or materials (i.e. fissionable materials or arms, ammunition or other goods or materials used for the purpose of supplying military establishments) or measures "taken in time of war or other emergency in international relations".

[42] Thomas Voland and Michel Petite, "Cybersecurity measures and WTO Law -Especially regarding the 5G networks", Eu ZW 2020, 218, March 24, 2020, p.224.

172. There is a long history of cases in which governments tried to abuse this article -as when in the 1970s Sweden based on national security grounds an import quota system for footwear, subsequently withdrawn.

173. One recent case in point was the imposition in 2018 by the US Government of tariff quotas on steel and aluminum imports, again on national security grounds. The EU, China and many other countries opposed the measure and requested the establishment of a WTO panel to rule on the case.

174. One of the most relevant legal issues that came up in the dispute was to what extent the "security exception" is "self-judging" by the member country invoking its use or, on the contrary, it is "justiciable" and its conformity with GATT rules can be judged by an WTO panel.

175. While the US claimed that Article XXI is "self-judging" and its use cannot be controlled by any WTO panel, the European Union strenuously opposed that view, as expressed in the EU's Opening Statement:[43]

> "*We want to stress the following three essential points. First, the measures at issue are safeguards. Second, they are not genuine national security measures. Third, Article XXI is "justiciable*".
>
> *The measures at issue are not genuine national security measures. You do not need to take our word for it. Instead, look at the structure and the language of the measures themselves, as well as statements by the US President, US Government departments, and high-ranking officials. They all clearly show that a specific objective of the measures is to protect the domestic steel and aluminum industry writ large, as an end in itself. Just recently, President Trump tweeted that, "by placing a 25% Tariff on "dumped" steel", the US now has a "big and growing [steel] industry", which was important, for example, in helping the US auto industry. He also tweeted that the steel industry is now "revived", that many jobs are created, and that "billions" are paid to the US treasury. The measures at issue understand the term "national security" as "broadly defined to include the economy, to include the impact on employment, to include a very big variety of things*".

176. Even if this case is still pending, on April 5, 2019 a different WTO panel ruled on the exceptional transit restrictions imposed in 2014 by Russia against Ukraine on national security grounds, during a period of political tensions between the two countries.[44]

177. The Panel found that WTO panels have jurisdiction to review aspects of a Member's invocation of Article XXI, that Russia had met the requirements for invoking the article and, therefore, that the transit bans and restrictions were covered by the GATT.

---

[43] Opening Oral Statement by the European Union, Case DS 548, United States — Certain Measures on Steel and Aluminum Products, Geneva, 4 November 2019, available at https://trade.ec.europa.eu/doclib/docs/2019/november/tradoc_158427.pdf

[44] Case DS512: Russia-Measures Concerning Traffic in Transit, available at https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds512_e.htm#:~:text=The%20Panel%20found%20that%20WTO,XXI(b)(iii)%20of

178. Specifically, the Panel decided that, while the chapeau of Article XXI (b) allows a Member to take action “which it considers necessary” for the protection of its essential security interests, this discretion is limited to circumstances that objectively “be found to meet the requirements in one of the enumerated subparagraphs of that provision”[45]. Consequently, the Panel rejected Russia's jurisdictional argument that Article XXI was totally “self-judging”. As the Panel argued “there is no basis for treating the invocation of Article XXI(b)(iii) of the GATT 1994 as an incantation that shields a challenged measure from all scrutiny”.[46]

179. The Panel found that "essential security interests", which is evidently a narrower concept than "security interests", may generally be understood to refer to those interests relating to the quintessential functions of the state, namely, the protection of its territory and its population from external threats, and the maintenance of law and public order internally.

180. The specific interests that are considered directly relevant to the protection of a state from such external or internal threats will depend on the particular situation and perceptions of the state in question and can be expected to vary with changing circumstances. For these reasons, it is left, in general, to every Member to define what it considers to be its essential security interests.

181. However, this does not mean that a Member is free to elevate any concern to that of an "essential security interest". Rather, the discretion of a Member to designate particular concerns as "essential security interests" is limited by its obligation to interpret and apply Article XXI(b)(iii) of the GATT 1994 in good faith. The Panel recalls that the obligation of good faith is a general principle of law and a principle of general international law which underlies all treaties (…) The obligation of good faith requires that Members not use the exceptions in Article XXI as a means to circumvent their obligations under the GATT 1994. A glaring example of this would be where a Member sought to release itself from the structure of "reciprocal and mutually advantageous arrangements" that constitutes the multilateral trading system simply by re-labelling trade interests that it had agreed to protect and promote within the system, as "essential security interests", falling outside the reach of that system.

182. In practical terms the Panel’s ruling implies that -if we set aside nuclear materials (i.e. subparagraph i) and military supplies (subparagraph ii)-, the article XXI (b) national security exception can only be invoked in times of an emergency in international relations or during a war (subparagraph iii)”.

7.2.2. The EU’s “appropriateness” and “proportionality” tests

183. The possibility for authorities to adopt exceptional restrictive measures to prevent potentially catastrophic risks even when there remains some degree of uncertainty as to the scope and proof of such risks was first envisaged in Germany in 1968 in its “Air Pollution

[45] Paragraph 7.101
[46] Paragraph 7.100.

Act". [47] Such "*Vorsorgeprinzip*" ("precautionary principle") found subsequently its way in 1987 into London Ministerial Declaration for the Second International Conference on the Protection of the North Sea and finally in 1992 was enshrined in two significant texts:

- The Rio Declaration on Environment and Development, under which "where there are threats if serious or irreversible damage, lack of full scientific certainty shall not be used as a reason for postponing cost-effective measures to prevent environmental degradation".[48]

- The Maastricht Treaty, which included in the EC Treaty the principle that Community policy on the environment shall be based on the precautionary principle and on the principles that preventive action should be taken, that environmental damage should as a priority be rectified at source and that the polluter should pay … 3. In preparing its policy on the environment, the Community shall take account of: – available scientific and technical data, … – the potential benefits and costs of action or lack of action …".[49]

184. It is worth noting that the Maastricht Treaty, while enshrining the precautionary principle on environmental policy, included also in the Treaty another important principle:

> "*The Member States and the Union shall act in accordance with the principle of an open market economy with free competition, favoring an efficient allocation of resources*".[50]

185. Within the European Union, the "precautionary principle", born originally as part of its environmental policy, broadened subsequently its scope and became a more general legal principle applicable to policy actions taking to prevent a potentially catastrophic risk (e.g. food poisoning) when there is no conclusive proof of the existence or severity of the potential danger.

186. This became apparent in 1996 when the European Commission decided to ban exports of beef from the United Kingdom to reduce the risk of BSE transmission and the UK challenged such measure. In its ruling in 1998[51], the European Court of Justice held that "where there is uncertainty as to the existence or extent of risks to human health, the institutions may take protective measures without having to wait until the reality and seriousness of those risks become fully apparent (…) That approach is borne out by Article 130r(1) of the EC Treaty, according to which Community policy on the environment is to pursue the objective inter alia of protecting human health. Article 130r(2) provides that that policy is to aim at a high level of protection and is to be based in particular on the principles that preventive action should be taken and that environmental protection requirements must be integrated into the definition and implementation of other Community policies."

---

[47] 1974 *Bundesinmissionsschutsgesetz*, art. 5.2 "Installations subject to authorization are to be constructed and operated in such a manner that…precaution is taken against damaging environmental effects".

[48] Rio Declaration on Environment and Development, Principle 15, June 14, 1992 U.N. Doc.A/Conf.151/5/Rev.1 (1992).

[49] Currently, Article 191.2 of the TFUE.

[50] Currently Article 120 of the TFUE.

[51] Judgement of 5 May 1998, cases C-157/96 and C-180/96.

187. Shortly thereafter, the Council urged the Commission "to be in the future even more determined to be guided by the precautionary principle in preparing proposals for legislation and in its other consumer-related activities and develop as a priority clear and effective guidelines for the application of this principle, which led the Commission to prepare in 2000 a full-fledged "Communication from the Commission on the precautionary principle".[52]

188. In the Communication the Commission argued that while the precautionary principle is mentioned in the Treaty only in connection with the environment, "in practice, its scope is much wider, and specifically where preliminary objective scientific evaluation, indicates that there are reasonable grounds for concern that the potentially dangerous effects on the environment, human, animal or plant health may be inconsistent with the high level of protection chosen for the Community. The Commission considers that the Community, like other WTO members, has the right to establish the level of protection - particularly of the environment, human, animal and plant health, - that it deems appropriate. Applying the precautionary principle is a key tenet of its policy, and the choices it makes to this end will continue to affect the views it defends internationally, on how this principle should be applied".

189. But, in the section which is more directly relevant for the purposes of this Opinion, the Commission recognized that where action is deemed necessary, measures based on the precautionary principle should be, inter alia:

- proportional to the chosen level of protection,
- non-discriminatory in their application,
- based on an examination of the potential benefits and costs of action or lack of action (including, where appropriate and feasible, an economic cost/benefit analysis).

190. For the Commission:

- "Proportionality means tailoring measures to the chosen level of protection. Risk can rarely be reduced to zero, but incomplete risk assessments may greatly reduce the range of options open to risk managers. A total ban may not be a proportional response to a potential risk in all cases. However, in certain cases, it is the sole possible response to a given risk".
- "Non-discrimination means that comparable situations should not be treated differently, and that different situations should not be treated in the same way, unless there are objective grounds for doing so".
- "Examining costs and benefits entails comparing the overall cost to the Community of action and lack of action, in both the short and long term. This is not simply an economic

[52] 2.2.2000 COM (2000) 1 final.

cost-benefit analysis: its scope is much broader, and includes non-economic considerations, such as the efficacy of possible options and their acceptability to the public. In the conduct of such an examination, account should be taken of the general principle and the case law of the Court that the protection of health takes precedence over economic considerations".

