Jonas Fechter | Janosch Wiesenthal (Eds.)

The Age of Open Strategic Autonomy

Nomos

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available on the Internet at http://dnb.d-nb.de

ISBN 978-3-7560-0843-8 (Print)
978-3-7489-1591-1 (ePDF)

Online Version
Nomos eLibrary

1st Edition 2025

Preface

From May 11 to 13, 2023, approximately 40 lawyers convened in Berlin to discuss the latest developments in the law of investment screening and related legal instruments, which are increasingly summarized under the umbrella of *Open Strategic Autonomy*. Given the complex geopolitical and geoeconomic circumstances that shape the current trade and investment environment, the conference *The Age of Open Strategic Autonomy* dealt with the legal strategies that the European Union employs to keep up with its strategic partners and rivals. The majority of the attendees were early career scholars and practitioners who offered a fresh perspective on this dynamic area of the law. The conference was organized under the auspices of the *CELIS Institute*, an independent non-profit, non-partisan research enterprise dedicated to promoting better regulation of foreign investments in the context of security, public order, and competitiveness. It was generously sponsored by leading law firms *Blomstein* and *Freshfields*.

Jonas Fechter and Janosch Wiesenthal

Table of Contents

Politicization and Securitization of the 5G Rollout: What Role for International Economic Law?

Iryna Bogdanova

China's ambition to become a global leader in emerging and foundational technologies, which is partly channelled through state-led industrial efforts such as "Made in China 2025", prompted a strong response from other states. These developments coincided in time with the rollout of the 5G infrastructure, surrounded by the controversy over the involvement of Chinese technology companies in the process. In this global context, politicization and securitization of the 5G rollout seem almost unavoidable. This outcome emanates not only from the vivid geopolitical tensions but also from the nature and economic implications of 5G that give rise to various types of national security risks.

This being set as a context, the chapter explores the role of international economic law in preventing geopolitically induced restrictions and in providing companies with a right to question their legality and to seek redress. The chapter proceeds in three parts. To set the stage for a subsequent discussion, the first part describes the 5G standard, its implications for the economy and relevant national security risks. Following this, the focus shifts to a discussion of the recent policies pursued by various states and aimed at restricting Huawei and other Chinese-based technology companies from participating in the 5G rollout. In the third part, these recent restrictions are analysed against the background of the respective obligations under international investment and WTO agreements. Finally, the possibility to justify such policies on national security grounds is examined. The conclusion recapitulates whether international economic law effectively constrains states from pursuing their policies, when the subject matter becomes securitized or politicized.

A. 5G: economic implications of its rollout and relevant national security risks

5G – the fifth generation of cellular networks – is not only the next generation of mobile cellular system but also "a big paradigm shift".[1] The 5G rollout 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).[2] These characteristics allow us to talk about three distinctive cases of application: enhanced mobile broadband (enabling larger data volumes and enhancing user experience), massive machine-type communication (enabling the "Internet of Things"), and ultra-reliable and low-latency communication (enabling autonomous vehicles and robotic-enabled remote surgery).[3]

The economic implications of the 5G rollout are far-reaching: 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".[4] Analysts have argued that the 5G rollout "holds the key to shaping the future of practically every industry by drastically transforming the way machines interact and function".[5] Corroborating this view, the 5G Automotive Association (5GAA) stated in its recent white paper that "5G will be a game-changer for architecting future automotive industry services."[6]

5G infrastructure will be of a considerable importance that surpasses the role played by any digital infrastructure of the past.[7] As a result, 5G and the infrastructure required for it to function are labelled by states as a "critical technology" and "critical infrastructure" respectively.[8] In this regard, recent G7 Leaders' Statement emphasized the need to build "resilient critical infrastructure" and for this purpose "to assess political, economic, and other risks of a non-technical nature posed by vendors and suppliers."[9]

---

1 Liyanage/Ahmad/Abro/Gurtov/Ylianttila/Nguyen/Brunstrom/Grinnemo/Taheri, p. 31 (31).
2 Duffy.
3 Dahlman/Parkvall/Sköld, p. 1 (1–6); Liyanage/Ahmad/Abro/Gurtov/Ylianttila/Nguyen/Brunstrom/Grinnemo/Taheri, p. 31 (32 et seq.).
4 Robles-Carrillo Telecommunications Policy 2021, 1 (3).
5 Poliakine.
6 5GAA Automotive Association, p. 13.
7 Friis/Lysne Development and Change 2021, 1174 (1181).
8 Some even argue that "5G networks will be the most critical infrastructures we have ever seen." Ibid.
9 G7 Leaders' Statement on Economic Resilience and Economic Security, 2023.

Considering that the building of 5G network requires "massive capital investment",[10] and that cost efficiency plays a significant role for the mobile operators,[11] the alleged government subsidization of Chinese tech companies, mostly Huawei,[12] which brings the prices for its 5G equipment significantly down,[13] should be viewed as a positive development. Yet, the opposite is the case: states increasingly prohibit Chinese tech companies (Huawei and ZTE) from participating in their 5G infrastructure projects. What are the risks that compel states to introduce these restrictions? The answer to this question lies in the nature of the 5G network and in the nature of Chinese tech companies. Furthermore, existing and potential risks are further exacerbated by the growing great-power rivalry over technological superiority.[14]

Security of 5G is multifaceted: experts have already acknowledged that it would be necessary to guarantee security at access, infrastructure, and service level.[15] Aside from the complex technical solutions,[16] security at each of these levels entails: (i) governments' responsibility to guarantee access to the future 5G infrastructure, (ii) security of infrastructure from various risks, including cyber-attacks, and (iii) security of the commercial and private data exchanged over the network. These risks, which require different mitigation strategies, play a significant role in the governments'

10 Poliakine.

11 "[...] the cost efficiency, which represents the economical aspect of the 5G system, must be increased in order to guarantee mobile operator's revenue." Liyanage/Ahmad/Abro/Gurtov/Ylianttila/Nguyen/Brunstrom/Grinnemo/Taheri, p. 31 (36).

12 "[...] 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 Global Asia 2019, 15.

13 "Huawei's prices are typically at least 30 percent lower than those of its competitors, benefitting from generous Chinese government direct and indirect subsidies." Rubin/Martinez/Dow/Puglisi, p. 30; Nakashima.

14 As the technological gap between China and other states has significantly decreased and against the background of China's ambitions to become a global leader in innovative technologies, the United States is actively engaged in the policies that disrupt international trade and investment flows in advanced technologies between it and China. Anthea Roberts and others argue that the US actions can be grouped into three categories: shielding (protection of domestic technological knowledge), stifling (actions to inhibit the strategic competitor's capacity) and spurring (stimulation of technological innovation). Roberts/Moraes/Ferguson JIEL 2019, 655.

