Policy Brief

Politicization of the 5G:
Divergent Policy Responses and Huawei's Litigation Strategy

Dr Iryna Bogdanova

Executive Summary

The great-power rivalry between the United States and China, the European Union's policy of technological sovereignty as well as the nature and economic implications of the fifth-generation wireless (5G) set the context for the politicization of said technology. This politicization is reflected in the growing resistance to the participation of the Chinese technology giant Huawei Technologies Co., Ltd. in the 5G projects.

As numerous states shore up legislation and administrative actions geared toward eliminating Huawei's participation in their 5G networks, China has maintained a proactive posture and redoubled efforts to export Chinese 5G infrastructure. In its turn, Huawei, as the company bearing financial and reputational costs deriving from the prohibitions on its participation in the 5G rollout, seized the opportunity of calling into question the legality of such restrictions. To achieve this, the company initiated administrative proceedings and disputes at the domestic and international levels.

I. The 5G rollout: economic benefits and security risks

The 5G – the fifth generation of cellular networks – would offer increased speed, reduced latency (the network's response time), and greater bandwidth (drastically increasing the ability to handle many more connected devices than previous networks) (Duffy 2020). These characteristics allow us to talk about three distinctive use cases: enhanced mobile broadband (enabling larger data volumes and enhancing user experience), massive machine-type communication (enabling Internet of Things), and ultra-reliable and low-latency communication (enabling autonomous vehicles and robotic-enabled remote surgery) (Dahlman et al., 2018).

The 5G network would spawn transformational effects. In other words, the 5G is not only the next generation of cellular networks but also "the essential technological component in the digital transformation of society and the economy in the most advanced countries over the next decade" (Robles-Carrillo 2021). Among the key changes enabled by the 5G are connected autonomous cars (Poliakine 2021), smart city infrastructure and traffic management (Remmert 2019), advanced industrial Internet of Things, and robotics (Wheeler 2019).

The 5G is a software-driven network and as Tom Wheeler (2019), former chairman of the US Federal Communications Commission, observed: "5G may be the last physical network overhaul in generations as upgrades will now be only a matter of replacing software and low-cost, commodity components." Given that 5G networks are defined and managed by software, the vendors who would continually update and patch them "will have persistent access to the network's most sensitive operations and functionality" (Grotto 2019). This characteristic of the future 5G networks reveals a significant security concern of which governments and telecommunications service providers are aware. Talking about

other risks, Roxana Radu and Cedric Amon (2021) conclude that "the most pressing 5G threats fall in the three main traditional categories of cybersecurity risk, being related to the compromise of confidentiality [spying on traffic and data circulated], availability [disruptions to the 5G networks] and integrity [modifications or alterations of traffic and information systems]".

II. The 5G rollout and divergent policy responses

Against the background of diverse risks emanating from the 5G rollout, which consist of a bundle combining national security, economic and societal considerations, governments have been evaluating the long-term effects of the security of their 5G infrastructure. These evaluations result in different policy responses that are summarized below.

Five Eyes Alliance

Countries comprising the Five Eyes intelligence sharing network – Australia, Canada, New Zealand, the United Kingdom, and the United States – have an uncompromising stance on the issue of Huawei and its participation in their 5G network. Specifically, all of these countries banned Huawei-produced equipment and services from their 5G networks.

EU risk-based approach

The EU's position on this matter is defined by indistinct delimitation of competences between the European Union and its Member States when it comes to the 5G technology (Robles-Carrillo 2021). At the Union level, the following steps were undertaken: in March 2019, the European Commission issued Recommendation 2019/534 and compelled Member States to carry out a risk assessment of the 5G network infrastructure, based on the Member States' input a coordinated European risk assessment was conducted and the relevant report was released in October 2019, which was followed by the release of 'Cybersecurity of 5G networks: EU toolbox of risk mitigating measures'.

