world trade institute

# Politicization of the 5G Rollout: Litigation Way for Huawei?

Iryna Bogdanova

WTI working paper no. 01/2023

b
UNIVERSITÄT
BERN

# Politicization of the 5G Rollout: Litigation Way for Huawei?

**Dr Iryna Bogdanova***

## Introduction

The People's Republic of China (China) ambition to become a global leader in emerging and foundational technologies, which is partly channeled through state-led industrial efforts such as Made in China 2025,[1] prompted a strong response. For example, the United States significantly tightened its export control regulations restricting China's ability to purchase and manufacture high-end chips[2] and expanded grounds for foreign direct investment screening by empowering the Committee on Foreign Investment in the United States (CFIUS) to review the transaction's effect on US technological leadership in specified industries before approving potential investments[3]. The European Union (EU), responding to the emerging great-power rivalry between the United States and China, has been pursuing the multidimensional policy of technological sovereignty proclaimed by Ursula von der Leyen in her 2019 political guidelines.[4] These developments labeled as a "technological de-coupling" emerged in response to China's significantly propelled potential and ambition to lead the technological race[5] and coincided in time with the rollout of the 5G infrastructure, surrounded by controversy over the involvement of Chinese tech companies in the process.

In this global context, politicization and securitization of the 5G rollout seem almost unavoidable.[6] This outcome emanates not only from the vivid geopolitical tensions but also from the nature and

* Iryna Bogdanova (Iryna.Bogdanova@wti.org) is a postdoctoral researcher at the World Trade Institute, University of Bern. Her current research project "Technological sovereignty: the emergence of a novel concept, its implementation and implications for international economic law" is financed by the Swiss National Science Foundation, SNSF grant number: IZSEZ0_212037. The author sincerely thanks Dr Zaker Ahmad and Yann Fauconnet for their valuable comments on an earlier draft.

[1] Institute for Security & Development Policy, 2018. "Made in China 2025", Backgrounder, https://isdp.eu/content/uploads/2018/06/Made-in-China-Backgrounder.pdf, accessed on 16 January 2023.

[2] US Department of Commerce, Bureau of Industry and Security, 2022. "Commerce Implements New Export Controls on Advanced Computing and Semiconductor Manufacturing Items to the People's Republic of China (PRC)", https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3158-2022-10-07-bis-press-release-advanced-computing-and-semiconductor-manufacturing-controls-final/file, accessed on 16 January 2023.

[3] Biden, J.R. 2022. Executive Order on Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States (Executive Order 14083), https://www.whitehouse.gov/briefing-room/presidential-actions/2022/09/15/executive-order-on-ensuring-robust-consideration-of-evolving-national-security-risks-by-the-committee-on-foreign-investment-in-the-united-states/ accessed on 16 January 2023.

[4] von der Leyen, U. 2019. "Political guidelines for the next European Commission 2019-2024", Speech in the European Parliament plenary session 27 November 2019, https://op.europa.eu/en/publication-detail/-/publication/62e534f4-62c1-11ea-b735-01aa75ed71a1/language-en, accessed on 16 January 2023.

[5] Bateman, J. 2022. "U.S.-China Technological "Decoupling": A Strategy and Policy Framework", Carnegie Endowment for International Peace, https://carnegieendowment.org/files/Bateman_US-China_Decoupling_final.pdf, accessed on 16 January 2023.

[6] "[…] every major issue associated with 5G networks has become politicized." Eurasia Group, 2018. "The Geopolitics of 5G", White Paper, https://www.eurasiagroup.net/siteFiles/Media/files/1811-

economic implications of the 5G that give rise to various types of national security risks, a point to which we will return later. Taking this as a starting point, the working paper briefly explains the economic implications and the national security risks of the 5G rollout. Following this, government policies on Chinese companies' participation in the 5G rollout are outlined. While many governments introduced policies curbing Chinese companies' participation in their 5G infrastructure, some of these companies, for example, Chinese technology giant Huawei Technologies Co., Ltd. (Huawei), devised a litigation strategy in an attempt to overturn such policies. This working paper explores Huawei's litigation strategy, which can be characterized by the use of domestic and international adjudicatory bodies as well as the invocation of national security as a justification for such policies. The latter aspect reflects the dominant trend toward politicization and securitization of the 5G.

### A. 5G technology: economic implications of its rollout and relevant national 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).[7] 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).[8]

Economic implications of the 5G rollout are far-reaching: analysts have argued that the rollout of 5G "holds the key to shaping the future of practically every industry by drastically transforming the way machines interact and function".[9] Thus, 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".[10]

---

14%205G%20special%20report%20public(1).pdf, accessed on 16 January 2023; Karsten Friis and Olav Lysne contend that the 5G rollout and the involvement of Chinese suppliers in the process were "securitized", in other words "[t]he topic was elevated from the realm of ordinary politics and treated as an emergency, thus legitimizing extraordinary countermeasures." Friis, K. and Lysne, O. 2021. "Huawei, 5G and Security: Technological Limitations and Political Responses," *Development and Change* 52(5):1174–1195.

[7] Duffy, C. 2020. "What is 5G? Your questions answered", CNN Business, https://edition.cnn.com/interactive/2020/03/business/what-is-5g/, accessed on 16 January 2023.

[8] 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.

[9] 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, accessed on 16 January 2023.

[10] Robles-Carrillo, M. 2021. "European Union policy on 5G: Context, scope and limits," *Telecommunications Policy* 45(8):1–14.

Talking about the risks to the 5G infrastructure, Roxana Radu and Cedric Amon 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]".[11] Indeed, the ability of 5G to connect billions of new devices augments existing risks: successful espionage efforts can potentially hand over troves of data, including commercially sensitive data and private data, to foreign governments and industry competitors.

Bearing in mind that the building of the 5G network "requires massive capital investment"[12] and that the alleged Chinese government subsidization of Huawei brings prices for the 5G equipment significantly down,[13] the following question arises: What are the risks that compel states to introduce restrictions preventing Chinese tech companies (mainly Huawei) from participating in their 5G infrastructure projects? The answer to this question lies in the nature of the 5G network and in the nature of Chinese tech companies.

The 5G is a software-driven network and as Tom Wheeler, 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."[14] As a result, the 5G and the infrastructure required for this technology to function can be labeled by states as a "critical technology" and a "critical infrastructure" respectively. 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."[15] This characteristic of the future 5G networks reveals another security concern of which governments and telecommunications service providers are aware.