191. The European Court of Justice had the opportunity to rule on the practical application of the precautionary principle in 2003, in a case concerning some trade restrictions. The Court's key findings were these:[53]

> "*If the twofold objective of Regulation No 258/97, namely ensuring the functioning of the internal market in novel foods and protecting public health against the risks to which those foods may give rise, is not to be adversely affected, protective measures adopted under the safeguard clause may not properly be based on a purely hypothetical approach to risk, founded on mere suppositions which are not yet scientifically verified.*
>
> *Such protective measures, notwithstanding their temporary character and even if they are preventive in nature, can be adopted only if they are based on a risk assessment which is as complete as possible in the particular circumstances of an individual case, which indicate that those measures are necessary in order to ensure that novel foods do not present a danger for the consumer, in accordance with the first indent of Article 3(1) of Regulation No 258/97*".

192. Even if not directly related to the "precautionary principle" as such, there is also abundant case law from the European Court of Justice which addresses similar issues and identify the tests to be met by any public restrictive measures which, while invoking public policy, national security or other public goals, are at odds with basic freedoms enshrined in the EU Treaties.

193. Thus, for instance, in *Scientology*, the Court addressed the limits applicable to the principle of "public policy" or "public security" and stated:[54]

> "*It should be observed, first, that while Member States are still, in principle, free to determine the requirements of public policy and public security in the light of their national needs, those grounds must, in the Community context and, in particular, as derogations from the fundamental principle of free movement of capital, be interpreted strictly, so that their scope cannot be determined unilaterally by each Member State without any control by the Community institutions (…).*
>
> *Thus, public policy and public security may be relied on only if there is a genuine and sufficiently serious threat to a fundamental interest of society (…). Moreover, those derogations must not be misapplied so as, in fact, to serve purely economic ends.*

[53] Judgement of September 2003, casa C-236/01 dealing with Regulation (EC) No 258/97 of the European Parliament and of the Council of 27 January 1997 concerning novel foods and novel food ingredients, paragraphs 106 and 107.

[54] Judgement of the Court of 14 March 2000, Association, Case C-54/99, paragraphs 17 and 18.

Second, measures which restrict the free movement of capital may be justified on public-policy and public-security grounds only if they are necessary for the protection of the interests which they are intended to guarantee and only in so far as those objectives cannot be attained by less restrictive measures)".

194. Similarly , when determining whether national restrictive measures were consistent with the principle of free trade within the EU's internal market enshrined in the EU Treaty (particularly, article 34 TFEU on free movement of goods), the Court has refined they had to meet: they should be both "appropriate" (i.e. well designed so as to achieve the objectives pursued) and "proportional" (i.e. absence of less restrictive measure which achieve the same objective").

195. Thus, for instance, in the famous case *Scotch Whisky Association* -on whether the establishment of a minimum sale price of alcohol in Scotland meant to protect human life and health was consistent with the free movement of goods-, the Court wrote: [55]

"*A restrictive measure such as that provided for by the national legislation at issue must satisfy the conditions set out in the Court's case-law with respect to proportionality, that is, the measure must be appropriate for attaining the objective pursued, and must not go beyond what is necessary to attain that objective*".

"*A fiscal measure which increases the taxation of alcoholic drinks is liable to be less restrictive of trade in those products within the European Union than a measure imposing a minimum price per unit (PMU)*".

"*It is for the referring court to determine whether a measure other than that provided for by the national legislation at issue in the main proceedings, such as increased taxation on alcoholic drinks, is capable of protecting human life and health as effectively as that legislation, while being less restrictive of trade in those products within the European Union*".

196. Similarly, in the case Monsanto – on whether Italy could block on health grounds, under Regulation 258/97, the import of genetically modified foods -, the Court wrote:[56]

"*Protective measures adopted under the safeguard clause may not properly be based on a purely hypothetical approach to risk, founded on mere suppositions which are not yet scientifically verified. Such protective measures, notwithstanding their temporary character and even if they are preventive in nature, can be adopted only if they are based on a risk assessment which is as complete as possible in the particular circumstances of an individual case, which indicate that those measures are necessary in order to ensure that novel foods do not present a danger for the consumer, in accordance with the first indent of Article 3(1) of Regulation No 258/97*".

[55] Case C-333/14, 23 December 2015, paragraphs 28, 46 and 49.
[56] Case C-236/01, 9 September 2003, paragraphs 106-107.

7.2.3. Spain's legal principles

197. Article 38 of the Spanish Constitution recognizes free enterprise within the framework of a market economy. It further states that the public authorities shall guarantee and protect its exercise and the safeguarding of productivity in accordance with the demands of the economy in general and, as the case may be, of its planning.

198. The Spanish Constitutional Court´s and Supreme Court's case law has paid attention to the limits of administrative discretionary powers when discriminating among individuals in similar situations and has drawn a sharp distinction between "arbitrariness" and "discretionary powers", declared to be opposite concepts by the Supreme Court in its ruling of November 21, 1985.[57] This long-standing case law has been reaffirmed recently by the Constitutional Court in STC 91/2019, which, in keeping with the ECJ's case law, refers to the "appropriateness" and "proportionality" tests:[58]

> "*For a different treatment to be constitutional it is necessary not only that the goal pursued is a legal one, but it is also indispensable that the legal consequences resulting from the distinction are adequate and proportional to such goal, such that the relation between the adopted measure, its effective result and the goal pursued by the law meet the constitutional test of proportionality, and avoid particularly grievous or excessive results*".

199. Moving closer to telecommunications, article 34.3 of Law 9/2014 states:

> "Regulations drawn up by the public administrations that affect the deployment of public electronic communications networks and land or urban planning instruments must include the necessary provisions to promote or facilitate the deployment of electronic communications network infrastructure in their territorial scope of action. In particular, they must ensure free competition in network installation and the provision of electronic communications services and the

[57] A detailed analysis of such case law can be found in Tomás Ramón Fernández, "Arbitrario, arbitraire, arbitrary. Pasado y presente de un adjetivo imprescindible en el discurso jurídico", Iustel, 2016.

[58] See STC 91/2019, FJ 4. The original text in Spanish of the complete paragraph reads: "Los rasgos esenciales del derecho a la igualdad del art. 14 CE se pueden resumir así: a) no toda desigualdad de trato en la ley supone una infracción del art. 14 de la Constitución, sino que dicha infracción la produce sólo aquella desigualdad que introduce una diferencia entre situaciones que pueden considerarse iguales y que carece de una justificación objetiva y razonable; b) el derecho a la igualdad exige que a iguales supuestos de hecho se apliquen iguales consecuencias jurídicas, debiendo considerarse iguales dos supuestos de hecho cuando la utilización o introducción de elementos diferenciadores sea arbitraria o carezca de fundamento racional; c) el derecho a la igualdad no prohíbe al legislador cualquier desigualdad de trato, sino sólo aquellas desigualdades que resulten artificiosas o injustificadas por no venir fundadas en criterios objetivos suficientemente razonables de acuerdo con criterios o juicios de valor generalmente aceptados; d) por último, para que la diferenciación resulte constitucionalmente lícita no basta con que lo sea el fin que con ella se persigue, sino que es indispensable además que las consecuencias jurídicas que resultan de tal distinción sean adecuadas y proporcionadas a dicho fin, de manera que la relación entre la medida adoptada, el resultado que se produce y el fin pretendido por el legislador superen un juicio de proporcionalidad en sede constitucional, evitando resultados especialmente gravosos o desmedidos".

availability of an adequate range of places and physical spaces in which the operators can decide to place their infrastructure".

200. Furthermore, in keeping with the principle of free competition, Article 59.2 states:

> "*The provision to third parties of the installation or maintenance of telecommunications equipment or systems shall take place under a system of free competition, with no limitations other than those established in this Law and its implementing regulations.*
>
> *Telecommunications equipment or system installation or maintenance services may be provided to third parties by natural or legal persons from a Member State of the European Union or of another nationality, when, in the second case, this is provided for in the international agreements binding the Kingdom of Spain. For all other natural or legal persons, the Government may authorise exceptions of a general or particular nature to the above-mentioned rule.*
>
> *The requirements for carrying out the activity consisting of providing telecommunications equipment or system installation or maintenance services to third parties that are associated with the technical capacity and professional qualifications to perform the activity, technical resources and minimum insurance coverage, surety or any other financial guarantee shall be set out in a Royal Decree. The requirements for entry to the activity and engaging in it shall be proportionate, non-discriminatory, transparent and objective and they shall be clearly and directly linked to the specific general interest that justifies them*".

201. Finally, to the extent that Huawei operates in Spain through its subsidiary Huawei Spain, it is worth mentioning the Bilateral Investment Promotion and Protection Agreement ("BIPPA") in force between Spain and China, dated 14 November 2005[59]. This BIPPA provides for continuous protection and security for mutual investments, prohibition of unfair or discriminatory measures, and the competence of an investment arbitration tribunal in case of conflict between a State and other party's investor. In the same vein, there is also an international treaty between Spain and China on the development of economic and industrial cooperation, dated 15 November 1984.[60]

7.3. Conclusions

202. The brief analysis made above of WTO, EU and Spanish law on the adoption of public restrictive measures to protect national, public policy or citizens' interests against potential risks show clearly that public authorities:

- Cannot act on the basis of mere suppositions, but should act on the basis of a proper risk-assessment which takes into account the specific circumstances of the case (including the measures already in place to mitigate risks and the potential cost of the restrictive measure);

[59] Published in the Spanish Official Gazette dated 8 July 2008.
[60] Published in the Spanish Official Gazette, dated 9 February 1985 and 17 September 1985.

- Cannot adopt restrictive measures which are not adequate to achieve the goal that they purportedly ("appropriateness test")

- Cannot adopt measures which are more restrictive that others which achieve the public objectives with the same, let alone more, effectiveness ("proportionality test").

8. Assessing the risk of PRC interference in Huawei (R5): key issues

203. Having set out in the previous section the legal tests to be met by any restrictive measure resulting from the application of the EU Toolbox -like the declaration of a supplier as a High Risk Vendor (HRV) due to a risk of a third-country State interference (i.e. R 5)- , it is now time to analyse whether, in the particular circumstances of Huawei, it might be justified that it is declared a HRV.

8.1. The risk of Chinese political interference in Huawei

204. As explained above, according to the EU Coordinated Risk Assessment and the EU Toolbox signs of potential interference of a non-EU country on a 5G vendor (like China's on Huawei) are a "strong link" between the supplier and the Government and the country's legislation, the supplier's corporate ownership and the third country's legislation.

205. Hence, the following aspects will be analysed for the case of Huawei:

- Is Huawei State-owned?