15 Liyanage/Ahmad/Abro/Gurtov/Ylianttila/Nguyen/Brunstrom/Grinnemo/Taheri, p. 31 (36 et seq.).

16 Ibid.

calculations on whether to allow Chinese entities to participate in the 5G rollout or not.[17]

To guarantee access to the future 5G infrastructure, states should be convinced that the equipment suppliers would not sabotage its functioning. This risk has been described in the EU coordinated risk assessment of the cybersecurity of 5G networks as follows: "*Lack of access controls*: a subcontractor with administrator's privileges on the network performs adverse action, leading to confidentiality/integrity and/or availability breach. The subcontractor's action may be due to a legal requirement imposed by a third country or rogue behaviour of the contractor's staff."[18]

In the current global context, the possibility to exercise control over the functioning of the foreign state's 5G infrastructure can be potentially utilized as a means of coercion, giving rise to a phenomenon known in international relations literature as a "weaponized interdependence".[19] In this regard, the testimony of James Andrew Lewis before the United States Senate Committee on the Judiciary succinctly summarizes the essence of the concerns regarding the use of Chinese-supplied 5G equipment: "The issue is not whether one trusts the Chinese company, but whether one trust the Chinese government."[20]

Talking about the cybersecurity risks to the 5G infrastructure, Roxana Radu and Cedric Amon conclude that along with the availability of the 5G networks, other most pressing 5G threats are the compromise of confidentiality (spying on traffic and data circulated) and integrity (modifications or alterations of traffic and information systems).[21] The ability of 5G to connect billions of new devices augments these risks: successful espionage efforts can potentially expose vast amounts of data, including commercially

17 For example, EU coordinated risk assessment of the cybersecurity of 5G networks released in 2019 enumerates all these types of risks. EU coordinated risk assessment of the cybersecurity of 5G networks, 2019.

18 Ibid, p. 25.

19 Henry Farrell and Abraham L. Newman argued that global networks generate "enduring power imbalances among states", and these asymmetric network structures "create the potential for 'weaponized interdependence', in which some states are able to leverage interdependent relations to coerce others." Farrell/Newman International Security 2019, 42. This possibility is not merely hypothetical: since recently, China has been emulating Western instruments of economic statecraft, including instruments of economic coercion, and showed its willingness to use them. Gao/Raess/Zeng/Bogdanova/Wang, p.160.

20 Lewis, p. 4.

21 Radu/Amon Journal of Cybersecurity 2021, 1.

sensitive and private data, to foreign governments and industry competitors. This is not hard to imagine considering the reported instances of cyber espionage, ransomware attacks and cyber-attacks targeting critical infrastructure, some of which were allegedly state-sponsored,[22] and the lack of binding international norms regulating the behaviour of state and non-state actors in the cyberspace[23]. For example, a devastating SolarWinds cyberattack – dubbed as "a huge cyber espionage campaign"[24] – compromised "about 100 companies and about a dozen government agencies", including the Department of Justice, the Department of Treasury, and the Cybersecurity and Infrastructure Security Agency entrusted with the function of protecting federal computer networks from cyberattacks.[25]

The risks of compromise of confidentiality and integrity are further exacerbated by the nature of 5G. 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."[26] 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."[27] Seen from the technical perspective, safety assessment of the 5G equipment aimed at detecting undesired features or their future emplacement is worthless, especially when malicious functionality can be easily installed at a later stage through a software update.[28] Given this, trust plays a decisive role in choosing 5G equipment supplier.[29]

A growing number of states are wary of allowing Chinese companies to participate in their 5G networks. There are a number of reasons for this. First, the relationship between the Chinese Communist Party and Chinese-based companies, which has been vividly described by Andrew Grotto with the following words: "the Chinese government considers Chinese compan-

22 Bogdanova/Vásquez Callo-Müller EJIL:Talk! Blog of the European Journal of International Law 2021.
23 Bogdanova/Vásquez Callo-Müller Vanderbilt Journal of Transnational Law 2021, 911.
24 Bing.
25 Temple-Raston.
26 Wheeler.
27 Grotto Global Asia 2019, 14.
28 Lysne/Elmokashfi/Nagelhus Schia/Gjesvik/Friis, p. 9; Friis/Lysne Development and Change 2021, 1174 (1183).
29 Ibid.

ies to be extensions of the state, whether a company likes it or not",[30] magnifies the existing 5G security concerns. 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),[31] which requires Chinese citizens and companies to cooperate with the Chinese intelligence agencies[32] and assist them in their intelligence work[33].

Talking about Huawei's designation as a "high-risk vendor", the reasons behind this can be succinctly summarized as follows: unclear ownership structure, potential affiliation with the Chinese military and long-standing espionage allegations.[34] Thus, concerns regarding Chinese companies' participation in the 5G projects can sprout from different roots.

Considering the risks associated with the 5G rollout and the nature of Chinese tech companies, both factors which could not be easily mitigated, and against the background of the geo-political tension between the United States and China, the participation of Chinese vendors in 5G infrastructure became securitized[35] or politicized[36].

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

Against the background of these diverse risks emanating from the 5G rollout, consisting of a mixture of 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

30 Grotto Global Asia 2019, 13.

31 National Intelligence Law of the People's Republic of China.

32 Wheeler.

33 Nakashima.

34 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, Journal of Chinese Political Science 2022, 151.

35 "[...] 5G and Chinese suppliers were securitized. The topic was elevated from the realm of ordinary politics and treated as an emergency, thus legitimizing extraordinary countermeasures." Friis/Lysne Development and Change 2021, 1174 (1175).

36 "[...] every major issue associated with 5G networks has become politicized." Eurasia Group, 2018.

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 Chinese-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 the 5G standard essential patents.[37]

I. Explicit bans on Chinese suppliers' participation in 5G

Since 2018, a growing number of states have either explicitly banned Huawei or taken other regulatory steps to exclude Huawei from their 5G networks.[38] For example, the Five Eyes intelligence sharing network – composed of Australia, Canada, New Zealand, the United Kingdom, and the United States – has an uncompromising stance on the issue of Huawei and its participation in their 5G networks. 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,[39] and in 2018, by labelling Huawei and its equipment as an unacceptable security risk, Australia formally banned it from its 5G network[40]. A few months later, New Zealand followed suit.[41] Other states have not remained idle 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 as early as 2012.[42] These concerns were expressed in a report on Huawei and ZTE Corporation released by the US House of Representatives Permanent Select Committee on Intelligence.[43] It should be noted that back then these

37 Ibid.
38 Sacks.
39 Peng JIEL 2015, 449.
40 BBC News, Huawei and ZTE.
41 CNBC.
42 Gallagher.
43 US Congress, House Permanent Select Committee on Intelligence, Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE, 2012.

concerns fell on deaf ears, and the lack of any response only reinforced the decline of the US telecommunications equipment industry.[44]

However, 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.[45] Furthermore, federal agencies were prohibited from entering into a contract with an entity that uses equipment, systems, or services provided by Huawei and several other Chinese companies.[46] 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.[47]

In March 2020, the Secure 5G and Beyond Act of 2020 was signed into law.[48] The Act requires the President, in consultation with the relevant federal agencies, to develop a strategy to secure and protect 5G as well as future generations of wireless communications systems in the United States and support US allies when it is needed.[49] That same month, the White House released the National Strategy to Secure 5G, which sets as its core priorities management of the supply chain risks and addressing of the risk of 'high-risk' vendors in 5G infrastructure.[50] The accompanying implementation plan was announced in 2021.[51]

In parallel to these developments, in the course of the last years, the United States engaged in multifaceted efforts to exclude Huawei from its telecommunications networks, for example by prohibiting certain transac-

44 Six key factors caused the collapse of the US telecommunications equipment industry: decline in private-sector R&D spending, restricted private-sector funding and development timelines, lack of federal government prioritization, avoidance of geopolitical competition in strategic technologies, federal government aversion to industrial policy and division of responsibility between economic and security-focused organizations. Rubin/Omar Loera Martinez/Dow/Puglisi, p. 27.