---

[11] 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.

[12] Poliakine (n 9).

[13] Nakashima, E. 2019. "U.S. pushes hard for a ban on Huawei in Europe, but the firm's 5G prices are nearly irresistible", The Washington Post, https://www.washingtonpost.com/world/national-security/for-huawei-the-5g-play-is-in-europe--and-the-us-is-pushing-hard-for-a-ban-there/2019/05/28/582a8ff6-78d4-11e9-b7ae-390de4259661_story.html, accessed on 16 January 2023; "[…] Huawei reports receiving hundreds of millions of dollars in government grants every year, including more than US$220 million in 2018. It also has a US$100 billion line of credit from Chinese state-owned banks that enables it to offer financing to customers at below market interest rates." 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, accessed on 16 January 2023.

[14] 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/, accessed on 16 January 2023.

[15] Grotto (n 13).

The reasons behind Huawei's designation as a "high-risk vendor" can be succinctly summarized as follows: unclear ownership structure; potential affiliation with the Chinese military and long-standing espionage allegations.[16] Furthermore, the relationship between the Chinese Communist Party and China-based companies, which has been vividly described by Andrew Grotto in the following words "the Chinese government considers Chinese companies to be extensions of the state, whether a company likes it or not",[17] also magnifies the existing frictions. Another stumbling block for building trust between Chinese tech companies and foreign governments is the National Intelligence Law of the People's Republic of China (2017),[18] which requires Chinese citizens and companies to cooperate with the Chinese intelligence agencies[19] and assist them in their intelligence work[20]. Thus, concerns regarding Huawei's participation in the 5G projects can sprout from different roots.

### B. Government policies on Chinese companies' participation in the 5G rollout

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 – some states introduce blanket bans on Chinese companies' participation in their 5G networks (e.g., Australia), others prefer risk-based government policies (e.g., the EU) and some allow their telecommunications service providers to make their own procurement choices (e.g., Switzerland). It should be noted that the prevailing majority of the restrictions against Chinese companies in the context of the 5G rollout target Huawei, a China-based company that is not only one of the largest global network equipment makers but also one of the primary holders of a significant share of 5G standard essential patents.[21]

Since 2018, a growing number of states have either explicitly banned Huawei or taken other regulatory steps to exclude Huawei from their 5G networks.[22] The gamut of the undertaken

[16] In a similar vein, Gregory Moore contends that "it is Huawei's business model, the nature of the Chinese Communist Party, and the legal relationship between Huawei (and potentially any Chinese company) and the Chinese state that create a potential security problem for nations that do 5G business with Huawei." Moore, G.J. 2022. "Huawei, Cyber-Sovereignty and Liberal Norms: China's Challenge to the West/Democracies," *Journal of Chinese Political Science*, https://doi.org/10.1007/s11366-022-09814-2.

[17] Grotto (n 13).

[18] National Intelligence Law of the People's Republic of China, http://www.npc.gov.cn/npc/c30834/201806/483221713dac4f31bda7f9d951108912.shtml, accessed on 16 January 2023.

[19] Wheeler (n 14).

[20] Nakashima (n 13).

[21] Eurasia Group (n 6).

[22] Sacks, D. 2021. "China's Huawei Is Winning the 5G Race. Here's What the United States Should Do To Respond", https://www.cfr.org/blog/china-huawei-5g, accessed on 16 January 2023.

measures is diverse: it includes both formal and informal actions (e.g., the use of diplomatic pressure to influence other countries not to use Chinese components in their 5G infrastructure[23]), domestic and international activities (e.g., use of intelligence-sharing partnerships such as the Five Eyes network to argue in favor of Huawei's exclusion from the 5G networks), economic policy measures and non-economic policy measures.

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. Australia's ban on Huawei was a harbinger of the future trend: in 2012, following a number of events, including cyberattacks targeting Australia and originated presumably from China, the Australian government prohibited Huawei from its National Broadband Network,[24] and in 2018, by labeling Huawei and its equipment as an unacceptable security risk, Australia formally banned it from its 5G network[25]. A few months later, New Zealand followed suit.[26] Other states have not stood idly either.

The United States has been voicing concerns regarding Huawei, its links with the Chinese government and military as well as potential risks of espionage and sabotage that emanate from the use of Huawei's equipment at least since 2012.[27] These concerns were expressed in a report on Huawei and ZTE Corporation released by the US House of Representatives Permanent Select Committee on Intelligence.[28] As the testing of the 5G technologies started, the US government began enacting various types of restrictions against Huawei. Starting from 2017, the US government implemented policies aimed at restricting the use of Huawei equipment: first, it was prohibited to use Huawei equipment in certain Department of Defence networks, and later this prohibition was extended to all US federal agencies.[29] Furthermore, federal agencies were prohibited from entering into a contract with an entity that uses equipment, systems, or services provided by Huawei and

[23] Ibid.

[24] Peng, S. 2015. "Cybersecurity Threats and the WTO National Security Exceptions," *Journal of International Economic Law* 18(2): pp. 449–478, https://doi.org/10.1093/jiel/jgv025.

[25] BBC News, 2018. "Huawei and ZTE handed 5G network ban in Australia", https://www.bbc.com/news/technology-45281495, accessed on 16 January 2023.

[26] CNBC, 2018. "New Zealand rejects Huawei's first 5G bid citing national security risk", https://www.cnbc.com/2018/11/28/new-zealand-rejects-huaweis-5g-bid-citing-national-security-risk.html, accessed on 16 January 2023.

[27] Gallagher, J. C. 2022. "U.S. Restrictions on Huawei Technologies: National Security, Foreign Policy, and Economic Interests", Congressional Research Service Report R47012.

[28] US Congress, House Permanent Select Committee on Intelligence, 2012. "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE", https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=96, accessed on 16 January 2023.