- Is Huawei State-controlled?

- Could Chinese security laws have illegal extraterritorial effects on Huawei's activities?

8.1.1. Is Huawei State-owned?

206. Huawei claims to be, as indicated above, a "private company wholly owned by its employees" -more than 100,000, who own their shares through "the Union"-. Its Employment Shareholding Scheme "effectively aligns employee contribution and development with the company's long-term development".

207. Huawei insists, more specifically, that:

- "It is not a state-owned enterprise. Unlike state-owned enterprises, no government agency or outside organization, including the Communist Party of China (CPC), is involved in Huawei's decision-making or business activities".

- "Huawei adopts a modern enterprise system. The Shareholders' Meeting is the company's highest authoritative body. The Board of Directors (BOD) is the decision-making body for corporate strategy, operations, and management. The Supervisory Board oversees the responsibility fulfillment of BOD members and senior management, as well as the standardization of BOD operations".

- "Article 19 of Chapter I in the Company Law of the People's Republic of China states:

  'In a company, an organization of the Communist Party of China shall be established to carry out the activities of the party in accordance with the charter of the Communist Party of China. The company shall provide the necessary conditions for the activities of the party organization.'

  According to publicly available information, all Chinese and foreign-funded companies have established CPC organizations as stipulated by the Company Law. Examples include Huawei, Walmart China, Nokia shanghai Bell China Co., Ltd., and SAIC General Motors Corporation Limited.

  Huawei's CPC organization is not involved in any of Huawei's business activities".

- "Employees' political beliefs are irrelevant to Huawei's business operations. An employee's decision to join the Communist Party of China (CPC) is a private matter. Huawei's business operations have nothing to do with the CPC's political activities.

208. Some authors have taken issue with Huawei's official contention that it is a private, employee-owned company, and suggests that it is in fact State-owned. They argue that:[61]

- "Huawei Tech is a single-shareholder limited liability company (one of the two basic corporate forms under China's company law) and is 100% owned by Huawei Holding, which in turn has only two shareholders: Ren Zhengfei, the founder, with nearly 1.14%, and an entity called Huawei Investment & Holding Company Trade Union Committee ("Huawei Holding TUC"), with the remaining".

- "Employees in the Huawei group do not own actual stock either in Huawei Tech or in Huawei Holding. Instead, they possess, via contract, a kind of virtual stock that allows them a share in the profits. But this virtual stock is a contract right, not a property right; it gives the holder no voting power in either Huawei Tech or Huawei Holding, cannot be transferred, and is cancelled when the employee leaves the firm, subject to a redemption payment from Huawei Holding TUC at a low fixed price. At present, this virtual stock ownership has nothing to do with financing or control. It is purely a profit-sharing incentive scheme".

- "Since Huawei Holding TUC is the only entity (other than Ren Zhengfei) that holds stock the Huawei Holding -the sole owner of Huawei Tech-, the key to understanding the ownership of the Huawei group lies in understanding Huawei Holding TUC. This is hard to do".

[61] Christopher Balding and Donald Clarke, "Who Owns Huawei?" (April 17, 2019), available at SSRN: https://ssrn.com/abstract=3372669 or http://dx.doi.org/10.2139/ssrn.3372669. Similar views are expressed by Tim Rühling in https://www.ui.se/globalassets/butiken/ui-paper/2020/ui-paper-no.-5-2020.pdf

- "The corporate governance picture – the critics continue- is further complicated by the fact that as a matter of law (and usually fact), trade union officers—those who decide what the trade union shall do with its assets, for example—owe their loyalty and are accountable to superior trade union organizations, all the way up to the All-China Federation of Trade Unions at the central level. The Communist Party controls the ACFTU, with the head of the ACFTU sitting on the Politburo. The Party apparatus at any given administrative level controls the trade union organizations at the level, and unions are de facto government organs. Union officials above the level of the enterprise union, while not technically civil servants, are treated as state employees, subject to the same administrative rules and pay scales, and with their salaries paid out of the state treasury. In short, the ACFTU is not simply a trade union but is organized, both legally and practically, as a state-adjacent organization that exists to support and execute state policy directives".

- "Thus, if Huawei Holding is 99%-owned by a genuine Chinese-style trade union operating the way trade unions in China are supposed to operate, it is in a non-trivial sense state-owned".

- "Finally, it is worth noting that it is undisputed that whatever the directors of either Huawei Tech or Huawei Holding may decide, Ren Zhengfei has a veto. This was publicly declared by Ren as part of a recent media campaign by Huawei".

- "Regardless of who, in a practical sense, owns and controls Huawei, it is clear that the employees do not".

209. In my view, it is obvious that Huawei's corporate structure is not the same as Ericsson's and Nokia's, to mention its two main competitors as 5G equipment suppliers, which are publicly listed companies in the Stock Exchanges of Stockholm and Helsinki, respectively. But it would be far-fetched to argue that Huawei is "effectively State-owned".

210. The legal nature of the rights held by Huawei's employees is not completely clear and at best it could be claimed that employees are "indirect" shareholders of Huawei or may be "beneficial owners" of the Huawei Technology shares held in trust by the *Union of Huawei Investment & Holding Co. Ltd.* This company would play a similar role to the one played in Spain and other countries by SICAVs, collective investment institutions in which their shareholders can control the entity that manages their investments in listed companies. The rights of Huawei's employees can also be assimilated to those known in the Anglo-Saxon world as "depositary receipts", such as the securities traded on the New York Stock Exchange representing shares of foreign companies listed on that market.

211. At the same time, it is not indeed a traditional, Western-style private company either publicly listed -like Ericcson or Nokia- or closely held by a limited number of significant shareholders (like, in Spain, say, El Corte Inglés o Mercadona).

212. A more apt comparison would be probably between Huawei and some big European cooperative private companies, in which most employees (the members of the "cooperative") have an economic interest in the company and have some say on the company's major decisions, even if they are far removed from the day-to-day business

decisions. There are indeed a number of significant European companies which, sometimes unbeknownst to the public at large, are not corporations, but cooperatives, like Crédit Agricole, Group BPCE or Covea in France, BVR and the Rewe Group in Germany, Rabo Bank in Holland or, in Spain, Cajamar, Cooperativa Mondragón, Mutua Madrileña or Mapfre in Spain.[62]

213. It may be true that the right held by Huawei's employees may not be legally identical to the Western concept of "company share", and this Opinion need not study this issue in depth. However, it is obvious that such rights bear a close resemblance to participation certificates in certain collective investment schemes (such as SICAVs) and to "share depositary receipts". That is because these rights are owned by Huawei's employees and because Huawei's ownership structure is quite similar to that of large European cooperatives. It is true that Huawei is not a listed company (and, as noted above, Huawei itself points out that this allows it to devote more resources to R&D, as it is not enslaved by short-term profit objectives) but this in no way implies that it is "State-owned".

214. But even if it is not State-owned, is it "State-controlled"? This is the question to which we now turn.

8.1.2. Is Huawei State-controlled?

215. Huawei recognizes that some of its employees and managers may be members of China's Communist Party (CCP), but that does not have any bearing on who controls the company or how it is run. It specifically argues that:[63]

- Huawei complies with article 19 of Chapter I of the China's Company Law, which states that "in a company, an organization of the Communist Party of China shall be established to carry out the activities of the party in accordance with the charter of the Communist Party of China (CPC). The company shall provide the necessary conditions for the activities of the party organization". This provision is followed not only by Huawei, but also by all other companies established in China, including the subsidiaries of US companies like, say, Walmart, Motorola, or General Motors. Huawei's CPC organization is not involved in any of Huawei's business activities. Furthermore, Huawei has never established any CPC organization outside China.

- "Whether or not Mr. Ren Zhengfei, other Huawei executives, or other employees are members of the CPC does not affect Huawei's decision making or operations". "An employee's decision to join the CPC is a private matter".

- "Huawei has a sound and effective governance structure which ensures its independent operations and management. This means no outside organizations control Huawei. Shareholding employees elect the Representatives' Commission (Commission) on a one-vote-per-share basis. The Commission, along with the Board of Directors and

[62] See for further details Euricse "World Cooperative Monitor 2019", available at https://www.euricse.eu/publications/world-cooperative-monitor-2019/

[63] https://www.huawei.com/minisite/who-runs-huawei/en/

Supervisory Board which are elected by the Commission, decides on and manages major company".

- "Huawei's 96,768 active shareholding employees, of which 86,514 employees with voting rights elected 115 shareholding employee representatives (terms of 5 years), the shareholding employee representative committee elected the chairman and 16 other directors, and the board of directors elected 4 (the vice chairman and three executive directors). The rotating chairman is served by three vice chairman. The rotating chairman leads the Board of Directors and its Executive Committee while in office. The board exercises decision-making authority for corporate strategy, operations, and management, and is the highest body responsible for corporate strategy, operations, management, and customer satisfaction".

216. Even if, as indicated above, Huawei is not State-owned, it has been argued that it is indirectly controlled by the State or the CPC through their influence and close links with senior managers and employees. There have been at least two specific claims:

- The former link of Mr. Ren with China's PLA.

- The links between Huawei's employees with Chinese intelligence.

217. It has been argued, for instance, that Mr. Ren was a high-ranking intelligence officer with the People's Liberation Army (PLA) and that his connections played a role in Huawei getting government support to help China overcome its reliance on foreign telecommunications gear.

218. Huawei responds that its founder, Mr. Ren, was a low-ranking soldier in the Engineering Corps of the PRC's Army. He retired in 1983 when the military was significantly downsized and has not engaged with the military since. "Over the past 70 years, more than 50 million people have left the Chinese military. Like the veterans in the US, many of these people look for new jobs in the government or private sectors". Mr. Ren himself has stated that "the US is overemphasizing my military background because it does not have any concrete evidence against Huawei".

219. Concerning the links between Huawei's employees with Chinese intelligence, American economist Christopher Balding, "using a unique dataset of CVs that leaked from unsecure Chinese recruitment databases and websites and emerged online in 2018" found that "key midlevel technical personnel employed by Huawei have strong backgrounds in work closely associated with intelligence gathering and military activities". [64]

220. From the analysis of those CVs, Mr. Balding draws the conclusion that "Huawei employees effectively confirm the rumored relationship between the Chinese state, military, and intelligence gathering services [and] the fears of links and acting in concert with the Chinese state (…) [T]here is a clear institutionalization where the Chinese state and intelligence

[64] Christopher Balding, "Huawei Technologies' Links to Chinese State Security" (July 5, 2019), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3415726

gathering assets are placed in Huawei within a systemic organization designed to facilitate information flows".