45 Gallagher, p. 12.

46 Ibid.

47 "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.

48 Secure 5G and Beyond Act of 2020, Public Law 116–129, 134 Stat. 223–227.

49 Ibid.

50 The National Strategy to Secure 5G of the United States of America, March 2020.

51 National Strategy to Secure 5G Implementation Plan, January 6, 2021.

tions involving foreign-owned information and communications technology and services,[52] and to hinder Huawei's technological capacity by tightening export restrictions.[53] The vast majority of these US policies declare that they pursue two objectives: to increase the security of the US networks and secure supply chains for information and communications technology and services.[54] For the United States, it is not only about the protection of communications networks but also about maintaining technological edge in an ongoing race with China for technological superiority.[55] In other words, the United States might significantly benefit from the first-mover advantage if it deploys 5G network rapidly.[56]

The United Kingdom allowed Huawei to provide equipment for the "non-core" parts of the country's 5G network before 2020.[57] In other words,

52 On May 15, 2019, President Trump issued Executive Order 13873 that prohibits various transactions involving foreign-owned information and communications technology and services (ICTS) if Commerce, in consultation with other executive branch agencies, determines that (i) such transactions involve ICTS designed, developed, manufactured, or supplied by persons or entities owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary; and if (ii) such transactions present an undue risk of sabotage or subversion to ICTS in the United States; an undue risk of catastrophic effects on the security or resiliency of critical infrastructure or the digital economy in the United States; or unacceptable risk to US national security or the security and safety of US persons. Exec. Order No. 13873 of May 15, 2019, Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 22689.
Pursuant to the Executive Order 13873 the Department of Commerce issued relevant regulation in January 2021, which creates a new process to review transactions involving information and communications technology and services on a case-by-case basis. The new rule – known as Supply Chain Rule – allows Commerce to either block a transaction, if it involves "foreign adversaries" and presents certain "undue or unacceptable risks", or negotiate risk-mitigation measures. Department of Commerce. Securing the Information and Communications Technology and Services Supply Chain, 86 Fed. Reg. 4909 (03/22/2021) (codified at 15 C.F.R. 7).

53 Mulligan/Linebaugh.

54 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". In May 2022, President Biden continued the national emergency declared in Executive Order 13873 for one year. Biden, J.R., Notice on the Continuation of the National Emergency with Respect to Securing the Information and Communications Technology and Services Supply Chain, 2022.

55 Harrell, p. 1; Lewis, p. 8.

56 Ibid.

57 Brooks.

the regulators followed the standard according to which the network is divided between "core" and "non-core" parts, although the usefulness of this division in the context of 5G is questioned by experts.[58] However, in 2020, the tide turned: the United Kingdom decided to terminate its cooperation with Huawei and as a result, 5G infrastructure already installed has to be removed by 2027.[59] 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.[60]

Canada joined similarly-minded political allies in May 2022 by banning Huawei and ZTE from its 5G networks,[61] a move that has been already described as a "long-awaited decision"[62]. 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".[63] For this reason, the existing 5G equipment and services provided by these companies should be removed or discontinued by 28 June 2024.[64]

Japan banned government purchases of telecommunications products from Huawei and ZTE Corp.[65] According to media reports, this led to the decision of the country's main mobile carriers not to use Huawei equipment in the 5G rollout.[66]

58 "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 36).

59 Gold.

60 Radu/Amon Journal of Cybersecurity 2021, 1 (12).

61 Innovation, Science and Economic Development Canada.

62 Carvin.

63 Innovation, Science and Economic Development Canada.

64 Ibid.

65 Reuters.

66 Kharpal.

II. Risk-based policies, including implicit bans on Chinese suppliers' participation in 5G

When the European Commission drafted the 5G Action plan in 2016, the idea of excluding certain suppliers from the 5G rollout had not gained traction yet.[67] This comes as no surprise: a 2020 study of the equipment used by European mobile operators revealed that first, "[i]n 15 of 31 countries, more than 50 % of the 4G RAN [radio access network] equipment comes from Chinese vendors" and second, "48 % of the 4G RAN equipment in the 31 countries comes from Chinese vendors".[68] These results confirm that Chinese equipment was widely used in the previous generation of mobile networks, and it was probably expected that the 5G rollout would not be any different.

The subsequent shift in the EU's position on this matter has been defined by its aspiration to "de-risk" from the potential threats to the critical infrastructure against the backdrop of geopolitical tensions with China.[69] The reasons for this is the acknowledgement that security of 5G networks is of essential importance for "the strategic autonomy of the Union".[70] Furthermore, the EU's cooperation with the United States under the EU-US Trade and Technology Council which reflects the new policy of "Open Strategic Autonomy" has contributed to this shift.[71] Recently, the unprovoked Russian war against Ukraine and the problematic energy dependence made any form of dependency that involves a potential political rival unbearable even as a thought.[72] In light of this, the risks associated with the 5G rollout and its future functioning are further exacerbated by the global geo-political tensions.

---

67 European Commission, 5G for Europe: An Action Plan, COM(2016) 588 final.

68 Strand Consult, Understanding the Market for 4G RAN in Europe.

69 The European economic security strategy released in June 2023 emphasizes the need "[t]o increase the security and resilience of 5G networks" and reminds that "the 5G Toolbox establishes a set of measures to be applied by all Member States, including measures to restrict or exclude high-risk suppliers." Furthermore, this security strategy urges "Member States that have not yet fully applied these measures to high-risk suppliers to do so without delay." Joint Communication to the European Parliament, the European Council and the Council on "European Economic Security Strategy", JOIN(2023) 20 final.

70 Robles-Carrillo Telecommunications Policy 2021, 1 (5 et seq.).

71 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.

72 For a similar view, please see Cerulus/Wheaton.

At the Union level, the following steps were undertaken: in March 2019, the European Commission issued Recommendation 2019/534 and obligated Member States to carry out a risk assessment of the 5G network infrastructure,[73] based on the Member States' input a coordinated European risk assessment was conducted and the relevant report was released in October 2019,[74] which was followed by the release of 'Cybersecurity of 5G networks: EU toolbox of risk mitigating measures' (EU toolbox of risk mitigating measures)[75].