[29] Gallagher (n 27).

several other Chinese companies.[30] The implementation of this rule was fraught with difficulties.[31] Later, the government funded the replacement of the existing Huawei equipment in the US networks, which has been widespread mostly in the rural areas of the country.[32]

In the course of the last years, as the race for technological superiority persists, the United States not only engaged in multifaceted efforts to ban Huawei from its telecommunications networks but also introduced other restrictions, e.g., tightened export restrictions.[33] The predominant majority of these US policies declare that they pursue two objectives: they enhance the security of the US networks and secure supply chains for information and communications technology and services.[34] Before 2020, the United Kingdom allowed Huawei to provide equipment for the "non-core" parts of the country's 5G network.[35] In other words, the regulators followed the standard according to which the network is divided between "core" and "non-core" parts, although the soundness of this division in the context of 5G is questioned by experts.[36] However, in 2020, the tide turned: the United Kingdom decided to terminate its cooperation with Huawei and as a result, already installed 5G infrastructure should be removed by 2027.[37] Security arrangements, for the most part, the country's participation in the Five Eyes intelligence sharing network, and close political affinity with the United States could explain this rapid shift.[38]

---

[30] Ibid.

[31] Ibid.

[32] "In March 2020, Congress […] created a program to "rip and replace" untrusted equipment in U.S. networks (P.L. 116-124), and later appropriated $1.9 billion for the program (P.L. 116-260, §901)." Ibid.

[33] Mulligan S. P. and Linebaugh C. D. 2021. "Huawei and U.S. Law", Congressional Research Service Report R46693, https://sgp.fas.org/crs/misc/R46693.pdf , accessed on 16 January 2023.

[34] For example, Executive Order 13873 declared a national emergency regarding the threat that emanates from "the unrestricted acquisition or use in the United States of information and communications technology or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries". Trump. D. J. 2019. Executive Order on Securing the Information and Communications Technology and Services Supply Chain (Executive Order 13873), https://www.govinfo.gov/content/pkg/FR-2019-05-17/pdf/2019-10538.pdf, accessed on 16 January 2023.
In May 2022, President Biden continued the national emergency declared in Executive Order 13873 for one year. Biden, J.R. 2022. Notice on the Continuation of the National Emergency with Respect to Securing the Information and Communications Technology and Services Supply Chain, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/05/12/notice-on-the-continuation-of-the-national-emergency-with-respect-to-securing-the-information-and-communications-technology-and-services-supply-chain-2/, accessed on 16 January 2023.

[35] Brooks, T. 2019. "Huawei's participation is a brave step for British 5G networks", CGTN, https://news.cgtn.com/news/3d3d774e786b6a4d34457a6333566d54/index.html, accessed on 16 January 2023.

[36] "The next generation of mobile networks will also blur the traditional distinction between the radio access network (RAN), consisting of base stations and antennas that handle the radio frequency (wireless) portion of the network, and the core portion, including central switching and transport networks that carry large amounts of data traffic. This is because the architecture of 5G pushes a lot of what would be formerly core functionality out to the "edge" of the network, with big implications for 5G network security." Eurasia Group (n 7).

[37] Gold, H. 2020. "UK bans Huawei from its 5G network in rapid about-face", CNN Business, https://edition.cnn.com/2020/07/14/tech/huawei-uk-ban/index.html, accessed on 16 January 2023.

[38] Radu and Amon (n 11).

Canada joined similarly-minded political allies in May 2022 by banning Huawei and ZTE from its 5G networks,[39] a move that has been already described as a "long-awaited decision"[40]. Acknowledging Chinese companies' alleged dependence from their state apparatus and the risks inherent in a potential breach of Canada's telecommunications supply chain, the Canadian government announced that "it intends to prohibit Canadian telecommunications service providers from deploying Huawei and ZTE products and services in their 5G networks".[41] For this reason, the existing 5G equipment and services provided by these companies should be removed or terminated by 28 June 2024.[42]

Japan decided to ban government purchases of telecommunications products from Huawei and ZTE Corp.[43] According to media reports, this lead to the decision of the country's main mobile carriers not to use Huawei equipment in the 5G rollout.[44]

South Korea's position on the use of Huawei equipment in its 5G networks is ambivalent: as John Hemmings accurately points out the "technology cold war" between the United States and China "puts South Korea squarely between its main security provider and its main trading partner."[45] In other words, a strong desire to avoid any confrontation with the main security and trade partners defines South Korean policies on Huawei and its role in the country's 5G infrastructure. 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.[46]

The EU's position on this matter is defined not only by its aspiration to become self-sufficient in critical technologies[47] and its cooperation with the United States under the EU-US Trade and

[39] Innovation, Science and Economic Development Canada, 2022. "Policy Statement: Securing Canada's Telecommunications System", https://www.canada.ca/en/innovation-science-economic-development/news/2022/05/policy-statement--securing-canadas-telecommunications-system.html, accessed on 16 January 2023.

[40] Carvin, S. 2022. "Banning Huawei Was the Start, Not the End, of Protecting Cyber Infrastructure", CIGI, https://www.cigionline.org/articles/banning-huawei-was-the-start-not-the-end-of-protecting-cyber-infrastructure/ accessed on 16 January 2023.

[41] Innovation, Science and Economic Development Canada (n 39).

[42] Ibid.

[43] Reuters, 2018. "Japan to ban Huawei, ZTE from govt contracts -Yomiuri", https://www.reuters.com/article/japan-china-huawei-idUSL4N1YB6JJ, accessed on 16 January 2023.

[44] 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, accessed on 16 January 2023.

[45] Hemmings, J. 2020. "South Korea's Growing 5G Dilemma", Center for Strategic and International Studies, https://www.csis.org/analysis/south-koreas-growing-5g-dilemma, accessed on 16 January 2023.

[46] 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, accessed on 16 January 2023.

[47] von der Leyen (n 4).

Technology Council[48] but also by indistinct delimitation of competences between the European Union and its Member States when it comes to the 5G technology[49]. At the Union level, the following steps were undertaken: in March 2019, the EU Commission issued Recommendation 2019/534 and obligated Member States to carry out a risk assessment of the 5G network infrastructure,[50] based on the Member States' input a coordinated European risk assessment was conducted and the relevant report was released in October 2019,[51] which was followed by the release of 'Cybersecurity of 5G networks: EU toolbox of risk mitigating measures' (EU toolbox of risk mitigating measures)[52].