221. Huawei responds that "it maintains strict policies for hiring candidates with military or government backgrounds. During the hiring process, these candidates are required to provide documentation proving they have ended their relationships with the military or the government.

222. In my view, there is a long tradition in Western thought, going back at least to the famous work by Adolf Berle and Gardiner Means "The Modern Corporation & Private Property" (1932) that recognized the separation in modern industrial corporations between "ownership" and "control" and came to the conclusion that such big companies are in practice controlled not by its shareholders, but by its managers. In Berle and Means' famous words:[65]

> "*Separation of ownership and controls becomes almost complete when not even a substantial minority interest exists, as in the American Telephone and Telegraph Company, whose largest holder is reported to own less than one per cent of the company's stock. Under such conditions control may be held by the directors or titular managers who can employ the proxy machinery to become a self-perpetuating body, even though, as a group they own but a small fraction of the stock of outstanding (…) Corporations where this separation has become an important factor may be classed as quasi-public in character in contradiction to the private, or closely held corporation in which no important separation of ownership and control has taken place*".

223. A few years later, American economist John Kenneth Galbraith confirmed that impression:[66]

> "*In recent decades there has been steady accumulation of evidence on the shift of power from owners to managers within the modern large corporation. The power of the stockholders has seemed increasingly tenuous. A small proportion of the stock is represented at stockholders' meetings for a ceremony in which banality is varied chiefly by irrelevance*".

224. In Galbraith´s view, power had shifted to what his described as the "technostructure":[67]

> "*The modern business organization, or that part which has to do with guidance, and direction, consists of numerous individuals who are engaged, at any given time, in obtaining, digesting or exchanging and testing information. A very large part of the exchange and testing of information is by word of mouth -a discussion in the office, at lunch or over the telephone. But the most typical procedures is through the committee and the committee meeting (…) Thus decision in the modern business enterprise is the product not of individuals but of groups*".

[65] Adolf A. Berle & Gardiner C. Means, "The Modern Corporation & Private Property", Transaction Publishers, 2006, see Chapter I, "Property in Transition", p. 6.
[66] John Kenneth Galbraith, "The New Industrial State", 1967, Penguin Books, Second Edition, p.65.
[67] Ibidem, p. 78-79.

225. US corporations, particularly listed companies, have gone through a number of changes since Galbraith wrote those words, as a result of the M&A mania and leveraged buy-outs of the 80s, the deregulatory revolution and the wave of privatizations started in the UK and US in the 80s, the dot.com explosion of the late XX century and the birth, early in the new century, of the new companies which would soon be labeled the "Big Tech", or the growing role of "shareholders' activism", which brought to bear the power and influence of private equity and other institutional investors on big listed companies. Probably as part of these factors, the "managerial capitalism" of the initial post-war decades was gradually abandoned, as described by two British economists:[68]

> "*By 2002, the basic idea of a big company -a multidivisional, hierarchical institution that could offer a lifetime career to its employees- had been unbundled*".

226. My contention is that Huawei, being a company which has become extremely large, is not listed, and sells equipment and services across the world, fits mostly the old Capitalist "managerial mould", in which a qualified, and almost exclusively Chinese "technostructure", inspired by the strategic views of one of its founders, Mr. Ren, is at the helm and a complex system of units, reporting lines and committees handle its business activities and decisions.

227. In those organizations, "power" and "control" are not easy to pinpoint, since they are the result of the interaction between a vast array of senior managers and committees and other collegial bodies, without any single individual enjoying a decisive role. In Huawei this collective approach is apparent in its characteristic system of the three rotating executive chairmen.

228. In that sense, Huawei's dominant corporate culture seems to reflect what the famous Irish business consultant Charles Handy famously described as an "Apollonian culture" or "culture of roles", in which there is no single "Zeus" god calling the shots and dominating the organization, but with decisions being the result of an complex and interactive decision process -resembling an Apollonian temple- in which the power of individual officials derive from their organizational roles, not from their personal relation with "Zeus".[69]

229. Huawei's founder, Mr. Ren Zhengfei, recognized himself how Huawei copied the structure of big American companies:[70]

> "*An important reason for Huawei's success today is that we learned most of our management practices from US companies. Since Huawei was founded, we hired dozens of US consulting firms to teach us how to manage the company. Now our entire system is very similar to those US companies. So the US should be proud*".

---

[68] John Micklethwait and Adrian Wooldridge, "The Company. A Short History of a Revolutionary Idea", Modern Library, 2003.

[69] Charles Handy, "Gods of Management. The Changing Work of Organisations", Arrow, 1978.

[70] "Ren Zhenfei and Yuval Noah Harari at Davos", interview conducted by Zanny Minton Beddoes, Editor-in-Chief of *The Economist*, January 21, 2020, Davos, Switzerland, available at https://www.huawei.com/en/facts/voices-of-huawei/davos

230. While not a "Zeus" figure, in Handy's terminology, Mr. Ren remains indeed an influential leader:[71]

> "*Within Huawei, Ren is regarded as more of a spiritual leader than a hands-on executive. His musings are often posted on an internal company website for employees to read. He's prone to military imagery and has likened his troubles with Washington to a war. 'People would stand up and clap whenever he came into a room', said a British national who worked for the company in Shenzhen and spoke on the condition of anonymity because he signed a nondisclosure agreement. 'People would linger on his every word. He was revered by everyone. Despite not being an active CEO and being a chairman, his decisions were always final'*."

231. Mr. Ren himself has recognized that he holds a "veto power" (something equivalent to what in Europe is known as a "golden share"):

> "'*Our Articles of Governance state that veto power can be inherited, but that's not going to be by my family', Ren said. 'Instead, veto power is going to be collectively exercised by an elite group made up of seven elected members. It is possible that none of them are my family members'. Ren said he was in no rush to relinquish his veto power — not with uncertainties in the global economy because of head winds such as Brexit. But the revelation underscores how Ren is increasingly willing to incrementally lift the veil over his company*".

232. Further illustration of that significant influence can be seen:

- In his sending letters to all Huawei employees, as he did, for instance, on 27 December 2018, entitled "Comprehensively Enhancing Software Engineering Capabilities and Practices to Build Trustworthy, Quality Products", to outline the transformation program and meeting the expectations of the UK's Oversight Board.

- In his recent efforts to engage with the international community and represent Huawei's view point, as he did, for instance, in his interview with *The Economist*,[72] when he offered to sale for a price to any willing buyer all of Huawei's 5G patents, and intimated that he had come up with the idea that very morning (presumably without prior consultation with any of the rotating-chairmen).

233. Looked at from the distance, it seems likely that Huawei is actually controlled not by the Chinese State or the CPC, but a tightly knit group of senior managers under the inspiration and leadership of Huawei's "founding father", Mr. Ren. Contrary to the view of Huawei's critics, Mr. Ren's spiritual leadership of Huawei clearly confirms that the company is not State-controlled.

---

[71] "The Man behind Huawei ", Los Angeles Times, April 10, 2019, available at https://www.latimes.com/projects/la-fi-tn-huawei-5g-trade-war/

[72] "Ren Zhengfei may sell Huawei's 5G technology to a Western buyer", *The Economist*, September 12, 2019.

234. Additionally, as a result of the competitive nature of the markets in which it sells, and in keeping with the business philosophy of its founder, Mr. Ren, it has developed a corporate culture in which "service to the customer" is the overriding objective.

235. Huawei remaining a big Chinese industrial group headquartered in China -even if has already significant overseas activities-, it cannot escape the hallmarks of the peculiar Chinese capitalists system, like the presence of CCP representatives within its rank and files.

236. These peculiar features, unheard of in modern Western corporations , do not detract from the fact that under all normal and foreseeable circumstances Huawei operates, and will operate, as a capitalist company, in which business objectives and market success are the overriding goals.

237. As Huawei's managers emphasize, the company is aware that the slightest deviation from an strict business approach and the emergence of mere rumors or indications of Huawei having acted following political instructions of the Chinese political authorities, let alone doing anything illegal and betraying their customers' trust (like planting illegal backdoors or sabotage devices in their equipment) would produce a devastating blow to its international ambitions of becoming (and remaining) the world leader in its area.

238. Finally, the arguments mentioned above about Mr. Ren's past activities in the PLA, almost 40 years ago, or the "links" with Chinese intelligence resulting from the analysis of the CVs of Huawei employees are so convoluted, are supported by so little evidence and carry so little legal weight to prove that Huawei is "State-controlled" that there is no need to discuss them. Were we to apply the same ridiculous standards to Western companies, including US ones, we would probably arrive also at the absurd conclusion that they are not private, but "State-controlled".

8.1.3. Could Chinese security laws have illegal extraterritorial effects?

239. The EU Toolbox refers to the "third's country legislation" as a potential factor to consider when assessing whether a supplier could be subject to "political interference" from its government.

240. The practical question is then whether Chinese laws related to the monitoring of citizens´ activities or data or, more broadly, requiring all market operators in China to cooperate with intelligence or national security authorities for the gathering of information could apply to Huawei's overseas activities and potentially require the planting in its equipment and programs of spying devices, illegal backdoors, sabotage devices or the like.

241. In this connection I have read the English versions of the relevant PRC's laws and regulations currently in force provided to me by Huawei, as well as the legal analysis of their content carried out by three specialized law firms, EY Chen&Co Law Firm, Clifford Chance LLP and Simmons & Simmons.

242. Such laws are the following:

- The Anti-terrorism Law, adopted at the 18th Session of the Standing Committee of the 12th National People's Congress on December 27, 2015 (the "Anti-terrorism Law");

- The Counter-espionage Law, adopted by the 11th Session of the Standing Committee of the 12th National People's Congress on November 1, 2014 (the "Counter-espionage Law");

- The Cybersecurity Law, adopted at the 24th Session of the Standing Committee of the 12th National People's Congress on November 7, 2016 (the "Cybersecurity Law");

- The National Intelligence Law, adopted at the 28th Session of the Standing Committee of the 12th National People's Congress on June 27, 2017 (the "National Intelligence Law"); and

- the National Security Law, adopted at the 15th Session of the Standing Committee of the 12th National People's Congress on July 1, 2015 (the "National Security law").