The EU coordinated risk assessment of the cybersecurity of 5G networks emphasizes that the risk profiles of individual suppliers can be assessed on the basis of several factors, among which the most essential is "[t]he likelihood of the supplier being subject to interference from a non-EU country." Furthermore, it has been highlighted that "[t]his is one of the key aspects in the assessment of non-technical vulnerabilities related to 5G networks." In order to overcome the risks associated with high-risk vendors, the EU toolbox of risk mitigating measures proposes to apply restrictions for suppliers considered to be high-risk.

Divergent stances in the Indo-pacific region

Japan decided to ban government purchases of telecommunications products from Huawei and ZTE Corp (Reuters 2018). Following this, the country's main mobile carriers decided not to use Huawei equipment in the 5G rollout (Kharpal 2019). A strong desire to avoid any confrontation with the main security (i.e., United States) and trade (i.e., China) partners defines South Korean policies on Huawei. South Korea did not impose any restrictions on the use of Huawei-produced equipment or services in its 5G networks, thus triggering a discussion on "digital entanglement" as a policy pursued by China in the region (Lee et al., 2020).

Switzerland: “dependence is hardly avoidable”

The issue of Huawei and its participation in the 5G rollout was discussed in the Swiss Parliament. In March 2019, a group of parliamentarians submitted a formal request to inquire more information on the issue from the Swiss Federal Council (Regazzi 2019), which functions as the executive body of the federal government and the collective head of state. In its response, the Federal Council emphasized that the US government did not present any evidence regarding alleged espionage allegations and the Huawei Cyber Security Evaluation Centre established in the United Kingdom has not provided any evidence either. Furthermore, it was highlighted that the global telecommunications market is increasingly dominated by a few globally active companies; as a result, all countries are dependent on a few global equipment suppliers. Switzerland did not introduce any restrictions targeting Chinese tech companies and allows its telecommunications service providers to make their procurement choices without any limitations.

As numerous states shore up legislation and administrative actions geared toward eliminating Huawei’s participation in their 5G networks, China has maintained a proactive posture. Analysts observe that “[l]eaders in Beijing are redoubling efforts to export Chinese fifth-generation wireless (5G) infrastructure, with notable success in Latin America, Africa, and central and eastern Europe” (Lee et al., 2020).

In its turn, Huawei, as the company bearing financial and reputational costs deriving from the prohibitions on its participation in the 5G rollout, seized the opportunity of calling into question the legality of such restrictions. Towards this end, the company initiated administrative proceedings and disputes at the domestic and international levels, a point to which we turn now.

III. Huawei’s response: litigation way for Huawei

Proceedings before domestic agencies and courts

To counter numerous restrictions implemented by the United States’ regulatory bodies targeting Huawei, the company relied upon the means of recourse offered by the US domestic legal system. Huawei took similar steps regarding measures introduced by the EU Member States, albeit at a smaller scale.

In 2018, John S. McCain National Defense Authorization Act for Fiscal Year 2019 was enacted. Pursuant to Section 889 of this Act, executive agencies are prohibited from (i) procuring Huawei-produced telecommunications equipment; (ii) contracting with the companies that use Huawei equipment or services; (iii) obligating or extending loan or grant funds to procure Huawei equipment and services. To challenge the constitutionality of Section 889, Huawei lodged a complaint at the United States District Court for the Eastern District of Texas in March 2019 (Huawei 2019). In essence, Huawei argued the unconstitutionality of Section 889 based on three grounds: (1) the Bill of Attainder Clause; (2) the Due Process Clause; and (3) the Vesting Clauses (Huawei Technologies USA, Inc. v. United States of America 2020). In the course of the court proceedings, the government argued that the primary purpose of Section 889 is “[t]o further national and informational security by protecting the networks of federal agencies, contractors, and grantees from the threat of cyber-attacks and -espionage by the Chinese government via companies in a position to exploit those networks.” The court dismissed all of Huawei’s legal claims.

In 2019, the FCC released an order and labeled two Chinese companies – Huawei and ZTE Corp. – as a threat to national security, and based on this determination government subsidies from the $8.5 billion

universal service fund could not be used to purchase their equipment and services (Federal Communications Commission 2019). The final designation order was issued on 30 June 2020; Huawei appealed it, and the FCC denied the appeal in December 2020 (Federal Communications Commission 2020).