Among various types of security threats, the EU coordinated risk assessment of the cybersecurity of 5G networks highlights supplier-specific vulnerabilities.[76] 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."[77] 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."[78] In order to overcome the risks associated with high-risk vendors, the EU toolbox of risk mitigating measures proposes to assess the risk profile of suppliers and apply restrictions for suppliers considered to be high-risk.[79] Besides, it is recommended that the EU Member States exchange best practices on their national frameworks for assessing suppliers' risk profiles.[80] In this way the concept of a "high-risk vendor" has been engrained, thus allowing EU Member States to exclude the companies that possess national security risks from their respective markets. The European Economic Security Strategy released in June 2023 emphasizes the need to increase the security and resilience of 5G networks and urges Member States to use the 5G Toolbox and fully implement measures against high-risk suppliers without delay.[81]

It should be noted that the implementation of the EU-wide rules on the 5G rollout is constrained by the indistinct delimitation of competences

73 European Commission, Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks, OJ L 88, p. 42–47.
74 EU coordinated risk assessment of the cybersecurity of 5G networks, 2019, p. 1–33.
75 Cybersecurity of 5G networks: EU toolbox of risk mitigating measures, 2020.
76 EU coordinated risk assessment of the cybersecurity of 5G networks, 2019, p. 22–23.
77 Ibid.
78 Ibid.
79 Cybersecurity of 5G networks: EU toolbox of risk mitigating measures, 2020, p. 12.
80 Ibid.
81 European Economic Security Strategy JOIN(2023) 20 final.

between the EU and its Member States when it comes to the 5G technology.[82] This has resulted in different approaches to the Chinese companies' participation in the national 5G projects among the EU Member States. For example, 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.[83]

Other EU Member States such as Germany and Italy are more hesitant to exclude Chinese suppliers from their domestic 5G networks.[84] Strand Consult recently reported that "some of Europe's largest operators have purchased and deployed Chinese 5G equipment in their networks after 2020."[85] This division in the EU Member States' approaches has been underlined in the first EU toolbox implementation report: only part of the Member States – fourteen states – confirmed that their national risk evaluation frameworks include assessment of the non-technical factors such as the origin of suppliers or the risk of interference into 5G networks from third countries.[86] The most recent implementation report issued in June 2023 re-affirmed that some states not only failed to introduce restrictions against high-risk vendors but also failed to adopt required legislative frameworks enabling them to do this.[87]

82 "Security in 5G networks is not defined as an EU competence in the Treaties. Nor is it a competence held entirely and exclusively by its Member States. Actually, 5G security materially and transversally concerns different areas in which the EU has competence and areas that fall within the competence of the States. But, in particular, it affects the main core of the EU's action, which is the internal market, in three main areas: 1) The legal regime for electronic communications; 2) The provisions on the security of networks and information systems; and 3) The latest regulations on cybersecurity. According to the Council and the European Commission, this corpus of rules is currently the main basis for EU action on 5G." Robles-Carrillo Telecommunications Policy 2021, 1 (6).

83 Cerulus.

84 Larsen.

85 Strand Consult, The Market for 5G RAN in Europe.

86 NIS Cooperation Group, Report on Member States' Progress, p. 17.

87 NIS Cooperation Group, Second report on Member States' Progress, p. 6 et seqq.

III. No restrictions on the use of Chinese suppliers in 5G rollout

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."[88] 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.[89]

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,[90] which functions as the executive body of the federal government and the collective head of state. In its response, the Federal Council expounded on four aspects: (i) the US government did not present any evidence regarding alleged espionage allegations; (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.[91] At present, Switzerland did not introduce any restrictions or prohibitions targeting Chinese

88 Hemmings, p. 1.
89 Lee/Rasser/Fitt/Goldberg.
90 Regazzi, F., Interpellation: Huawei und die Herausforderungen von 5G. Risiken und Chancen für die Schweiz, 2019.
91 Ibid.

tech companies and allows its telecommunications service providers to make their procurement choices without any limitations, i.e., the country defers to private industry on the use of Chinese equipment. Although recently the Federal Council announced its plans to enhance the security of telecommunications systems and digital infrastructures.[92]

Brazil partners with Huawei to build its 5G infrastructure[93] with other countries in the region also being interested in the cheap 5G equipment provided by Chinese vendors.[94]

As numerous states shore up legislation and administrative actions geared towards 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.[95] 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."[96]

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.[97]

C. Restrictions on Chinese companies' participation in the 5G rollout and international economic law

Chinese tech companies, mainly Huawei, raised to a prominence as one of the major global suppliers of the 5G equipment, in part, thanks to Chinese government support.[98] This government support took different forms: economic support (e.g., government subsidies, export financing, low interest

92 SWI swissinfo.ch.
93 Pham.
94 Myers/Montenegro.
95 Eurasia Group, 2020.
96 Lee/Rasser/Fitt/Goldberg, p. 1.
97 Bogdanova, WTI working paper no. 01/2023, 1.
98 Rubin/Omar Loera Martinez/Dow/Puglisi, p. 30.

loans etc.), regulatory measures (e.g., guaranteed access to the Chinese market), and political support (e.g., active participation in standard setting bodies).[99] The existing international economic order did not function as a constraint for the aforesaid policy actions, although some states voiced their concerns regarding these policies.

In this part, the analysis will focus on proving the thesis that the existence of substantive legal norms and institutional dispute settlement is incapable of constraining individual states or groups of states from implementing policies that undermine international economic order if the interests at stake are securitized/politicized as it is the case with the 5G rollout.

I. WTO law

1. WTO as a rule maker

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.[100] During this meeting, China's representative argued that Australia introduced origin-based prohibitions on Chinese telecom products in violation of its commitments under Art. I:1 (Most Favoured Nation, MFN), Art. X (Publication and Administration of Trade Regulations), and Art. XI (General Elimination of Quantitative Restrictions) of the GATT 1994.[101] 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.[102]

99 Ibid.
100 WTO, Committee on Market Access, Minutes of the Committee on Market Access 9 October 2018.
101 Ibid.
102 Ibid.

The issue was later discussed during the Council for Trade in Goods meetings in November 2018[103] and in April 2019.[104] The Australian delegate insisted that there was no import prohibition on equipment originating from abroad and that the measure was not 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.[105] The issue was also discussed at the Council for Trade in Services.[106]

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.[107] Recently, in April 2022, Belgium's draft law introducing additional security measures for the provision of mobile 5G services was labelled by China as a special trade concern and included in the Council for Trade in Goods agenda.[108] As of now, all these restrictive measures have escaped review under the WTO dispute settlement mechanism.

These discussions at the various WTO Committees demonstrate that in theory ambiguously-formulated rules enshrined in the various WTO Agreements might be breached by the countries that restrict market access to Chinese tech companies, Huawei and ZTE.

2. WTO as a litigation forum and national security exceptions

Chinese tech companies can lobby its government to initiate a dispute before the WTO. Any such dispute would unavoidably bring about the discussion of national security exceptions embedded in several WTO Agreements. Art. XXI of the GATT 1994 and similar exceptions in the GATS and the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) contemplate a number of security exceptions. The national security exception that allows WTO Members to take unilateral trade-restrictive

103 WTO, Council for Trade in Goods, Minutes of the Meeting of the Council for Trade in Goods 12 and 13 November 2018.
104 WTO, Council for Trade in Goods, Proposed Agenda, Doc. G/C/W/763, 2019.
105 Ibid.
106 WTO, Annual Report of the Council for Trade in Services to the General Council, WTO Doc. S/C/60, 2020.
107 WTO, Report of the Council for Trade in Goods, WTO Doc. G/L/1418, 2021.
108 WTO, Report of the Council for Trade in Goods, WTO Doc. G/L/1463, 2022.

measures is embedded in Art. XXI(b)(iii) of the GATT 1994 (GATS and TRIPS have similar provisions) and it reads as follows:

> Nothing in this Agreement shall be construed:
>
> [...] (b) to prevent any Member from taking any action which it considers necessary for the protection of its essential security interests
> [...] (iii) taken in time of war or other emergency in international relations.