243. I find persuasive the conclusions of those legal analysis that none of the aforementioned laws:

- Have extraterritorial effect outside China; nor

- Empower Chinese authorities to order telecommunication equipment manufacturers, like Huawei, to plant backdoors, eavesdropping devices or spyware in telecommunication equipment.

244. Such legal analyses conclude that Chinese law does not gran relevant authorities the power to compel an overseas affiliate of a Chinese company to disclose or gran access to data stored overseas. Generally speaking, Chinese law enforcement authorities do not have authority to enforce Chinese laws against or compel assistance from foreign entities, except indirectly via judicial assistance of foreign law enforcement authorities under relevant bilateral treaties.

245. Those conclusions are consistent with the Declaration from Mr. Jihong Chen and Mr. Jianwei Fang, partners of the Chinese legal firm Zhong Lun, before the U.S. Federal Communications Commission dated 27 May 2018, in which they state that:

- "Unless clearly specified in the legislation, Chinese law generally does not have extraterritorial jurisdiction".

- "China has limited extraterritorial jurisdiction only when an actor commits terrorist activities against Chinese nationals, citizens or institutions, or commits terrorist activities stipulated in the international treaties concluded or participated in by China. Companies that are legally engaged in equipment manufacturing and sales are not the objects of extraterritorial jurisdiction of the Chinese government and therefore have no legal assistance obligation."

246. Such declaration was accompanied by a memorandum prepared by the law firm Clifford Chance for Huawei, dated 11 December 2018, which states:

> "*We have requested Zhong Lun to further elaborate on its statement that 'unless clearly specified in the legislation, Chinese law generally does not have extraterritorial jurisdiction'*".

247. Zhonglun has provided the following elaborations:

(i) if the PRC legislature intends to give any legal provision extraterritorial effect, it would normally use express language to indicate so; and

(ii) the PRC Ministry of Foreign Affairs has repeatedly expressed the PRC government's general objection to long-arm extraterritorial jurisdiction".

248. Huawei has further explained to me that:

- "Mr. Yang Jiechi, a member of the Political Bureau of the Communist Party of China (CPC) Central Committee and Director of the Office of the Foreign Affairs Commission of the CPC Central Committee, stated formally in February 2019, during the 55th Munich Security Conference, that the Chinese government always requires Chinese firms to abide by international rules and the laws and regulations of the countries where they operate, and that China has no law requiring companies to install backdoors or collect foreign intelligence".

- "Premier Li Keqiang reiterated this point at a press conference following a recent session of the National People's Congress. On April 12, 2019, at the "16+1 Summit" in Croatia, Premier Li repeatedly told all our employees not to install backdoors on networks. This represents Chinese state leaders' position on backdoors, so it is impossible for us to install backdoors on our equipment".

- "Even if we were ordered to, Huawei would still not install backdoors. If a single backdoor was found in even one of the 170 countries where we operate, our sales would shrink in all of them. Then a large number of our employees would resign, but [could not] leave. [They] would have to repay tens of billions of dollars in debts. If [they] could not pay, [they] would be hounded by creditors every day. How [could they] live a life like that? So we would never follow anyone's instructions to install backdoors. It will never happen".

- "We are committed to complying with all applicable laws and regulations in the EU. We will make commitments to local governments about what we will and will not do in the countries where we operate, and be audited accordingly. This will help increase their trust in us".

- "The UK has the most stringent oversight of Huawei. We trust the UK and Germany, so we are open to their checks. They also pay a lot attention to our problems and provide us with constructive criticism. This process has further helped build trust. We are happy

to make these commitments and submit ourselves to audits according to the EU's management requirements".

- "Cyber security and privacy protection are Huawei's top priorities. We are willing to sign no-backdoor and no-spy agreements with any country".

8.1.4. Why (only) Huawei?

249. Huawei has pointed out that the supply chain of all manufactures of 5G equipment (including Ericsson and Nokia) is a global one, with significant activities taking place in all cases in China. As a consequence, "much of the US infrastructure using Ericsson and Nokia [equipment] is made in China". Also, "if Beijing really wants to have access to, say, German telecommunications networks, Chinese intelligence agencies may intervene in the supply chains of Ericsson and Nokia".

250. More specifically, according to Huawei:

- Ericsson has in China 11,000 employees (i.e. around 11.6% of its global workforce), with 5,000 of them being R&D employees. It has also there 5 Innovation Centres, including one 5G Innovation Centre. Furthermore, it has in Nanjing the largest Telecom System Manufacture and Supply Centre, including 5G.

- Nokia has in China more than 16,000 employees (i.e. around 15,5% of its global workforce), with more than 10,000 being R&D employees. It has there 4 Telecom System Manufacturing Bases (Dongguan, Shenzhen, Beijing and Suzhou). Nokia China is partly owned by the Chinese Government, its CEO is appointed by the Chinese Government and its chairman since July 2017, Mr. Yuan Xi, is also a CCO party secretary.

251. Thus, Huawei claims that in a world of global supply chains, "whether communication equipment is secure shall not [depend on] its country of origin. Instead, the security of products of the communications system shall be assured through a global unified security standards".

252. Even if I am in no position to confirm the specific figures supplied to me by Huawei, it is clear that:

- Ericsson's 2019 Annual Report confirms that it operates a global supply chain and has manufacturing sites, service delivery centers and R&D in China.[73]

- Nokia's 2019 Annual Report confirms that it operates a global supply chain and has at least one manufacturing plant in China.[74]

[73] Ericsson 2019 Annual Report, p.17, available at https://www.ericsson.com/495c1f/assets/local/investors/documents/2019/ericsson-annual-report-2019-en.pdf.
[74] Nokia 2019 Annual Report, p. 120, available at https://www.nokia.com/system/files/2020-03/Nokia%20in%202019%20annual%20report_1.pdf

253. Hence, to the extent that all plants in China, whatever the company, are subject to similar local legislation, there is no obvious reason why the purported malicious planting of illegal devices on orders from the Chinese authorities or the CCP would spare local plants or subcontractors of non-Chinese companies.

254. Indeed, there are good reasons to think that the nationality of the supplier of equipment is a very bad proxy for the vulnerability to potential malicious cyber-attacks. Actually, not other than the head of the UK's NCSC, Mr. Ciaran Martin, recently stated:[75]

> "*Over the past two years, the UK government has, based on NCSC findings, attributed state-sponsored malicious cyber activity against the UK to Russia, China, North Korea and Iran. There is also a serious and sustained threat from organised cyber crime.*
>
> *These attacks have come against a range of targets spanning different sectors. Their aims have been different. The methods have been different. The supply chain, and where suppliers are from, is one issue but it is not the only issue. Last year, the NCSC publicly attributed some attacks on UK networks, including telecoms networks, to Russia. As far as we know, those networks didn't have any Russian kit in them, anywhere. The techniques the Russians used to target those networks were looking for weaknesses in how they were architected and how they were run.*
>
> *So we are not naïve. Far from it. In the 1,200 or so significant cyber security incidents the NCSC has managed since we were set up, the country of origin of suppliers has not featured among the main causes for concern in how these attacks are carried out*."

255. In other words, focusing on the nationality of suppliers could be a clear case of barking at the wrong tree. Or, as stated more elegantly by the Intelligence and Security Committee of the UK Parliament, "the 'flag of origin' for telecommunications equipment is not the critical element in determining cyber security".[76]

8.1.5. Conclusions

256. My conclusions from the analysis of the issues considered in this Section could be summarized as follows:

- Even if China embraced years ago key principles of a market economy, it remains a Communist country, not a Western democracy, and this implies that companies headquartered in China show features (like the presence of CCP representatives within the company) unheard of in Western market economies.

- Irrespective of that, there is not the slightest evidence, let alone convincing proof, that:

[75] Mr. Ciaran Martin's speech at CyberSec in Brussels, February 20, 2019, available at https://www.ncsc.gov.uk/speech/ciaran-martins-cybersec-speech-brussels

[76] Intelligence and Security Committee of the UK's Parliament, "Statement on 5G suppliers", July 19, 2019, available at http://isc.independent.gov.uk/.

- Huawei is a State-owned company.
- Huawei is State-controlled.
- Huawei might be compelled by Chinese laws to carry out activities (like planting illegal devices in their equipment) which might create in Spain the cyber-security risks envisaged in the EU Toolbox.

- The "flag of origin" of 5G equipment, let alone the nationality of the supplying company, is not a particularly relevant element for cybersecurity purposes.

257. Under all normal and foreseeable scenarios, Huawei's corporate culture, business ethic, internal security systems and economics objectives will keep Huawei fully aligned with its customer's interests and make Huawei an ally in preserving the integrity and resilience of Spain's 5G network against cyber-attacks.

258. What about a hypothetical "stressed scenario" of heightened geopolitical frictions between China and any Western power with effects on Spain? What if, for instance, under those circumstances new legislation were to be passed in China or Huawei were nationalized?

259. Irrespective of the probability assigned to such hypothetical scenarios, the key idea to bear in mind would be the unavoidable time lag between any such politically-motivated illegal decision by the Chinese authorities and its potential effect on Spain's 5G Network: unless Huawei`s equipment already installed in Spain's network was already vulnerable to such illicit maneuvers, it would remain unaffected, provided any necessary maintenance or upgrade operations could be safely carried out by non-compromised personnel.

260. In other words, even if Huawei's business objective and culture were ever to be overridden under hypothetical and dramatic circumstances, any notional attempts of espionage or sabotage by Huawei of Spain´s 5G networks would likely be ineffective, provided the right precautions were taken when installing, maintaining and upgrading the 5G network.

261. Hence, the best strategy to mitigate the potential risk of a foreign State interference, as described in Toolbox's R5, would be not to declare Huawei a "High-Risk Vendor" (HRV), but to enforce effectively a system of certifications, inspections and control of all suppliers, as envisaged in the Toolbox's technical measure 9 (TM09). As an added bonus, this would protect Spain's 5G network against potential political interference from any country, including the US's national security and intelligence agencies.