Among various types of security threats, the EU coordinated risk assessment of the cybersecurity of 5G networks highlights supplier-specific vulnerabilities.[53] In particular, it has been emphasized 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."[54] Furthermore, it has been emphasized that "[t]his is one of the key aspects in the assessment of non-technical vulnerabilities related to 5G networks."[55] In order to overcome the risks associated with high-risk vendors, the EU toolbox of risk mitigating measures, which groups mitigating measures into strategic and technical categories, proposes to assess the risk profile of suppliers and apply restrictions for suppliers considered to be high-risk.[56] Besides, it is recommended that the EU Member States exchange best practices on their national frameworks for assessing suppliers' risk profiles.[57] In this way the concept of a "high-risk vendor" has been engrained, thus allowing EU Member States to exclude the companies that possess risks to national security from their respective markets.

---

[48] EU-US Trade and Technology Council, https://ec.europa.eu/info/strategy/priorities-2019-2024/stronger-europe-world/eu-us-trade-and-technology-council_en, accessed on 16 January 2023.

[49] "[…] 5G is a novel area of competence. As such it is not assigned to a single authority, but rather involves the competences of the Union on the one hand, and those of its Member States on the other. While Member States have started to adopt measures based on national interest or security grounds, the EU has recognised that the security of 5G networks is a matter of strategic importance which requires a common European approach." Robles-Carrillo (n 10).

[50] 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, accessed on 16 January 2023.

[51] 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, accessed on 16 January 2023.

[52] 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, accessed on 16 January 2023.

[53] EU coordinated risk assessment of the cybersecurity of 5G networks (n 51).

[54] Ibid.

[55] Ibid.

[56] Cybersecurity of 5G networks: EU toolbox of risk mitigating measures (n 52).

[57] Ibid.

A number of EU and non-EU Member States signed with the United States Memorandums of Understanding (MoU), which among other things stipulate their desire to exclude suppliers who lack transparent ownership and are subject to foreign influence from their 5G networks.[58] Along with this, the draft Transatlantic Telecommunications Security Act, which provides actions that should be undertaken by the United States to improve the security of the telecommunications networks (5G and future generations) in Central and Eastern European countries, was passed by the House and is now under consideration at the Senate.[59] This resolve to cooperate with Central and Eastern European countries illustrates the US strategy to counter Chinese influence in the region.

The issue of Huawei and its participation in the 5G rollout was also discussed in the Swiss Parliament (*Bundesversammlung*). In March 2019, a group of parliamentarians submitted a formal request (*Interpellation*) to inquire more information on the issue from the Swiss Federal Council,[60] which functions as the executive body of the federal government and the collective head of state. In its response, the Federal Council expounded on the four aspects: (i) the US government did not present any evidence regarding alleged espionage allegations and in the meantime, the Huawei Cyber Security Evaluation Centre established in the United Kingdom has not provided any evidence of Huawei's equipment being used for espionage; (ii) global market of telecommunications is increasingly dominated by the United States and China, and while it is advisable for Switzerland not to take sides in the increasing tension between the two, the Swiss population and economy should be protected from various types of cybersecurity risks and this should be achieved through the relevant cybersecurity regulation; (iii) for the construction of their telecommunications networks, the Swiss telecommunications service providers procure the corresponding technologies and services by themselves and for this purpose select equipment offered by suppliers available on the market; (iv) in view of the high investments for the development and production of corresponding network components, only a few globally active companies can operate on this market and resulting dependencies on such equipment suppliers affect all countries and are hardly avoidable at present.[61] As of this writing, Switzerland did not introduce any restrictions or prohibitions targeting Chinese tech companies and allows its telecommunications service providers to make their

[58] Cerulus, L. 2020. "Huawei challenges legality of 5G bans in Poland, Romania", Politico, https://www.politico.eu/article/huawei-hints-at-legal-action-against-5g-bans-in-poland-romania/#, accessed on 16 January 2023.

[59] Transatlantic Telecommunications Security Act (H.R.3344), https://www.congress.gov/bill/117th-congress/house-bill/3344/text, accessed on 16 January 2023.

[60] 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, accessed on 16 January 2023.

[61] Ibid.

procurement choices without any limitations, i.e., the country defers to private industry on the use of Chinese equipment.

As numerous states shore up legislation and administrative actions geared toward eliminating Huawei's participation in their 5G networks, China has maintained its proactive posture and signed Memorandums of Understanding (MoU) with a number of countries as a part of its Digital Silk Road project.[62] Some of these MoU guarantee market access for Chinese tech companies, including their access to 5G rollout. Analysts from the Center for a New American Security 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."[63]

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.

### C. Huawei's litigation strategy: what do we know so far?

Alain Pellet and Tessa Barsac describe litigation strategy as a "multifaceted and dynamic concept",[64] which among other things "implies choices concerning the mode of settlement to be used, the forum to be seised and the size and composition of the bench"[65]. In the context of restrictions prohibiting Huawei from participation in the 5G rollout, the company's litigation strategy has been so far multidimensional: Huawei seized all available opportunities and initiated administrative proceedings, and disputes before domestic and international tribunals.

#### *I. Proceedings before domestic agencies and disputes before domestic 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-

[62] Eurasia Group 2020. "The Digital Silk Road: Expanding China's Digital Footprint", https://www.eurasiagroup.net/files/upload/Digital-Silk-Road-Expanding-China-Digital-Footprint-1.pdf, accessed on 17 January 2023.

[63] Lee et al. (n 46).

[64] Pellet, A. and Barsac, T. 2019. "Litigation Strategy", Max Planck Encyclopedia of International Law, https://opil.ouplaw.com/view/10.1093/law-mpeipro/e3109.013.3109/law-mpeipro-e3109?prd=OPIL, accessed on 17 January 2023.

[65] Ibid.

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.[66] 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.[67] 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.[68] 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."[69]

From the beginning, some legal commentators were skeptical of Huawei's chances to succeed and they noted that this dispute might pursue two objectives: first, re-establish Huawei's reputation, i.e. "an effort to clear itself of accusations that it is a security threat",[70] and second, challenge the legitimacy of US accusations by "force[ing] the federal government to provide more evidence to support its allegations of so-called backdoors in Huawei's equipment"[71]. Despite this skepticism, it is worthwhile to briefly analyze Huawei's arguments and the court's decision.