In *Russia – Traffic in Transit*, the WTO panel interpreted this clause for the first time and for this purpose introduced a framework to analyse the invocation of the national security justification. The panel distinguished between objective and subjective elements of the national security clause: the prerequisite "taken in time of war or other emergency in international relations" was interpreted as an objective element[109] that operates as a "limitative qualifying clause"[110]. This objective element not only requires an objectively established existence of war or other emergency in international relations but also the coincidence in time of trade-restrictive measures and such events.[111] According to the panel report, the WTO Member's determination of the subjective elements of the national security exception – a determination of "essential security interests" and the necessity of such measures ("necessary for the protection") – should be reviewed against the background of the principle of good faith.[112] For this reason, a WTO Member should articulate its essential security interests "sufficiently enough to demonstrate their veracity".[113] Furthermore, the element "necessary for the protection" requires a minimum degree of plausibility between trade-restrictive measures and their ability to contribute to the protection of declared security interests.[114]

In October 2018, Qatar requested consultations with Saudi Arabia concerning measures that in its view violated the TRIPS Agreement,[115] and

109 WTO, Panel Report Russia — Measures Concerning Traffic in Transit, WT/DS512/R, para. 7.101 (Panel Report Russia – Traffic in Transit).
110 Ibid, para. 7.65.
111 Ibid, para. 7.70.
112 Ibid, para. 7.132. and para. 7.138.
113 Ibid, para. 7.134.
114 Ibid, para. 7.138.
115 WTO, Saudi Arabia – Measures Concerning the Protection of Intellectual Property Rights, Request for Consultations by Qatar, WTO Doc. WT/DS567/1 IP/D/40, 4 October 2018.

which were a part of the broader efforts to isolate Qatar instituted by its neighbouring countries in June 2017.[116] In the dispute that followed, the panel, in order to assess whether respondent has properly invoked national security clause of Art. 73(b)(iii) of the TRIPS Agreement, abide by the analytical framework developed by the panel in *Russia – Traffic in Transit*.[117]

In the most recent WTO disputes, panels reached similar conclusions. For example, the panel in *US – Origin Marking (Hong Kong, China)* concluded:

> The grammatical structure of Article XXI(b) as discerned from the text, thus, suggests that what is in the subparagraphs is not subject to the invoking Member's own determination but is instead subject to objective determination by a panel. The role of the subparagraphs, thus, would be to circumscribe (and limit) the circumstances in which the invoking Member may take action which it considers necessary for the protection of its essential security interests.[118]

In other words, the panel in *US – Origin Marking* confirmed that the subparagraph "taken in time of war or other emergency in international relations" is subject to an objective determination by the WTO adjudicators.

In *Russia – Traffic in Transit*, the panel equated the term "war" with an armed conflict,[119] while defining "emergency in international relations" as "a situation of armed conflict, or of latent armed conflict, or of heightened tension or crisis, or of general instability engulfing or surrounding a state."[120] In a more recent report in *US – Steel and Aluminium Products (Switzerland)*, the panel observed that:

> [...] the reference to "war" informs the meaning of "emergency in international relations" as part of the circumstances "in time of" which a Member may act under Article XXI(b) for the protection of its essential security interests. In particular, the Panel considers that an "emergency in international relations" within the meaning of Article XXI(b)(iii) must

116 BBC News, Qatar Crisis.

117 WTO, Panel Report Saudi Arabia – Measures Concerning the Protection of Intellectual Property Rights, WT/DS567/R and Add.1, (dispute terminated while appeal pending), para. 7.241.

118 WTO, Panel Report US – Origin Marking Requirement (Hong Kong, China), WT/DS597/R, circulated to WTO Members on 21 December 2022, appealed on 26 January 2023, para. 7.89, (Panel Report US – Origin Marking).

119 Panel Report Russia – Traffic in Transit (n 109), para. 7.72.

120 Ibid, para. 7.76.

be, if not equally grave or severe, at least comparable in its gravity or severity to a "war" in terms of its impact on international relations.[121]

The panel in *US – Origin Marking* further clarified that "the emergency [emergency in international relations] does not necessarily have to originate in the invoking Member's own territory and bilateral relations but could happen more broadly in relations among a wider group of WTO Members."[122] Additionally, the panel elucidated that "the further removed that a situation is from war or comparable threat to international peace and security, the more explanation a respondent would usually need to provide as to why a given situation is close to the breakdown in relations between two or more countries, or Members, in the sense of Art. XXI(b)(iii)."[123]

Analysis of this case law demonstrates that the possibility to justify restrictions against Chinese companies' participation in the 5G rollout under the WTO national security exceptions is significantly constrained by the objective prerequisite "taken in time of war or other emergency in international relations". In particular, a WTO Member that is willing to invoke the national security exception to justify its actions should be able to establish several elements: it should be demonstrated that (i) a "war" or "other emergency in international relations" existed; (ii) this particular emergency gave rise to security interests, – "i.e., defence or military interests, or maintenance of law and public order interests", for a WTO Member relying upon a national security exception; and (iii) the restrictive measures were "taken in time" of such emergency.

Despite the enormous potential of the technology companies such as Huawei and ZTE to engage in acts of cyber espionage, cyber theft and unauthorized interference in the users' privacy and even possibility to completely undermine functioning of the 5G infrastructure, restrictive measures imposed against such companies might potentially fall short of being justified under the WTO national security exception as it is formulated and applied by the WTO adjudicators.

121 WTO, Panel Report, United States – Certain Measures on Steel and Aluminium Products, WT/DS556/R, circulated to WTO Members on 9 December 2022, appealed on 26 January 2023, para. 7.157.

122 Panel Report US – Origin Marking (n 118), para. 7.307.

123 Ibid, para. 7.312.

II. International investment agreements (IIAs)[124]

1. IIAs as standard setters

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.[125] Huawei made several attempts to overturn this decision at the Swedish domestic courts.[126] On the last day of the year 2020, after Huawei failed in domestic courts,[127] the company submitted a written notification to Sweden and requested negotiations to reach an amicable solution.[128] 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.[129] 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.[130]

Turning to the substance of the legal claims before the investor-state tribunal, according to Huawei, Sweden violated the following obligations under the China-Sweden BIT: (i) fair and equitable treatment (FET) under Art. 2(1); (ii) national treatment standard, which is incorporated through the operation of the MFN clause contained in Art. 2(2); (iii) prohibition of expropriation and nationalization under Art. 3, and hence, Huawei is entitled to full reparation.[131]

Art. 2(1) of the China-Sweden BIT reads as follows: "Each Contracting State shall at all times ensure fair and equitable treatment to the invest-

124 International investment agreements cover two types: (i) bilateral investment treaties and (ii) treaties with investment provisions.
125 Huawei Technologies Co., Ltd. v. The Kingdom of Sweden, Request for Arbitration, 2022.
126 Ahlander/Mukherjee.
127 Ibid.
128 Huawei Technologies Co., Ltd. v. The Kingdom of Sweden, Notice on Intent, 2020.
129 Huawei Technologies Co., Ltd. v. Kingdom of Sweden (ICSID Case No. ARB/22/2).
130 Hepburn/Peterson.
131 Huawei Technologies Co., Ltd. v. The Kingdom of Sweden, Request for Arbitration, 2022.

ments by investors of the other Contracting State."[132] This formulation is known as unqualified FET, which "may result in a low liability threshold and brings with it a risk for State regulatory action to be found in breach of it."[133] Investment tribunals tend to interpret the FET as a requirement for contracting states to act consistently, transparently, reasonably, without ambiguity, arbitrariness or discrimination, in an even-handed manner, as well as to ensure due process in decision-making and respect legitimate expectations of investors.[134]