Afterward, Huawei Technologies Co. Ltd., along with its unit Huawei Technologies USA Inc. filed a case before the 5th US Circuit Court of Appeals in order to overturn the FCC designation of Huawei as a national security threat and challenge its alleged ties to the Chinese military (Sevastopulo 2021). The crux of Huawei's legal claims is that such designation "was not based on evidence and that the agency [the FCC] exceeded its authority by making judgments about national security" (Canfield 2020). In June 2021, the court denied Huawei's petition for review (Huawei Technologies USA, Inc., vs. Federal Communications Commission 2021).

Over in Europe, Huawei either sent formal requests to competent authorities or launched court proceedings in response to various measures proposed or implemented by the EU Member States.

Discussions at the World Trade Organization

At least since 2018, China raised an issue of restrictions excluding Chinese companies from participation in the 5G networks at the WTO. It started with China's proposal to discuss Australian actions restricting the use of 5G equipment produced by Huawei and ZTE at the Committee on Market Access in October 2018 (WTO, Committee on Market Access 2019). During this meeting, China's representative argued that Australia introduced origin-based prohibitions on Chinese telecom products in violation of its commitments under Article I:1 (MFN), Article X (Publication and Administration of Trade Regulations), and Article XI (General Elimination of Quantitative Restrictions) of the GATT 1994. The Australian representative contended that the government's objective was to strengthen the security of Australia's telecommunications networks, and towards this end, additional requirements apply, which were origin-neutral and did not exclude Chinese suppliers. The issue was discussed at the subsequent meetings as well.

In 2021, China brought the issue of Sweden's restrictions on Huawei's participation in their 5G networks to the attention of the Council for Trade in Goods (WTO, Report of the Council for Trade in Goods 2021). Recently, in April 2022, Belgium's draft law introducing additional security measures for the provision of mobile 5G services was labeled by China as a special trade concern and included in the Council for Trade in Goods agenda (WTO, Report of the Council for Trade in Goods 2022).

Litigation before international investment tribunals

In 2020, the Swedish Post and Telecom Agency auctioned licensing rights in the 3.5 GHz and 2.3 GHz bands for the upcoming Swedish 5G network. In order to participate in this auction, authorized mobile network operators were prohibited from using equipment sourced from Huawei (Huawei Technologies Co., Ltd. v. The Kingdom of Sweden 2022).

After Huawei failed in domestic courts, Huawei initiated an ICSID arbitration based on the China-Sweden BIT in January 2022. This dispute appears to be the first investment dispute to question the legality of a country's decision to restrict Huawei from its domestic 5G network.