The Bill of Attainder Clause reads as follows: "No Bill of Attainder or ex post facto Law shall be passed."[72] In *United States v. Lovett*, the court described the rationale behind this clause as a prohibition of all legislative acts "no matter what their form, that apply either to named individuals or to easily ascertainable members of a group in such a way as to inflict punishment on them without a judicial trial".[73] To decide whether the Bill of Attainder applies the two-pronged test was developed: "First, has the legislature acted with specificity? Second, has it imposed punishment?".[74]

---

[66] 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, accessed on 17 January 2023.
[67] 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, accessed on 17 January 2023.
[68] 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, accessed on 17 January 2023.
[69] Ibid.
[70] Ide, B. and Huang, J. 2019. "China's Huawei Sues US Government Over Ban", VOA, https://www.voanews.com/a/china-s-huawei-sues-us-government-over-ban/4817139.html, accessed on 17 January 2023.
[71] Ibid.
[72] The United States Constitution, Article I, Section 9: Powers Denied Congress, https://constitutioncenter.org/the-constitution/full-text, accessed on 17 January 2023.
[73] United States v. Lovett, consolidated with United States v. Watson, and United States v. Dodd. 1946. Supreme Court of the United States, https://www.law.cornell.edu/supremecourt/text/328/303, accessed on 17 January 2023.
[74] Huawei Technologies USA, Inc. and Huawei Technologies Co., LTD. v. United States of America, et al. (n 68).

The court in *Huawei Techs. USA, Inc. v. United States* agreed with Huawei that Section 889 meets the specificity prong and thoroughly analyzed the requirement of punishment, which consists of a three-part inquiry, i.e. the "historical test", the "functional test", and the "motivational test".[75] Regarding the "historical test", Huawei argued that Section 889 is an improper bill of attainder under three historical "punishments": (1) brand of disloyalty and infamy; (2) employment bar; and (3) banishment.[76] In this regard, the court decided the following: (i) Section 889 is not a statute that rises to the level of punishment based on infamy and disloyalty; (ii) Section 889 does not preclude Huawei from engaging in its chosen profession; (iii) Huawei is not being permanently banned from doing business in the United States and thus, Section 889 does not meet the historical definition of punishment for banishment.[77] When analyzing Huawei's arguments, the court drew parallels to the court decision, in which constitutionality of the section 1634 of the 2018 NDAA prohibiting the use of Kaspersky Lab products was stipulated.[78] Entrusted with the task of defining whether Section 889 establishes a "punishment" for the purposes of the Bill of Attainder under the "functional test", the court first identified the purpose of Section 889, then evaluated the balance between the burden imposed and identified purpose in order to determine if the statute is "reasonably tailored".[79] The conclusion of the court was that "given the reasonable balance between the burden[s] imposed by [Section 889] and the nonpunitive [national security, informational security, and federal funding] objective[s] it furthers, [the Court] easily concludes that Congress has not done so here ["piling on . . . additional, entirely unnecessary burden[s]"]."[80] With respect to the "motivational test", which is defined as "inquiring whether the legislative record evinces a congressional intent to punish", the court decided that the legislative record does not provide the required evidence of punitive intent, and thus, the requirements of this test were not met.[81]

The Due Process Clause of the Fifth Amendment provides, in relevant part, that "[n]o person shall … be deprived of life, liberty, or property, without due process of law."[82] Emphasizing that "contracting with the federal government is a privilege, not a constitutionally guaranteed right", the court concluded that: "Despite Section 889's particularized nature and its impact on Huawei's

[75] Ibid.
[76] Ibid.
[77] Ibid.
[78] Kaspersky Lab, Inc. and Kaspersky Labs Limited, Appellants v. United States Department of Homeland Security. 2018. United States Court of Appeals for the District of Columbia Circuit, https://casetext.com/case/kaspersky-lab-inc-v-us-dept-of-homeland-sec-kirstjen-m-nielsen, accessed on 17 January 2023.
[79] Huawei Technologies USA, Inc. and Huawei Technologies Co., LTD. v. United States of America, et al. (n 68).
[80] Ibid.
[81] Ibid.
[82] The United States Constitution (n 72).

current and future contractual relationships, it is rationally related to a legitimate congressional purpose and thus does not violate Huawei's due process rights."[83]

The Vesting Clauses provide that "[a]ll legislative Powers herein granted shall be vested in a Congress of the United States"; that "[t]he executive Power shall be vested in a President of the United States"; and that "[t]he judicial Power of the United States, shall be vested in one supreme Court, and in such inferior Courts as the Congress may from time to time ordain and establish."[84] The essence of Huawei's claim is that when Congress enacted Section 889, it adjudicated facts and applied the law to Huawei and this action violates the Vesting Clauses.[85] Huawei further clarified that "because Section 889 adjudicates that Huawei is connected to the Chinese government, Section 889 does prevent the Executive and Judicial branches from performing their constitutional functions."[86] In the court's view, "Section 889–part of an appropriations bill–is the upshot of an "inherent[ly]" congressional function. […] It does nothing to prevent the other two branches of government from performing their vested constitutional functions. Accordingly, Huawei's challenge of Section 889 under the Vesting Clauses fails."[87]

The abovementioned analysis demonstrates that the court dismissed all of Huawei's legal claims.

In April 2018, the US Federal Communications Commission (FCC) issued a notice of proposed rulemaking, which put forward that the funds from the universal service funds could not be spent "to purchase or obtain any equipment or services produced or provided by any company posing a national security threat to communications networks or the communications supply chain."[88] This notice drew extensive comments, and it was in the context of this notice that Huawei contended that the proposed rule "would exceed the Commission's [FCC] statutory authority, would be arbitrary and capricious under the APA [Administrative Procedure Act], and would violate covered companies' due process rights".[89]

---

[83] Huawei Technologies USA, Inc. and Huawei Technologies Co., LTD. v. United States of America, et al. (n 68).
[84] The United States Constitution, Article I Section 1: Congress, Article II Section 1, and Article III Section 1 (n 72).
[85] Huawei Technologies USA, Inc. and Huawei Technologies Co., LTD. v. United States of America, et al. (n 68).
[86] Ibid.
[87] Ibid.
[88] Federal Communications Commission, 2018. Notice of Proposed Rulemaking in the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs, WC Docket No. 18-89, https://transition.fcc.gov/Daily_Releases/Daily_Business/2018/db0418/FCC-18-42A1.pdf, accessed on 17 January 2023.
[89] Huawei Technologies USA, Inc., Huawei Technologies Co. LTD, vs. Federal Communications Commission, 2021. United States Court of Appeals for the Fifth Circuit, https://www.docketalarm.com/cases/US_Court_of_Appeals_Fifth_Circuit/19-60896/Huawei_Tech_USA_v._FCC/00505905664/#q=party%3A%28Dell+Technologies%29+OR+party%3A%28Microsoft%29+OR+party%3A%28Samsung+Electronics%29+OR+party%3A%28LG+Electronics%29+OR+party%3A%28Lenovo%29+OR+party%3A%28Toshiba%29+OR+party%3A%28Huawei%29+OR+party%3A+%28Sony%29, accessed on 17 January 2023.