The MFN clause, through which the national treatment standard is incorporated according to Huawei's submission, stipulates that "[i]nvestments by investors of either Contracting State in the territory of the other Contracting State shall not be subjected to a treatment less favourable than that accorded to investments by investors of third States."[135] In substance, national treatment requires contracting parties to extend to foreign investors treatment that is at least as favourable as the treatment they accord to their national investors in the "like" circumstances.[136] In other words, the national treatment ensures equality of competitive opportunities between national and foreign investors.[137] Commentators observe that attempts of investors to invoke MFN clauses to argue that such clauses grant more favourable substantive provisions, which host states have accorded to other investors according to other investment treaties, are frequent in practice, but case law demonstrates limitations on the use of MFN clauses in this way.[138]

The last Huawei claim is based on the guarantees under Art. 3, which reads: "Neither Contracting State shall expropriate or nationalize, or take any other similar measure in regard to, an investment made in its territory by an investor of the other Contracting State, except in the public interest, under due process of law and against compensation, the purpose of which shall be to place the investor in the same financial position as that in which the investor would have been if the expropriation or nationalization had

132 Agreement on the mutual protection of investments between the Kingdom of Sweden and the People's Republic of China (China-Sweden BIT).
133 UNCTAD, Fair and Equitable Treatment, p. 22.
134 Ibid.
135 Art. 2 (2) China-Sweden BIT.
136 UNCTAD, National Treatment.
137 Ibid.
138 Esmé.

not taken place."[139] It is expected that the essence of the legal claim under this provision would be an argument that actions of the Swedish regulator constituted an indirect expropriation. The existing case law exemplifies that different types of measures can give rise to the claims of expropriation, including regulatory measures.[140]

Without making any attempts to predict the outcome of this investor-state dispute, it is reasonable to assume that these legal claims have some merit and might give a ground for the tribunal to rule that Sweden breached its international obligations.

2. Investor-state arbitration as a litigation forum and national security as an exception

In the context of possible investor-state disputes initiated by Huawei, it should be noted that China has concluded 170 IIAs out of which 130 are in force now.[141] Chinese-based Huawei is a global multinational corporation that established multiple entities abroad. This reinforced by the fact that Huawei significantly invested in foreign jurisdictions gives it a strong foothold to bring investment claims against foreign governments, arguing that its rights and legitimate expectations were violated post-establishment.[142]

Looking at the investor-state dispute settlement options available to Huawei in relation to the restrictions preventing company's participation in the 5G rollout, Ioannis Glinavos analysed potential Huawei claims based on the China-Germany BIT,[143] while Jarrod Hepburn and Luke Eric Peterson scrutinized restrictions on Huawei's participation in the 5G rollout against the backdrop of the BITs signed between China and Czech Republic, Canada, Australia and New Zealand.[144] In Glinavos' view, restrictions preventing Huawei participation in 5G projects face a risk of being inconsistent with the cornerstone standards guaranteed under the IIAs: in case of

139 Art. 3 (1) China-Sweden BIT.
140 San Martin.
141 Based on the information from International Investment Agreements Navigator, Investment Policy Hub, UNCTAD, https://investmentpolicy.unctad.org/international-investment-agreements/countries/42/china.
142 This view is corroborated by other scholars, for example, Chaisse/Choukroune/Jusoh/Glinavos, p. 2451 (2476); Hepburn/Peterson.
143 Chaisse/Choukroune/Jusoh/Glinavos, p. 2451 (2476–2477).
144 Hepburn/Peterson (n 130).

the China-Germany BIT, these standards are MFN treatment and national treatment.[145]

If, for example, Sweden's restrictions are found to be inconsistent with its obligations, neither the China-Sweden BIT[146] nor the amendment protocol[147] contain public order or national security exceptions. China has 130 IIAs in force with only 13 of them prescribing an explicit security exception clause,[148] and four of them containing definitions used for security exceptions.[149] These security exceptions are drafted to justify restrictions implemented in the exceptional circumstances such as war, armed military conflicts or actions taken to maintain international peace and security under the UN Charter.[150] Contrary to WTO law, international investment law is fragmented and national security exceptions are not always incorporated in the IIAs.

Even so, Sweden can invoke the customary international law defence of necessity embodied in Art. 25 of the Draft Articles on Responsibility of States for Internationally Wrongful Acts, a move which allowed some states to successfully defend their government policies in the past.[151] To justify its conduct under the plea of necessity, several prerequisites should be fulfilled: (i) the challenged measure safeguards an "essential interest" of the state; (ii) this measure should be the only way of safeguarding that interest;

145 Chaisse/Choukroune/Jusoh/Glinavos, p. 2451 (2477).
146 China-Sweden BIT.
147 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.
148 These IIAs are: China-Hong Kong CEPA Investment Agreement (2017), Australia-China FTA (2015), China-South Korea FTA (2015), China-Japan-South Korea Trilateral Investment Agreement (2012), China-Colombia BIT (2018), China-India BIT(2006), China-Finland BIT (2004), China-Mauritius BIT (1996), China-South Korea BIT (1996), China-Czech Republic BIT (1991), China-New Zealand BIT (1088), China-Sri Lanka BIT (1986) and China-Singapore BIT (1985).
149 Australia-China FTA (2015), China-South Korea FTA (2015), China-Japan-South Korea Trilateral Investment Agreement (2012) and China-Finland BIT (2004).
150 For example, Art. 12.14 of the China – South Korea FTA (2015) provides: Notwithstanding any other provisions in this Chapter other than the provisions of Article 12.5.4 each Party may take any measure: (a) which it considers necessary for the protection of its essential security interests; (i) taken in time of war, or armed conflict, or other emergency in that Party or in international relations; or (ii) relating to the implementation of national policies or international agreements respecting the non-proliferation of weapons; (b) in pursuance of its obligations under the United Nations Charter for the maintenance of international peace and security.
151 Carpentieri.

(iii) the measure addresses a "grave and imminent peril"; (iv) no other essential interest of the state, another state, or the international community should be seriously impaired as a result.[152] 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."[153] In light of this, it remains to be seen if the 5G rollout and the risks associated with it can qualify for this purpose, although some scholars are sceptical of such a possibility.[154]

D. Concluding remarks

Considering the risks embedded in the 5G rollout and the nature of Chinese tech companies (both factors which could not be easily mitigated) and against the background of the geo-political tension between the United States and China, the participation of Chinese vendors in the 5G infrastructure became securitized and politicized.

This securitization and politicization has led to the policies that prevent Chinese tech companies' participation in the 5G rollout. These restrictions are antithetical to the principle of free-market and the idea of economic liberalization underpinning the existing international economic order, its rules and institutions. States that introduce such restrictions often justify them as necessary actions aimed at the securing of their national security interests. It remains to be seen if the 5G rollout and the risks associated with it can be justified under the existing national security clauses.

Ideally, obligations under international economic law should operate as a constraint on the states' discretion to act discriminatory, unfairly or unreasonably. However, as the state practice demonstrates, the existing international economic law, which includes normative rules and dispute settlement mechanisms, does not constrain states from pursuing their policies if the subject matter of such policies becomes securitized or politicized, as it is the case with the 5G rollout.