List of references

1. Duffy, C. 2020. "What is 5G? Your questions answered", CNN Business, https://edition.cnn.com/interactive/2020/03/business/what-is-5g/
2. Dahlman, E., Parkvall, S., and Sköld, J. 2018. "What Is 5G?" In: Dahlman, E., Parkvall, S., and Sköld, J. (Eds.), *5G NR: the Next Generation Wireless Access Technology*. Academic Press, pp. 1-6.
3. Robles-Carrillo, M. 2021. "European Union policy on 5G: Context, scope and limits," *Telecommunications Policy* 45(8):1-14.
4. Poliakine, R. 2021. 'What You Should Know About 5G Technology And What The Future Holds', Forbes, https://www.forbes.com/sites/forbestechcouncil/2021/08/12/what-you-should-know-about-5g-technology-and-what-the-future-holds/?sh=4d21cfd9636b
5. Remmert, H. 2019. '5G Applications and Use Cases', *DIGI*, https://www.digi.com/blog/post/5g-applications-and-use-cases
6. Wheeler, T. 2019. "5G in five (not so) easy pieces", Report adapted from a presentation made at the request of the Government Accountability Office, https://www.brookings.edu/research/5g-in-five-not-so-easy-pieces/
7. Grotto, A. 2019. "The Huawei problem: A risk assessment," *Global Asia* 14(3):13–15, https://www.globalasia.org/v14no3/cover/the-huawei-problem-a-risk-assessment_andrew-grotto
8. Radu, R. and Amon, C. 2021. "The governance of 5G infrastructure: between path dependency and risk-based approaches," *Journal of Cybersecurity* 7(1):1–16.
9. Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks, OJ L 88, 29.03.2019, p. 42–47, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019H0534,
10. EU coordinated risk assessment of the cybersecurity of 5G networks, 2019, https://digital-strategy.ec.europa.eu/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security
11. Cybersecurity of 5G networks: EU toolbox of risk mitigating measures, 2020, https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures
12. Reuters, 2018. "Japan to ban Huawei, ZTE from govt contracts-Yomiuri", https://www.reuters.com/article/japan-china-huawei-idUSL4N1YB6JJ
13. Kharpal, A. 2019. "Here's which leading countries have barred, and welcomed, Huawei's 5G technology", CNBC, https://www.cnbc.com/2019/04/26/huawei-5g-how-countries-view-the-chinese-tech-giant.html
14. Lee K., Rasser M., Fitt J. and Goldberg C. 2020. "Digital Entanglement: Lessons Learned from China's Growing Digital Footprint in South Korea", Center for a New American Security, https://www.cnas.org/publications/reports/digital-entanglement
15. Regazzi, F. 2019, Interpellation: Huawei und die Herausforderungen von 5G. Risiken und Chancen für die Schweiz, https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193051
16. John S. McCain National Defense Authorization Act for Fiscal Year 2019, Public Law 115-232, https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf
17. Huawei, 2019. "Huawei Sues the U.S. Government for Unconstitutional Sales Restrictions Imposed by Congress", https://www.huawei.com/en/news/2019/3/huawei-sues-the-us-government
18. Huawei Technologies USA, Inc. and Huawei Technologies Co., LTD. v. United States of America, et al. 2020. United States District Court Eastern District of Texas, Memorandum Opinion and Order, https://docs.justia.com/cases/federal/district-courts/texas/txedce/4:2019cv00159/188186/51
19. Federal Communications Commission, 2019. Report and Order In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, WC Docket No. 18-89, PS Docket No. 19-351, PS Docket No. 19-352, https://www.fcc.gov/document/protecting-national-security-through-fcc-programs-0
20. Federal Communications Commission, 2020. Memorandum Opinion and Order In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – Huawei Designation. PS Docket No. 19-351, https://www.fcc.gov/document/fcc-affirms-designation-huawei-national-security-threat-0
21. Sevastopulo, D. 2021. "Huawei challenges its designation as a threat to US security", Financial Times, https://www.ft.com/content/b7c2294d-9207-4fae-8fed-d63a80c99618
22. Canfield, S. 2020. "Huawei Challenges FCC Security Risk Label at Fifth Circuit", Courthouse News Service, https://www.courthousenews.com/huawei-challenges-fcc-security-risk-label-at-fifth-circuit/,

23. Huawei Technologies USA, Inc., Huawei Technologies Co. LTD, vs. Federal Communications Commission, 2021. United States Court of Appeals for the Fifth Circuit.
24. WTO, Committee on Market Access, 2019. Minutes of the Committee on Market Access 9 October 2018, https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/G/MA/M68.pdf&Open=True
25. WTO, Report of the Council for Trade in Goods, 2021. WTO Doc. G/L/1418, https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/G/L/1418.pdf&Open=True
26. WTO, Report of the Council for Trade in Goods, 2022. WTO Doc. G/L/1463, https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/G/L/1463.pdf&Open=True
27. Huawei Technologies Co., Ltd. v. The Kingdom of Sweden, Request for Arbitration, 2022. https://jusmundi.com/en/document/other/en-huawei-technologies-co-ltd-v-kingdom-of-sweden-request-for-arbitration-friday-7th-january-2022