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.[90] The final designation order was issued on 30 June 2020, Huawei appealed it, and the FCC denied the appeal in December 2020.[91]

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.[92] The crux of Huawei's legal claims is that such designation "was not based on evidence and that the agency [FCC] exceeded its authority by making judgments about national security".[93] In June 2021, the court denied Huawei's petition for review based on the grounds summarized below.[94]

To overturn the FCC's order issued in November 2019, Huawei advanced the following legal arguments: (1) the order exceeded the FCC's statutory authority; (2) it was arbitrary, capricious, and an abuse of discretion under the Administrative Procedure Act (APA); (3) it was adopted in violation of the notice-and-comment requirements of 5 U.S.C. § 553; (4) it was void for vagueness and retroactive in violation of the Constitution and the APA; (5) it violated the Constitution's Appointments Clause and statutory and constitutional due process protections; and (6) it was otherwise contrary to law.[95] Huawei appealed both the FCC's order issued in November 2019 and the designation of Huawei as a national security threat as it was declared in the order.[96]

[90] 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, accessed on 17 January 2023.

[91] 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, accessed on 17 January 2023.

[92] 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, accessed on 17 January 2023.

[93] 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/, accessed on 17 January 2023.

[94] Huawei Technologies USA, Inc., Huawei Technologies Co. LTD, vs. Federal Communications Commission (n 89).**Error! Hyperlink reference not valid.**

[95] Ibid.**Error! Hyperlink reference not valid.**

[96] Ibid.**Error! Hyperlink reference not valid.**

The court dismissed part of Huawei's legal claims based on the ripeness doctrine,[97] which "prevent[s] the courts, through avoidance of premature adjudication, from entangling themselves in abstract disagreements over administrative policies."[98]

When faced with a need to decide whether the FCC exceeded its statutory authority, the court relied upon the *Chevron* two-step test to determine whether 47 U.S.C. §§ 254(c)(1)(D) and 201(b) (labeled as the "public interest" provisions) as well as 47 U.S.C. § 254(b)(1) (referred to as the "quality services" provision) grant authority to the FCC to designate Huawei as a national security threat. By applying the *Chevron* deference doctrine,[99] the court decided that firstly, as long as "the FCC asserts only the authority to consider national security concerns in the narrower sphere of regulating USF [Universal Service Fund] "support mechanisms"", these actions are covered by the existing FCC's regulatory authority[100] and secondly, the FCC reasonably interpreted the term "quality services" in § 254(b)(1) as supporting its limited exercise of national security judgment in defining "quality services" as "secure services".[101]

Huawei argued that the notice of proposed rulemaking issued by the FCC in April 2018 "failed to give adequate notice of the designation process adopted" in the FCC's November 2019 order.[102] According to the Administrative Procedure Act (APA), an agency must publish notice of the legal authority for a proposed rule and the substance of the rule; also, an opportunity for interested

[97] "Thus, Huawei cannot satisfy the first prong of the finality test as to the initial designation, and its challenges to that part of the order are unfit for judicial review. Accordingly, we must dismiss its claims related to the initial designation for lack of jurisdiction." Ibid.**Error! Hyperlink reference not valid.**

[98] Ibid.**Error! Hyperlink reference not valid.**

[99] The Chevron deference doctrine consists of two steps: a "court must first determine whether Congress "has spoken to the precise question at issue." If so, the inquiry ends, because the courts and agencies must "give effect to the unambiguously expressed intent of Congress." If the statute is silent or ambiguous regarding the specific point, the court decides whether the agency interpretation is "based on a permissible construction of the statute."" The United States Department of Justice, 2021. "Chevron, U.S.A. v. Natural Res. Def. Council, 467 U.S. 837 (1984)", https://www.justice.gov/enrd/chevron-usa-v-natural-res-def-council, accessed on 17 January 2023.

[100] "Against this backdrop, the USF Rule accords with the FCC's previous consideration of national security concerns in the communications realm. Under the rule, the FCC makes initial and final designations based on "all available evidence," including determinations by Congress, the President, and other executive agencies, as well as classified information, and it "seek[s] to harmonize its determinations" with those of other agencies and Congress. 34 FCC Rcd. at 11438–39. Thus, as in granting licenses under § 310(b)(4) and service certificates under § 214(a), the FCC's designation of an entity as a national security risk consistent with the public interest is informed by the views of expert agencies. We therefore conclude that the agency reasonably interpreted the public interest provisions, especially in light of its coincident authority under § 254(b)(1), to allow it to adopt the rule." Huawei Technologies USA, Inc., Huawei Technologies Co. LTD, vs. Federal Communications Commission (n 89). **Error! Hyperlink reference not valid.**

[101] Ibid. **Error! Hyperlink reference not valid.**

[102] Ibid. **Error! Hyperlink reference not valid.**

persons to participate in the rulemaking must be provided.[103] The court disagreed with Huawei and concluded that "the rulemaking fairly acquainted Huawei with the subject and issues delineated".[104] The next argument advanced by Huawei is that the FCC acted arbitrarily and capriciously in adopting the November 2019 order. Specifically, Huawei contended that the FCC failed to consider relevant evidence and legal arguments; that the FCC's cost-benefit analysis "ignored important aspects of the problem and is irrational"; and that the FCC rejected an alternate approach that would have "served its putative national security objective more effectively and at lower cost."[105] The court disagreed with these arguments and ruled that the FCC "acted within a zone of reasonableness."[106] Furthermore, Huawei claimed that the FCC's November 2019 order is vague and standardless in violation of the APA.[107] The crux of Huawei's argument is that the rule, which allows the designation of certain companies as a national security threat to the integrity of communications networks or communications supply chain, fails to define key terms such as "national security threat", "integrity", and "communications supply chain" and hence, this rule does not provide "meaningful guidance" to affected companies.[108] After conducting a thorough analysis of the case law presented by Huawei to substantiate its legal arguments, the court came to the conclusion that cited cases do not support Huawei's claims and rejected them.[109]