152 International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, 2001.

153 Paddeu/Waibel, Foreign Investment Law Journal 2022, 160.

154 Du, Emory International Law Review 2023, 1.

Bibliography

5GAA Automotive Association, Accelerating 5G Adoption for Connected and Autonomous Mobility Services: White Paper, 2023, https://5gaa.org/content/uploads/2023/04/5gaa-wp-market-pull-mapu.pdf (last accessed: 8 February 2024).

Ahlander, Johan/Mukherjee, Supantha, Swedish court upholds ban on Huawei selling 5G network gear, 2021, https://www.reuters.com/technology/swedish-court-upholds-ban-huawei-selling-5g-network-gear-2021-06-22/ (last accessed: 8 February 2024).

BBC News, Huawei and ZTE handed 5G network ban in Australia, 2018, https://www.bbc.com/news/technology-45281495 (last accessed: 8 February 2024).

BBC News, Qatar Crisis: What You Need to Know, 2017, https://www.bbc.com/news/world-middle-east-40173757 (last accessed: 8 February 2024).

Bing, Christopher, Suspected Russian hackers spied on U.S. Treasury emails – sources, 2020. https://www.reuters.com/article/us-usa-cyber-treasury-exclsuive/suspected-russian-hackers-spied-on-u-s-treasury-emails-sources-idUKKBN28N0PG?edition-redirect=uk (last accessed: 8 February 2024).

Bogdanova, Iryna, Politicization of the 5G Rollout: Litigation Way for Huawei?, WTI working paper no. 01/2023, 2023, https://ssrn.com/abstract=4345025 (last accessed: 8 February 2024).

Bogdanova, Iryna/Vásquez Callo-Müller, María, Unilateral Cyber Sanctions: Between Questioned Legality and Normative Value, Vanderbilt Journal of Transnational Law 2021, 911.

Bogdanova, Iryna/Vásquez Callo-Müller, María, Unilateral Economic Sanctions to Deter and Punish Cyber-Attacks: Are They Here to Stay?, EJIL:Talk! Blog of the European Journal of International Law 2021, https://www.ejiltalk.org/unilateral-economic-sanctions-to-deter-and-punish-cyber-attacks-are-they-here-to-stay/ (last accessed: 8 February 2024).

Bogdanova, Iryna/Wang, Anqi, China's Use of Export Restrictions and WTO Law: Are We Heading Towards 'Weaponization' of Exports?' in Gao/Raess/Zeng (eds.), China and the WTO: A Twenty-Year Assessment, Cambridge 2023, p. 160.

Brooks, Thom, Huawei's participation is a brave step for British 5G networks, 2019, https://news.cgtn.com/news/3d3d774e786b6a4d34457a6333566d54/index.html (last accessed: 8 February 2024).

Carpentieri, Leonardo, Necessity as a Defence, 2023, https://jusmundi.com/en/document/publication/en-necessity-as-a-defence (last accessed: 8 February 2024).

Carvin, Stephanie, Banning Huawei Was the Start, Not the End, of Protecting Cyber Infrastructure, 2022, https://www.cigionline.org/articles/banning-huawei-was-the-start-not-the-end-of-protecting-cyber-infrastructure/ (last accessed: 8 February 2024).

Cerulus, Laurens, Huawei challenges legality of 5G bans in Poland, Romania, 2020, https://www.politico.eu/article/huawei-hints-at-legal-action-against-5g-bans-in-poland-romania/# (last accessed: 8 February 2024).

Cerulus, Laurens/Wheaton, Sarah, How Washington chased Huawei out of Europe, 2022, https://www.politico.eu/article/us-china-huawei-europe-market/ (last accessed: 8 February 2024).

CNBC, New Zealand rejects Huawei's first 5G bid citing national security risk, 2018, https://www.cnbc.com/2018/11/28/new-zealand-rejects-huaweis-5g-bid-citing-national-security-risk.html (last accessed: 8 February 2024).

Dahlman, Erik/Parkvall, Stefan/Sköld, Johan, What Is 5G? in Dahlman/Parkvall/Sköld (eds.), 5G NR: the Next Generation Wireless Access Technology, London/ San Diego/ Cambridge/ Oxford 2018, p.1.

Du, Ming, Huawei Strikes Back: Challenging National Security Decisions before Investment Arbitral Tribunals, Emory International Law Review 2023, 1.

Duffy, Clare, What is 5G? Your questions answered, 2020, https://edition.cnn.com/interactive/2020/03/business/what-is-5g/ (last accessed: 8 February 2024).

Esmé, Shirlow, Most Favoured Nation Treatment, 2023, https://jusmundi.com/en/document/publication/en-most-favoured-nation-treatment (last accessed: 8 February 2024).

Eurasia Group, The Digital Silk Road: Expanding China's Digital Footprint, 2020 https://www.eurasiagroup.net/files/upload/Digital-Silk-Road-Expanding-China-Digital-Footprint-1.pdf (last accessed: 8 February 2024).

Eurasia Group, The Geopolitics of 5G: White Paper, 2018, https://www.eurasiagroup.net/siteFiles/Media/files/1811-14%205G%20special%20report%20public(1).pdf (last accessed: 8 February 2024).

Farrell, Henry/Newman, Abraham, Weaponized Interdependence: How Global Economic Networks Shape State Coercion, International Security 2019, 42.

Friis, Karsten/Lysne, Olav, Huawei, 5G and Security: Technological Limitations and Political Responses, Development and Change 2021, 1174.

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

Glinavos, Ioannis, Which Way Huawei? ISDS Options for Chinese Investors, in Chaisse/ Choukroune/Jusoh (eds.), Handbook of International Investment Law and Policy, Singapore 2020.

Gold, Hadas, UK bans Huawei from its 5G network in rapid about-face, 2020, https://edition.cnn.com/2020/07/14/tech/huawei-uk-ban/index.html (last accessed: 8 February 2024).

Grotto, Andrew, The Huawei problem: A risk assessment, Global Asia 2019, 13, https://www.globalasia.org/v14no3/cover/the-huawei-problem-a-risk-assessment_andrew-grotto (last accessed: 8 February 2024).

Harrell, Peter, 5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation, Testimony before the United States Senate Committee on the Judiciary, 2019, https://www.jstor.org/stable/resrep28738 (last accessed: 8 February 2024).

Hemmings, John/Cho, Sungmin, South Korea's Growing 5G Dilemma, 2020, https://www.csis.org/analysis/south-koreas-growing-5g-dilemma (last accessed: 8 February 2024).

Hepburn, Jarrod/Peterson, Luke Eric, 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, 2019, 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/ (last accessed: 8 February 2024).

Innovation, Science and Economic Development Canada, Policy Statement: Securing Canada's Telecommunications System, 2022, https://www.canada.ca/en/innovation-science-economic-development/news/2022/05/policy-statement--securing-canadas-telecommunications-system.html# (last accessed: 8 February 2024).

Kharpal, Arjun, Here's which leading countries have barred, and welcomed, Huawei's 5G technology, 2019, https://www.cnbc.com/2019/04/26/huawei-5g-how-countries-view-the-chinese-tech-giant.html (last accessed: 8 February 2024).

Larsen, Henrik, Telecom Troubles: Adapting Networks to Defend Europe, 2023, https://cepa.org/article/telecom-troubles-adapting-networks-to-defend-europe/ (last accessed: 8 February 2024).