8.2. Huawei's track-record

262. When assessing a vendor's risk profile it is necessary to consider not only its nationality, corporate structure and supply chain, but its track-record and practices in terms of cyber-security and cooperation with public authorities of the countries to which they supply equipment. This will be the focus of the following paragraphs.

8.2.1. No past cyber-security incidents

263. As Huawei rightly states, while it has served 3 billion people in over 170 countries and regions over the past 30 years, there is no public record of any major network outages or cybersecurity incidents which could besmirch its track record on cyber-security.

264. For instance, in 2008 the French newspaper "Le Monde" reported that the servers of the headquarters of the African Union in Addis-Abeba had been hacked via a back-door, and it recalled that the building had been built back in 2012 by the Chinese. But there is in the report not even a reference to Huawei, which reportedly installed the organization internet system, and denied any role in the case.[77]

265. In another colorful episode, in February 2020 the German press reported that a US delegation had presented evidence to the German authorities that back in 2009 Huawei had had access to mobile communication information as a result of its equipment having been used for law enforcement purposes. The evidence was, however, so weak that German *Der Spiegel* reported on the efforts of the US delegation to convince German authorities with the title "A backdoor that only the US can see".[78]

266. It is true that in its 2019 Report, the Oversight Board of HCSEC made the following finding:[79]

> "*Poor software engineering and cyber security processes lead to security and quality issues, including vulnerabilities. The number and severity of vulnerabilities discovered, along with architectural and build issues, by the relatively small team in HCSEC is a particular concern. If an attacker has knowledge of these vulnerabilities and sufficient access to exploit them, they may be able to affect the operation of the network, in some cases causing it to cease operating correctly. Other impacts could include being able to access user traffic or reconfiguration of the network elements*".

267. But the Report makes clear in that same paragraphs that the vulnerabilities discovered in Huawei's engineering and software were neither crucial, nor intentional:

- However, the architectural controls in place in most UK operators limit the ability of attackers to engender communication with any network elements not explicitly exposed to the public which, with other measures in place, makes exploitation of vulnerabilities harder. These architectural controls and the operational and security management of the networks by the UK operators will remain critically important in the coming years to manage the residual risks caused by the engineering defects identified.

---

[77] See https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html

[78] "Einer Hintertür, die nur die USA sehen", https://www.spiegel.de/netzwelt/netzpolitik/huawei-und-die-spionage-vorwuerfe-eine-hintertuer-die-nur-die-usa-sehen-a-c9c40afd-51a3-43d3-a853-75d1fcdd1946.

[79] "Huawei Cyber Security Evaluation Center (HCSEC) Oversight Board Annual Report 2019", A report to the National Security Adviser of the United Kingdom, March 2019 available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf

- These findings are about basic engineering competence and cyber security hygiene that give rise to vulnerabilities that are capable of being exploited by a range of actors. NCSC does not believe that the defects identified are a result of Chinese state interference.

8.2.2. Pro-active cyber-security attitude and cooperation with authorities

268. Huawei has made over the years a sustained effort to cooperate with its customers and with public authorities in ensuring that its equipment and products are safe and not vulnerable to cybersecurity risks. In Mr. Ren's words:[80]

> "*At Huawei, cyber-security and privacy protection are always the company's top priorities. Huawei resolutely incorporates requirements of the EU's General Data Protection Regulation (GDPR) into all of our business processes. We are now investing heavily to upgrade existing networks and build new networks.*
>
> *Second, for more than 30 years, Huawei has provided network services in more than 170 countries and regions, serving approximately three billion users. We have maintained a proven track record in security. In fact, we have never had any major security incidents, I think that record speaks for itself.*
>
> *Besides, we are more than willing to submit ourselves to strict oversight in countries where we operate. At present, the UK has conducted the most stringent oversight of Huawei. Why is the UK determined to continue using our equipment? Even though they've spotted a few problems and flaws in our equipment, but they may trust us more than other suppliers because we have been more rigorously reviewed*".

269. More specifically, as described in previous Sections of this Opinion, Huawei has indeed voluntarily established:

- An internal Independent Cybersecurity Lab (ICSL), a, ISO-certified security verification unit which is independent from business teams and from R&D departments.

- Three Transparency Centers in Europe, which allow customers to check and inspect Huawei's equipment, including its source code, without compromising Huawei's intellectual property. As already indicated, this is the oldest and most active center is the UK's HCSEC, chaired by the UK`s most senior cyber-security authority, tasked with the review of Huawei's equipment and processes and monitored by a strong Oversight Board. The Oversight Board has confirmed Huawei's close engagement in the verification process of its equipment and in the remediation work needed to fix the technical glitches discovered. The Oversight Board has specifically confirmed that the software vulnerabilities discovered were not the result of any State interference.

  According to public information, no other major global telecom equipment provider has accepted such a rigorous external monitoring.

[80] *The Economist*, September 12, 2019, op. cit.

- A robust, highly-placed and autonomous Global Cyber-Security Office (GSPO), with his boss having direct reporting and communication line with the rotating chairman, through the Global Cyber Security and User Privacy Protection Committee.

  Even though there is not yet an international practice or standard on Chief Information Officers (CIO), Huawei's GSPO (Global Cyber Security and Privacy Officer) place in the corporate structure evidence the key importance attached to his role, in line with the practices in other leading global telecom companies (like Telefónica or Apple).

- The appointment of an independent EU DPO, in keeping with the requirements of article 37 GDPR. It has been confirmed that he does not receive any instructions regarding the exercise of his tasks, cannot be dismissed or penalised in the performance of his tasks and reports to the highest management level (the Rotating Chairman) through the Global Cyber Security and Privacy Protection Committee ("GCSPC") as required by article 38 GDPR.

270. Such proactive cooperative attitude of Huawei in dealing with cyber-security risks are at odds with the accusations that it might be intent on planting illegal backdoors or sabotage devices to make 5G networks vulnerable to China-sponsored espionage or sabotage attempts.

8.3. The costs of declaring Huawei a High-Risk Vendor (HRV)

271. As indicated above, when assessing the convenience of adopting any restrictive measure to fight a hypothetical risk, the principle of proportionality requires to take into account the likely costs of the restriction being considered.

272. In the case of a full ban of the use of Huawei equipment for the EU's 5G networks, given the limited number of vendors other than Huawei (i.e. essentially Ericsson and Nokia), the exclusion of Huawei would have a significant competitive effect, to the detriment of MNOs, with effects on two, or even three, fronts:

- Costs of equipment, which might likely be higher in the absence of Huawei, a low cost producer whose commercial pressure has significantly lowered prices;

- Less technological innovation, as MNOs could neither benefit from cutting-edge Huawei technological solutions, nor from the pressure to innovate that results from higher competition.

- Less competition on security standards, since, as stated by the Intelligence and Security Committee of Parliament, "requiring Mobile Network Operators to use equipment from more than one vendor increases competition between those vendors which will force them to improve their security standards".[81]

273. Even if the adverse economic consequences of a full ban on Huawei are hard to calculate with accuracy, preliminary calculations made last year, at the request of Huawei, by UK's

[81] "Statemen on 5G suppliers", op. cit. p.2

consultancy Oxford Economics suggested that they could be high.[82] The calculations were based on the following:

- First, the estimated increase in investment costs for MNOs resulting from the higher prices charged, in the absence of Huawei, by the two remaining competitors (i.e. Nokia and Ericsson), which according to Oxford Economics' calculations would be, depending on the country, somewhere between 9% and 29% higher (see figure below).

- Second, assuming MNOs kept their nominal annual investment in the 5G rollout, the cost increase would translate into a delayed 5G roll-out, so that fewer people would have access to 5G by 2024.

- Third, less access to 5G would translate in turn into a lower productivity growth of somewhere between 0.15%-0.30% per year from 2020 to 2035, leading to a significantly lower GDP in 2035 than in case of no restrictions on 5G suppliers.

Fig. 1: Economic impacts of restricting a player of Huawei's size from competing in the 5G infrastructure market

Market	Price impact (% increase in investment costs)	Reduction in number of people with access to 5G by 2023 (millions)	Reduction in GDP in 2035 (US$ billions, 2019 prices)
Australia	8% to 27%	0 to 3.1	0.8 to 8.2
Canada	8% to 24%	2.2 to 5.7	1.0 to 6.7
France	9% to 29%	2.1 to 5.7	2.6 to 15.6
Germany	9% to 29%	3.8 to 10.0	2.4 to 13.8
Japan	9% to 27%	7.2 to 19.1	5.3 to 34.3
India	8% to 27%	15.9 to 45.3	4.7 to 27.8
United Kingdom	9% to 29%	3.9 to 10.4	1.8 to 11.8
United States	8% to 24%	0 to 27.1	8.6 to 63.0

Note: In Australia and the US, 5G rollout is expected to cover a vast majority of the population over the next 2-3 years with almost no increase in coverage in the following years. In our low cost scenario, the increase in investment costs leads to delays in rollout of a few months, despite which a vast majority of the population receives access by 2023.

Source: Oxford Economics

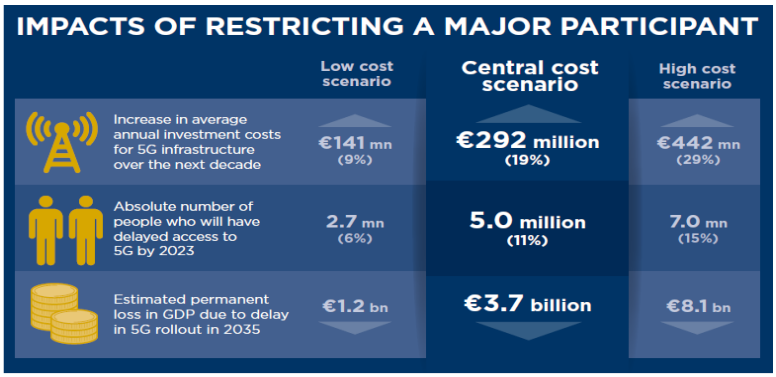
274. Oxford Economics has recently updated and expanded its 2019 preliminary analysis on the cost of European countries preventing Huawei from competing with Ericsson and Nokia as a potential 5G supplier. [83]In the specific case of Spain, they considered three basic scenarios, depending on the increase in investment costs resulting from the absence of Huawei: 9% (low cost scenario), 19% (central cost scenario) and 29% (high cost scenario).