The last argument presented by Huawei is that the initial designation process "(1) "rests on an error of law," namely the assumption the agency could initially designate companies without process, and (2) fails to provide such procedures consistent with the Constitution."[110] The court reminded that the initial designation of Huawei might have potentially caused a reputational injury, yet the court quoted *Texas v. Thompson* wherein it was stated that "[a]llegations of damages to one's reputation" by a state actor's statements generally "fail to state a claim of denial of a constitutional right," unless they are "accompanied by an infringement of some other interest."[111] Finding no other interest requiring due process protection, the court dismissed Huawei's claims.[112] Furthermore, the court

[103] The Administrative Procedure Act, Public law 79-404, 5 U.S.C. §§ 553 (b)(2), (3), and § 553(c).
[104] Huawei Technologies USA, Inc., Huawei Technologies Co. LTD, vs. Federal Communications Commission (n 89). **Error! Hyperlink reference not valid.**
[105] Ibid.**Error! Hyperlink reference not valid.**
[106] Ibid.**Error! Hyperlink reference not valid.**
[107] Ibid.**Error! Hyperlink reference not valid.**
[108] Ibid.**Error! Hyperlink reference not valid.**
[109] Ibid.**Error! Hyperlink reference not valid.**
[110] Ibid.**Error! Hyperlink reference not valid.**
[111] Ibid.**Error! Hyperlink reference not valid.**
[112] Ibid.

agreed with the FCC that the November 2019 order afforded "pre-deprivation due process through the initial designation procedures".[113]

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. For example, in September 2020, in response to the 5G security rules proposed by Poland and Romania, Huawei sent an official letter to the EU competition chief Margrethe Vestager arguing that the proposed draft laws "are predicated on several violations of EU law."[114] This claim was addressed in several meetings[115] and phone calls[116] without any tangible results.

The same year, the Swedish Post and Telecom Agency prohibited the country's mobile network operators engaged in the 5G rollout from sourcing equipment and components from Huawei. To repeal this decision, Huawei initiated a dispute before the administrative court alleging the decision's inconsistency with Swedish administrative and EU law. The court of the first instance[117] and later, the administrative court of appeal[118] dismissed the company's legal claims. Thereafter, Huawei initiated an investment dispute before the International Centre for Settlement of Investment Disputes, which is discussed in more detail below.

### *II. Discussions at the World Trade Organization*

At least since 2018, China raised an issue of restrictions excluding Chinese companies' participation in the 5G networks at the WTO. It started with China's proposal to discuss Australia's actions restricting the use of 5G equipment produced by Huawei and ZTE – "discriminatory market access prohibition on 5G equipment" – at the Committee on Market Access in October 2018.[119] 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

[113] Ibid.**Error! Hyperlink reference not valid.**

[114] Huawei EU Public Affairs, 2020. Letter to Executive Vice President Vestager, https://www.politico.eu/wp-content/uploads/2020/10/Letter-from-Huawei-to-EVP-Vestager-Redacted.pdf, accessed on 17 January 2023.

[115] Report on meeting with Huawei, 2020. https://www.asktheeu.org/en/request/8633/response/28723/attach/4/Huwaei%20meeting%20report%20Redacted.pdf?cookie_passthrough=1, accessed on 17 January 2023.

[116] Reply to Huawei's letter of 11 September 2020. https://www.asktheeu.org/en/request/8633/response/28723/attach/2/Reply%20letter%20to%20Huawei%20Redacted.pdf?cookie_passthrough=1, accessed on 17 January 2023.

[117] Ahlander, J. and Mukherjee, S. 2021. "Swedish court upholds ban on Huawei selling 5G network gear", Reuters, https://www.reuters.com/technology/swedish-court-upholds-ban-huawei-selling-5g-network-gear-2021-06-22/, accessed on 17 January 2023.

[118] Mukherjee, S. 2022. "Swedish court upholds ban on Huawei sale of 5G gear", Reuters, https://www.reuters.com/business/media-telecom/swedish-court-upholds-ban-huawei-sale-5g-gear-2022-06-22/, accessed on 17 January 2023.

[119] 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, accessed on 17 January 2023.

(Publication and Administration of Trade Regulations), and Article XI (General Elimination of Quantitative Restrictions) of the GATT 1994.[120] The Australian measure does not explicitly name Huawei as a risk to its national security, but instead aims to protect against security risks that might arise from "the involvement of vendors who are likely to be subject to extrajudicial directions from a foreign government that conflict with Australian law."[121] 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 applied, which were origin-neutral and did not exclude Chinese suppliers.[122]

The issue was later discussed during the Council for Trade in Goods meetings in November 2018[123] and in April 2019.[124] The Australian delegate insisted that there was no import prohibition on equipment sourced from abroad or targeted at a particular country or supplier; however, it was highlighted that a new security obligation "to do their utmost to protect networks and facilities from unauthorized access and interference" was imposed on carriers, carriage service providers, and carriage service intermediaries.[125] The issue was also discussed at the Council for Trade in Services.[126]

Discussing Australia's measures against the backdrop of the national security concerns addressed by them, legal scholars are skeptical of the possibility to justify such restrictions under the WTO national security exceptions.[127] This author has also argued that restrictions on information and communications technology and services, which target Huawei and which might be inconsistent with WTO obligations, could not always be justified under the WTO national security exceptions, as it is interpreted and applied by the WTO panels.[128]

---

[120] Ibid.

[121] Weihuan, Z. and Qingjiang, K. 2019. "Why Australia's Huawei ban is unjustifiable under the WTO", CGTN, https://news.cgtn.com/news/3d3d414d78517a4d34457a6333566d54/index.html, accessed on 17 January 2023.

[122] WTO, Committee on Market Access (n 119).

[123] WTO, Council for Trade in Goods, 2019. Minutes of the Meeting of the Council for Trade in Goods 12 and 13 November 2018, https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/G/C/M133.pdf&Open=True, accessed on 17 January 2023.

[124] WTO, Council for Trade in Goods, 2019. Proposed Agenda, Doc. G/C/W/763, https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/G/C/W763.pdf&Open=True, accessed on 17 January 2023.