Lee, Kristine/Rasser, Martijn/Fitt, Joshua/Goldberg, Coby, Digital Entanglement: Lessons Learned from China's Growing Digital Footprint in South Korea, 2020, https://www.cnas.org/publications/reports/digital-entanglement (last accessed: 8 February 2024).

Lewis, James Andrew, 5G: The Impact on National Security, Intellectual Property, and Competition, Statement before the United States Senate Committee on the Judiciary, 2019, https://www.jstor.org/stable/resrep37608 (last accessed: 8 February 2024).

Lysne, Olav/Elmokashfi, Ahmed/Schia, Niels Nagelhus/Gjesvik, Lars/Friis, Karsten, Critical Communication Infrastructures and Huawei, TPRC47: The 47th Research Conference on Communication, Information and Internet Policy 2019, https://ssrn.com/abstract=3426222 (last accessed: 8 February 2024).

Moore, Gregory J., Huawei, Cyber-Sovereignty and Liberal Norms: China's Challenge to the West/Democracies, Journal of Chinese Political Science 2022, 151.

Mulligan, Stephen P./Linebaugh Chris D., Huawei and U.S. Law, Congressional Research Service Report R46693, 2021, https://sgp.fas.org/crs/misc/R46693.pdf (last accessed: 8 February 2024).

Myers, Margaret/Montenegro, Guillermo Garcia, Latin America and 5G: Five Things to Know, 2019, https://www.thedialogue.org/analysis/latin-america-and-5g-five-things-to-know/ (last accessed: 8 February 2024).

Nakashima, Ellen, U.S. pushes hard for a ban on Huawei in Europe, but the firm's 5G prices are nearly irresistible, 2019, 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 (last accessed: 8 February 2024).

Nguyen, Van-Giang/Brunstrom, Anna/Grinnemo, Karl-Johan/Taheri Javid, 5G Mobile Networks: Requirements, Enabling Technologies, and Research Activities, in Liyanage, Ahmad, Abro, Gurtov, Ylianttila (eds.), A Comprehensive guide to 5G security, 2018.

NIS Cooperation Group, Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity, 2020.

NIS Cooperation Group, Second report on Member States' Progress in implementing the EU Toolbox on 5G Cybersecurity, 2023.

Paddeu, Federica/Waibel, Michael, Necessity 20 Years On: The Limits of Article 25, ICSID Review – Foreign Investment Law Journal 2022, 160.

Peng, Shin-yi, Cybersecurity Threats and the WTO National Security Exceptions, JIEL 2015, 449.

Pham, Manny, Brazil, China join hands for upgrade to 5G and cybersecurity, 2023, https://developingtelecoms.com/telecom-technology/optical-fixed-networks/14867-brazil-china-join-hands-for-upgrade-to-5g-and-cybersecurity.html (last accessed: 8 February 2024).

Poliakine, Ran, What You Should Know About 5G Technology And What The Future Holds, 2021, https://www.forbes.com/sites/forbestechcouncil/2021/08/12/what-you-should-know-about-5g-technology-and-what-the-future-holds/?sh=4d21cfd9636b (last accessed: 8 February 2024).

Radu, Roxana/Amon, Cedric, The governance of 5G infrastructure: between path dependency and risk-based approaches, Journal of Cybersecurity 2021, 1.

Reuters, Japan to ban Huawei, ZTE from govt contracts -Yomiuri, 2018, https://www.reuters.com/article/japan-china-huawei-idUSL4N1YB6JJ (last accessed: 8 February 2024).

Roberts, Anthea/Moraes, Henrique Choer/Ferguson, Victor, Toward a Geoeconomic Order in International Trade and Investment, JIEL 2019, 655.

Robles-Carrillo, Margarita, European Union policy on 5G: Context, scope and limits, Telecommunications Policy 2021, 1.

Rubin, Alex/Martinez, Alan Omar Loera/Dow, Jake/Puglisi Anna, The Huawei Moment: CSET Policy Brief, Center for Security and Emerging Technology, 2021, https://cset.georgetown.edu/publication/the-huawei-moment/ (last accessed: 8 February 2024).

Sacks, David, China's Huawei Is Winning the 5G Race. Here's What the United States Should Do To Respond, 2021, https://www.cfr.org/blog/china-huawei-5g (last accessed: 8 February 2024).

San Martin, Isabel, Expropriation, 2023, https://jusmundi.com/en/document/publication/en-expropriation (last accessed: 8 February 2024).

Strand Consult, The Market for 5G RAN in Europe: Share of Chinese and Non-Chinese Vendors in 31 European Countries, 2023, https://strandconsult.dk/the-market-for-5g-ran-in-europe-share-of-chinese-and-non-chinese-vendors-in-31-european-countries/ (last accessed: 8 February 2024).

Strand Consult, Understanding the Market for 4G RAN in Europe: Share of Chinese and Non-Chinese Vendors in 102 Mobile Networks, 2020, https://strandconsult.dk/understanding-the-market-for-4g-ran-in-europe-share-of-chinese-and-non-chinese-vendors-in-102-mobile-networks/ (last accessed: 8 February 2024).

SWI swissinfo.ch, Switzerland to tighten up defences against cyber attacks, 2023, https://www.swissinfo.ch/eng/sci-tech/switzerland-to-tighten-up-defences-against-cyber-attacks/49062790 (last accessed: 8 February 2024).

Temple-Raston, Dina, A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack, 2021, https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack (last accessed: 8 February 2024).

UNCTAD, Fair and Equitable Treatment: UNCTAD Series on Issues in International Investment Agreements II, 2012.

UNCTAD, National Treatment: UNCTAD Series on issues in international investment agreements, 199.

Wheeler, Tom, 5G in five (not so) easy pieces, 2019, https://www.brookings.edu/research/5g-in-five-not-so-easy-pieces/ (last accessed: 8 February 2024).

Contributors

Dr Iryna Bogdanova

World Trade Institute

iryna.bogdanova@wti.org

Dr Iryna Bogdanova is a postdoctoral researcher at the World Trade Institute (WTI), University of Bern. Her current research project aims to clarify, comprehend, and structure the evolution of the concept of technological sovereignty, which denotes policies implemented by states to decrease their dependence on foreign-produced "critical technologies", along with its sphere of influence in international economic law.

Dr Sophie Bohnert LL.M. (College of Europe)

Wirtschaftsuniversität Wien

sophie.bohnert@wu.ac.at

Sophie Bohnert holds a Bachelor's and Master's degree in Business Law from the Vienna University of Economics and Business/Maastricht University, as well as a Bachelor's degree in Business, Economics, and Social Sciences (major in Business Administration) from the Vienna University of Economics and Business. Sophie also holds a postgraduate Master's degree in European Legal Studies, specialising in European Law and Economic Analysis, from the College of Europe in Bruges. Sophie currently works as a teaching and research assistant (doctoral candidate) at the Institute for European and International Law at the Vienna University of Economics and Business.

Dr Carsten Bormann M.Jur (Oxford)

Oppenhoff & Partner Rechtsanwälte

carsten.bormann@oppenhoff.eu

Carsten Bormann is an attorney in Oppenhoff's public law and foreign trade practice. In addition to foreign direct investment screening, he advises on a variety of complex regulatory issues as well as compliance and internal investigations. Recently, he has been increasingly involved in climate change litigation and ESG regulation.