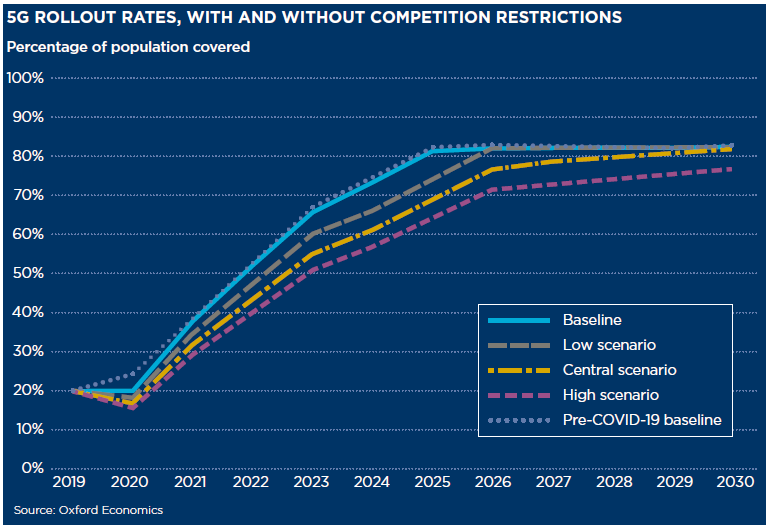
275. As shown on the table below, in the central cost scenario annual investment costs for Spain's MNOs would increase by €292 million, which would translate into 5 million fewer potential

[82] Oxford Economics, "The Economic Impact of Restricting Competition in 5G Network Equipment", December 2019, Fig.1, p. 5 , available at https://www.oxfordeconomics.com/recent-releases/Economic-Impact-of-Restricting-Competition-in-5G-Network-Equipment

[83] Oxford Economics, "The Economic Impact of Restricting Competition in 5G Network Equipment", June 2020, available at https://www.oxfordeconomics.com/recent-releases/The-Economic-Impact-of-Restricting-Competition-in-5G-Network-Equipment.

clients having access to 5G networks by 2023 and an annual loss of GDP or €3.7 billion by 2035.[84]





276. Besides, even if, contrary to the wishes of US hawks, a "rip and tear" strategy of already-installed Huawei equipment were not legally mandated, the ban on Huawei would be hard to reconcile with the 5G NSA architecture planned in Spain, as already-installed Huawei stations could not be upgraded to serve the new 5G network and they would have to be either duplicated (one set for the legacy 4G network, a different one for the new 5G) or ripped off altogether and be replaced by a new one. Either possibility would entail, in all likelihood, huge additional costs for MNOs and long delays in the actual deployment of the 5G networks, as borrowing constraints and investment caps might compel MNOs to stretch their projects over longer horizons.

277. By way of illustration, as reported recently in the Financial Times, "Vodafone has warned that the UK's hopes of leading the world in 5G technology would be dealt a terminal blow if the government removes Huawei from the country's telecoms infrastructure. As Scott Petty, chief technology officer of Vodafone UK, told the Financial Times' The UK's leadership in 5G will be lost if mobile operators are forced to spend time and money replacing existing equipment'. (…) Mr. Petty said that, rather than stripping out Huawei equipment, 'efforts

[84] *Ibidem*, p. 75.

should instead be focused on expanding 5G coverage, developing 5G capabilities for UK industry, and investing in the next stage of this important technology"[85].

278. Besides, under this scenario, MNOs might require compensation from Governments, since in all likelihood they would the legal restrictions on the use of their Huawei equipment as expropriatory in nature, as was the case decades ago when, as a result of ETA-related pressures against nuclear electricity plants in the Basque country, they were shut-down under the so-called "moratoria nuclear".

8.4. The existence of more effective and less restrictive alternatives

279. The EU Toolbox itself and the experience of the UK with the HCSEC suggest that there would less intrusive, less discriminatory and more effective alternatives to address the hypothetical risks which might purportedly justify the declaration of Huawei as a HRV.

280. Such measures could be, for instance, the establishment, for all the relevant equipment used in 5G networks, irrespective of their supplier or the place where they were manufactured, of:

- A mandatory (but nimble) system of EU-wide cyber-security certification, as envisaged in in technical measure 9 (TM09) –"using EU certification for 5G network components, customer equipment and/or suppliers' processes- and supporting action 5 (SA 05) – "ensuring the application of standard technical and organizational security measures through specific EU-wide certification scheme-.

- Facilities for their inspection or revision (including controls of software and source code), along similar lines as those currently in place in the UK for the HCSEC.

281. It is beyond the scope of this legal Opinion to specify how such certification and inspection systems could be organized (whether for equipment or suppliers, machines or processes, etc.). But the mere reading of the EU Toolbox suggests that, concerning cyber-security risks- some of the "technical measures" that it suggests would make unnecessary some of the "strategic measures" that it advocates.

282. Concerning cyber-security risks, as such, this view is shared by some analysts, like Tim Rühlig, from the Swedish Institute of International Affairs:[86]

> "*More effective means [than excluding Huawei altogether from the rollout of the 5G infrastructure] are available for mitigating network security risks. The most effective are better end-to-end encryption, which makes spying difficult; and network redundancies that increase the availability of coverage coupled with vendor diversity. Vendor diversity relies on the assumption that all 5G equipment will contain vulnerabilities, but different suppliers' equipment will come with*

[85] "Vodafone warns ripping out Huawei would cost UK lead in 5G", *Financial Times*, June 9, 2020.

[86] Tim Rühlig, "Who controls Huawei? Implications for Europe", UI paper 5/2020, Swedish Institute of International Affaris, 27 February, 2020, p.4-5, available at https://www.ui.se/globalassets/butiken/ui-paper/2020/ui-paper-no.-5-2020.pdf

different kinds of vulnerabilities which will impose higher cost for attackers to identify and effectively exploit the. These means could be combined with improved evaluation and certification of products and processes, including source code reviews or network flow monitoring".

283. Actually, by reducing vendor diversity, the exclusion of Huawei could be counter-productive:[87]

> "*An appropriate European response would tackle network security issues by technical means rather than a ban on Huawei. Better end-to-end encryption, redundancy and vendor diversity will be the most important, albeit costly measures to implement (…)*
>
> *An outright ban on Huawei would contradict the goal of vendor diversity, particularly with regard to the Radio Access Network which is currently supplied by only three firms: Huawei, Nokia and Ericsson*".

284. Finally, as already indicated, a general system of certification and control of 5G equipment, irrespective of the supplier, might help prevent the interference in EU communications networks of all foreign States, including the US and its intelligence agencies, which under Chapter 26 of the Foreign Intelligence Surveillance Act (FISA) permits the US Government to conduct electronic surveillance outside the US, as explicitly laid out in the FISA Amendment Act of 2008.

8.5. Conclusions

285. The examination of jurisprudence and doctrines on the "national security exception" in Article XXI of GATT, on the so-called "precautionary principle" and on other Spanish regulations leads to the inescapable conclusions that, when assessing any non-technical risks from a vendor of equipment for 5G networks, like Huawei, and considering potential restrictive measures to mitigate such risks, in Spain -and probably in many other EU countries-:

- Restrictions cannot be based on "mere suppositions" or be the result of a "profiling" of suppliers based on their nationality.

- Risk-assessments should consider mitigation measures in place -so that mostly "residual risks" are considered- and the track-record of the supplier assessed.

- The costs of restrictive measures should be objectively balanced against its likely benefits.

- Less intrusive and discriminatory, and more focused alternatives should be preferred when they achieve the same or even better results. Specifically, there are technical measures -some of them, like certification schemes, advocated by the Toolbox- which

[87] Tim Rühlig, *ibidem*, p.19.

would be more effective and proportional than imposing any specific restriction on 5G suppliers like Huawei.

9. General conclusions

In light of the previous analysis, and subject to the limitations described in the Introduction, the main conclusions of this Opinion can be summarized as follows:

I. The EU Toolbox is a "soft law" instrument prepared by cyber-security experts, within the framework of the NIS Cooperation Group. Hence, by its very nature and origin, the Toolbox is silent on the legal criteria to be applied by Member States when making the risk assessment recommended in strategic measure 3 (SM 03).

II. In keeping with European and Spanish legal principles and case law, adopting restrictive measures to protect against hypothetical risks cannot be based on mere speculation. Furthermore, more effective and less restrictive and costly alternatives capable of achieving a public goal -like the cybersecurity of 5G networks- should be preferred to less effective and more disruptive and costly ones.

III. Spain has a robust legal and regulatory framework, which endows Spanish authorities with the powers suggested by the EU Toolbox. Their rigorous enforcement powers, by allowing them to impose heavy fines and corrective measures, can operate as a highly effective risk mitigator.

IV. The risk assessment of individual vendors, like Huawei, cannot be carried out using nationality-based profiling techniques, but requires considering Huawei's specific track record, commitments and mitigation measures in the prevention of cyber-security risks.

V. Huawei has made over the years a sustained effort to cooperate with its customers and with public authorities in ensuring that its equipment and products are safe and not vulnerable to cybersecurity risks. As part of that effort it has voluntarily established:

- An internal Independent Cybersecurity Lab (ICSL), a security verification unit which is independent from business teams and from R&D departments.

- Three Transparency Centers in Europe, which allow customers and public authorities to check and inspect Huawei's equipment, including its source code, without compromising Huawei's intellectual property.

  The oldest and most active center is the UK's HCSEC, chaired by the UK`s most senior cyber-security authority, tasked with the review of Huawei's equipment and processes and monitored by a strong Oversight Board. The Oversight Board has confirmed Huawei's close engagement in the verification process of its equipment and in the remediation work needed to fix the technical glitches discovered. The Oversight Board has specifically confirmed that the software vulnerabilities discovered were not the result of any State interference.

According to public information, no other major global telecom equipment provider has accepted such a rigorous external monitoring

- A robust, highly-placed and autonomous Global Cyber-Security Office (GSPO), with his boss having direct reporting and communication line with the rotating chairman, through the Global Cyber Security and User Privacy Protection Committee.