[125] WTO, Council for Trade in Goods (n 123).

[126] WTO, Annual Report of the Council for Trade in Services to the General Council, 2020. WTO Doc. S/C/60, https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/S/C/60.pdf&Open=True, accessed on 17 January 2023.

[127] Voon, T. and Mitchell, A. 2019. "Australia's Huawei ban raises difficult questions for the WTO", East Asia Forum, https://www.eastasiaforum.org/2019/04/22/australias-huawei-ban-raises-difficult-questions-for-the-wto/, accessed on 17 January 2023.

[128] Bogdanova, I. 2021 "Targeted Economic Sanctions and WTO Law: Examining the Adequacy of the National Security Exception", *Legal Issues of Economic Integration* 48(2): pp. 171-200, https://doi.org/10.54648/leie2021010.

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.[129] 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.[130] As of now, all these restrictive measures have escaped review under the WTO dispute settlement mechanism.

### *III. 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.[131] Huawei made several attempts to overturn this decision at the Swedish domestic courts.[132] On the last day of the year 2020, after Huawei failed in domestic courts,[133] the company submitted a written notification to Sweden and requested negotiations to reach an amicable solution.[134] Being unable to find such a solution, Huawei initiated an ICSID arbitration based on the China-Sweden BIT (1982, amended in 2004) in January 2022.[135] This dispute appears to be the first case to question the legality of a country's decision to restrict Huawei from its domestic 5G network, even though in 2019, Huawei was threatening arbitration proceedings against the Czech Republic.[136] Thus, this move has certainly rattled nerves among the states that prohibited Huawei's participation in their 5G projects.

---

[129] 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, accessed on 17 January 2023.

[130] 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, accessed on 17 January 2023.

[131] 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, accessed on 17 January 2023.

[132] Ahlander, J. and Mukherjee, S. (n 117).

[133] Ibid.

[134] Huawei Technologies Co., Ltd. v. The Kingdom of Sweden, Notice on Intent, 2020. https://jusmundi.com/en/document/other/en-huawei-technologies-co-ltd-v-kingdom-of-sweden-notice-of-intent-tuesday-5th-january-2021, accessed on 17 January 2023.

[135] Huawei Technologies Co., Ltd. v. Kingdom of Sweden (ICSID Case No. ARB/22/2), https://icsid.worldbank.org/cases/case-database/case-detail?CaseNo=ARB/22/2, accessed on 17 January 2023.

[136] Hepburn, J. and Peterson, L.E. 2019. "Analysis: As Huawei Invokes Investment Treaty Protections in Relation to 5G Network Security Controversy, What Scope is There for Claims Under Chinese Treaties With Czech Republic, Canada, Australia and New Zealand?", IAReporter, https://www.iareporter.com/articles/analysis-as-huawei-invokes-investment-treaty-protections-in-relation-to-5g-network-security-controversy-what-scope-is-there-for-claims-under-chinese-treaties-with-czech-republic-canada-australia-a/, accessed on 17 January 2023.

According to Huawei's submission, Sweden violated the following obligations under the China-Sweden BIT: (i) fair and equitable treatment under Article 2(1); (ii) national treatment standard, which is incorporated through the operation of the MFN clause contained in Article 2(2); (iii) prohibition of expropriation and nationalization under Article 3, and hence, Huawei is entitled to full reparation.[137] Neither the China-Sweden BIT[138] nor the amendment protocol[139] contain public order or national security exceptions. Even so, Sweden can invoke customary international law defense of necessity embodied in Article 25 of the Draft Articles on Responsibility of States for Internationally Wrongful Acts, the move which allowed some respondents to successfully defend their government policies before.[140] To justify its conduct under the plea of necessity, several prerequisites should be fulfilled: challenged measure safeguards an "essential interest" of the state; this measure should be the only way of safeguarding that interest; the measure addresses a "grave and imminent peril"; no other essential interest of the state, another state, or the international community should be seriously impaired as a result.[141] In the past, states have invoked the plea of necessity "[…] in the context of the Argentine financial crisis in 2001, […] in the context of war, revolutions, national security crises and public order and security."[142] In light of this, it remains to be seen if the 5G rollout and the risks associated with it can qualify for this purpose.

**Concluding remarks**

The idea of restricting access to the supplier, e.g. Huawei, who offers the lowest price on the market is antithetical to the free-market principles underpinning the global economic order. The invocation of national security to justify such moves only complicates the matter and confirms our assumption that the 5G rollout is politicized and securitized. As the national security rhetoric is increasingly infiltrating global economic affairs, being already heralded as a "shift to a new geo-economic world order",[143] it remains to be seen if the dispute settlement mechanisms created by the international

[137] Huawei Technologies Co., Ltd. v. The Kingdom of Sweden (n 131).
[138] Agreement on the mutual protection of investments between the Government of the Kingdom of Sweden and the Government of the People's Republic of China, 1982, https://investmentpolicy.unctad.org/international-investment-agreements/treaty-files/6044/download accessed on 17 January 2023.
[139] Protocol, Amendment to the Agreement on Mutual Protection of Investments Between the Government of the Kingdom of Sweden and the Government of the People's Republic of China of March 29, 1982, 2004, https://investmentpolicy.unctad.org/international-investment-agreements/treaty-files/6042/download, accessed on 17 January 2023.
[140] Leonardo, C. 2023. "Necessity as a Defence", Jus Mundi, https://jusmundi.com/en/document/publication/en-necessity-as-a-defence, accessed on 17 January 2023.
[141] International Law Commission, 2001. Draft Articles on Responsibility of States for Internationally Wrongful Acts, https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf, accessed on 17 January 2023.
[142] Paddeu, F. and Waibel, M. 2022. "Necessity 20 Years On: The Limits of Article 25," *ICSID Review – Foreign Investment Law Journal* 37(1-2): pp. 160–191, https://doi.org/10.1093/icsidreview/siab047.
[143] Roberts, A., Moraes, H.C. and Ferguson, V. 2019. "Toward a Geoeconomic Order in International Trade and Investment," *Journal of International Economic Law* 22(4): pp. 655–676, https://doi.org/10.1093/jiel/jgz036.

economic order could restrain states from imposing their will on their domestic constituencies as well as their trading partners.