  Even though there is not yet an international practice or standard on Chief Information Officers (CIO), Huawei's GSPO (Global Cyber Security and Privacy Officer) place in the corporate structure evidence the key importance attached to his role, in line with the practices in other leading global telecom companies (like Telefónica or Apple).

- The appointment of an independent EU DPO, in keeping with the requirements of article 37 GDPR. It has been confirmed that he does not receive any instructions regarding the exercise of his tasks, cannot be dismissed or penalised in the performance of his tasks and reports to the highest management level (the Rotating Chairman) through the Global Cyber Security and Privacy Protection Committee ("GCSPC") as required by article 38 GDPR.

Such proactive cooperative attitude of Huawei in dealing with cyber-security risks are at odds with the accusations that it might be intent on planting illegal backdoors or sabotage devices to make 5G networks vulnerable to China-sponsored espionage or sabotage attempts.

VI. Speculation about Huawei's equipment being particularly exposed to the risk of the Chinese authorities interference seems unfounded. It further overlooks the fact that a significant part of the supply chain of all 5G vendors, including Ericsson and Nokia, include manufacturing activities carried out in China.

VII. More specifically, it is my opinion that:

- Huawei is a private company, not unlike a Spanish cooperative, and it is not State-owned.

- There is not the slightest evidence that Huawei is "State-controlled".

- The risk that Huawei or some of its employees might be compelled to embed illegal devices in its 5G equipment or programs is extremely remote and not higher than for other manufacturers.

- Huawei's track-record on cybersecurity is excellent.

- Huawei has shown over the years a spirit of cooperation, including on cybersecurity with all the European authorities and European MNOs, and has voluntarily submitted to the strictest controls.

VIII. As far as Chinese legislation is concerned, I have read the English versions of the following PRC's laws:

- The Anti-terrorism Law, adopted at the 18th Session of the Standing Committee of the 12th National People's Congress on December 27, 2015 (the "Anti-terrorism Law");

- The Counter-espionage Law, adopted by the 11th Session of the Standing Committee of the 12th National People's Congress on November 1, 2014 (the "Counter-espionage Law");

- The Cybersecurity Law, adopted at the 24th Session of the Standing Committee of the 12th National People's Congress on November 7, 2016 (the "Cybersecurity Law");

- The National Intelligence Law, adopted at the 28th Session of the Standing Committee of the 12th National People's Congress on June 27, 2017 (the "National Intelligence Law"); and

- the National Security Law, adopted at the 15th Session of the Standing Committee of the 12th National People's Congress on July 1, 2015 (the "National Security law").

I am not a specialist in Chinese law, but I have read the legal analysis carried out, at Huawei's request, by three specialized law firms, EY Chen&Co, Clifford Chance LLP and Simmons&Simmons, and I find persuasive their conclusions that none of the aforementioned laws:

- Have extraterritorial effect outside China;

- Empower Chinese authorities to order telecommunication equipment manufacturers, like Huawei, to plant backdoors, eavesdropping devices or spyware in telecommunication equipment.

- Chinese law does not grant relevant Chinese authorities the power to compel an overseas affiliate of a Chinese company to disclose or gran access to data stored overseas. Generally speaking, Chinese law enforcement authorities do not have authority to enforce Chinese laws on overseas companies or compel their assistance, except indirectly via judicial assistance of foreign law enforcement authorities under relevant bilateral treaties.

IX. In the case of a full ban on the use of Huawei equipment for EU's 5G networks, given the limited number of vendors other than Huawei (i.e. essentially Ericsson and Nokia), the exclusion of Huawei would have a significant competitive effect, with effects on several fronts:

- A increase in costs of equipment, since Huawei's competitive pressure, a low-cost producer, has significantly lowered prices, for the benefit of mobile network operators and final users;

- Less technological innovation, as mobile network operators could neither benefit from cutting-edge Huawei technological solutions, nor from the pressure to innovate that results from higher competition.

- Less competition on security standards, since, as stated by the Intelligence and Security Committee of Parliament, "requiring Mobile Network Operators to use equipment from more than one vendor increases competition between those vendors which will force them to improve their security standards".[88]

X. Oxford Economics estimated in June 2020 the cost to European countries of preventing Huawei from competing with Ericsson and Nokia as a potential 5G supplier[89]. In the specific case of Spain, they considered three basic scenarios, depending on the increase in investment costs resulting from the absence of Huawei: 9% (low cost scenario), 19% (central cost scenario) and 29% (high cost scenario). In the central cost scenario, annual investment costs for Spain's mobile network operators would increase by €292 million, which would translate into 5 million fewer potential clients having access to 5G networks by 2023, with the consequent loss of productivity.

Besides, even if a "rip and tear" strategy of the already-installed Huawei equipment were not legally mandated, the ban on Huawei would be hard to reconcile with the 5G NSA (*non-stand alone*) architecture planned in Spain, as already-installed Huawei stations could not be upgraded to serve the new 5G network and they would have to be either duplicated (one set for the legacy 4G network, a different one for the new 5G) or ripped off altogether and be replaced by a new one. Either possibility would entail, in all likelihood, huge additional costs for mobile network operators and long delays in the deployment of the 5G networks, as borrowing constraints and investment caps might compel mobile network operators to stretch their projects over longer horizons.

XI. The cyber-security risks resulting from interference from States (R5, according to the Toolbox's terminology) could be more effectively addressed by a general system of mandatory verification and/or inspection of all relevant 5G equipment, coupled with strict controls for subsequent activities of maintenance or upgrade of equipment. Any such certification, inspection or controls should apply across the board to all suppliers, irrespective of their nationality or where such equipment was manufactures, procured or developed.

XII. On the basis of the above and of the information I have reviewed, it is my opinion that there are no legal grounds to impose on Huawei any specific restrictions as part of strategic measure 3 (SM 03) of the Toolbox, as such restrictions would not be appropriate or suitable, nor would they be proportional.

[88] Intelligence and Security Committee of the UK's Parliament, "Statement on 5G suppliers", July 19, 2019, *op. cit.*, p.2.

[89] Oxford Economics, "The Economic Impact of Restricting Competition in 5G Network Equipment", June 2020, available at https://www.oxfordeconomics.com/recent-releases/The-Economic-Impact-of-Restricting-Competition-in-5G-Network-Equipment.

The measure would not be "appropriate" or "suitable" to achieve the public goal pursued -i.e. the cybersecurity of Spain´s 5 G Networks-, since the potential cybersecurity risks of 5G networks:

- Are not related to the nationality of the supplier of equipment, but to the cybersecurity measures used in the design, manufacturing, control, verification and inspection of the equipment, whatever its supplier or its nationality. Even if this is a technical question beyond the expertise of the author of this Report, Huawei's assertion that all its equipment meet the most demanding cybersecurity standards, including allowing source code inspection, and, hence, its second to none in terms of cybersecurity seems true.

- Such cybersecurity goal might actually be jeopardized by imposing restrictions on one supplier, Huawei, and forcing MNOs to rely exclusively on the two other suppliers.

The measure would not be "proportional" either since there are other less restrictive, more effective and less costly measures to achieve the pursued goal, namely, the establishment of a robust system of verification, certification, inspection, testing, audit or, more generally, control of all relevant equipment used in 5G networks, to be applied on a general basis, irrespective of the supplier and regardless of where such equipment was designed or manufactured.

10. Final considerations

I. Legal standards and constitutional principles applicable to what Dershowitz has called the "preventative State" may not necessarily be the same in the US as in the EU or Spain.

II. There is in American history a case of a non-technical risk-assessment by the US Government, made on the basis of "racial profiling", which, while partially endorsed at the time by the US Supreme Court[90], does not meet the legal principles describe above in this Opinion and was indeed subsequently disavowed in the US. It was the mass detention of around 110,000 Americans of Japanese ancestry following the attack on Pearly Harbour in December 1941, as described by Alan Dershowitz:[91]

> "*Rumours were circulated that Hawaians of Japanese ancestry were signalling enemy pilots and submarines, that Japanese-American had intentionally infiltrated the power and water companies, and that they had formed sabotage and espionage rings numbering in the thousands. None of these stories proved true. The records of the FBI and Army and Navy intelligence indicate that there was not a single instance of espionage or sabotage by a resident of Japanese ancestry before, during, and after World War II. The absence of such activities did not, however, satisfy a hysterical population with deep-rooted racial antagonisms. Indeed, the attorney*

[90] In *Korematsu v. United States* (1944), the US Supreme Court, while not dealing with the internment in detention camps, upheld Roosevelt's decision to exclude Japanese Americans from the West Coast Military Area.

[91] Alan M. Dershowitz, "Preemption. A Knife that Cuts Both Ways", Norton, 2006, p.111-112.

general of California, Earl Warren, expressed the Alice in Wonderland view that it was the very absence of sabotage that was 'the most ominous sign in our whole situation [since] it was designed to lull us into a false sense of security (…)We believe that when we are dealing with the Caucasian race we have methods that will test their loyalty. But when we deal with the Japanese…we cannot form any opinion that we believe to be sound".

US General John De Witt, head of the Western Defense Command, expressed Warren's views in more succinct pithy terms:

"*A Jap's a Jap. There is no way to determine their loyalty*".

III. Evan under political pressure from a powerful political ally, the Spanish Government should not apply to Huawei what in essence would amount to a "De Witt profiling approach" if it were to declare, on the basis of Huawei's nationality, that it is a High-Risk Vendor (HRV).

IV. In short, the cybersecurity of future 5G networks is an essential public objective whose risks must be mitigated by the European and Spanish authorities with the appropriate technical measures described in the Toolbox, among which technical measure 9 (TM 9) stands out: using EU certification for 5G network components, customer equipment and/or suppliers' processes. On the contrary, applying to Huawei restrictions as a 5G supplier in application of "strategic measure" 3 (SM03) for being a Chinese company would constitute political arbitrariness without any legal basis.

V. Deng Xiaoping famously said: "*Black cat, white cat, the important thing is that it catches mice*". In that vein, an approach much more consistent with European and Spanish legal norms and case law would be for the Spanish Government to apply to all 5G suppliers this updated version of Deng's saying:

"Chinese cats, Western cats, the important thing is that all l of them are 100% cybersecurity-compliant".

Madrid, 4th of July, 2020
Manuel Conthe Gutiérrez