Emory International Law Review

Volume 37 | Issue 1

2022

Huawei Strikes Back: Challenging National Security Decisions Before Investment Arbitral Tribunals

Ming Du

Huawei Strikes Back: Challenging National Security Decisions Before Investment Arbitral Tribunals

Cover Page Footnote

As a direct reaction to rising investment from China amid the transformation of the geopolitical context in which China has emerged as a great power, Western countries, including the United States, have introduced new or reinforced existing national security screening mechanisms. Confronting weaponized national security reviews in host countries, Chinese investors have recently begun to challenge national security decisions before international investment arbitral tribunals, claiming that such decisions have breached host countries' obligations under international investment treaties. Chinese telecoms giant Huawei's investment treaty claim against the Government of Sweden before the International Centre for Settlement of Investment Disputes (ICSID) over its exclusion from the rollout of 5G network in January 2022 is one of the most prominent examples. This article takes stock of the whole body of arbitral awards rendered on national security decisions in investment arbitration and applies it to Huawei's ongoing complaint against the Government of Sweden. As the first critical analysis of whether the ban on Huawei from supplying 5G infrastructure on national security grounds violated the Government of Sweden's investment treaty obligations, this article argues that Huawei is likely to fight an uphill battle in persuading the arbitral tribunal that the Swedish national security decision is inconsistent with the China-Sweden bilateral investment treaty. The analytical framework provided in this article is useful to analyze all future investment disputes initiated by foreign investors regarding host countries' national security decisions. Moreover, this article argues that Huawei's challenge of the national security decision of the Government of Sweden is not an isolated incident, but an outgrowth of a long-brewing tension between China's state capitalism and the liberal international economic order. Whether the investment arbitral tribunal may handle the Huawei dispute adroitly is a litmus test of the resiliency of international investment norms to accommodate systemic friction between heterogeneous political-economic models and rising strategic distrust in the era of geoeconomics.

HUAWEI STRIKES BACK: CHALLENGING NATIONAL SECURITY DECISIONS BEFORE INVESTMENT ARBITRAL TRIBUNALS

Ming Du[*]

ABSTRACT

As a direct reaction to rising investment from China amid the transformation of the geopolitical context in which China has emerged as a great power, Western countries, including the United States, have introduced new or reinforced existing national security screening mechanisms. Confronting weaponized national security reviews in host countries, Chinese investors have recently begun to challenge national security decisions before international investment arbitral tribunals, claiming that such decisions have breached host countries' obligations under international investment treaties. Chinese telecoms giant Huawei's investment treaty claim against the Government of Sweden before the International Centre for Settlement of Investment Disputes (ICSID) over its exclusion from the rollout of 5G network in January 2022 is one of the most prominent examples.

This article takes stock of the whole body of arbitral awards rendered on national security decisions in investment arbitration and applies it to Huawei's ongoing complaint against the Government of Sweden. As the first critical analysis of whether the ban on Huawei from supplying 5G infrastructure on national security grounds violated the Government of Sweden's investment treaty obligations, this article argues that Huawei is likely to fight an uphill battle in persuading the arbitral tribunal that the Swedish national security decision is inconsistent with the China-Sweden bilateral investment treaty. The analytical framework provided in this article is useful to analyze all future investment disputes initiated by foreign investors regarding host countries' national security decisions. Moreover, this article argues that Huawei's challenge of the national security decision of the Government of Sweden is not an isolated incident, but an outgrowth of a long-brewing tension between China's state capitalism and the liberal international economic order. Whether the investment arbitral tribunal may handle the Huawei dispute adroitly is a

[*] Professor, Durham Law School, UK.

litmus test of the resiliency of international investment norms to accommodate systemic friction between heterogeneous political-economic models and rising strategic distrust in the era of geoeconomics.

TABLE OF CONTENTS

INTRODUCTION

As the international economic order is transitioning away from a neoliberal order, in which deeper economic integration was viewed as contributing to mitigating conflicts and preserving world peace, towards a new geoeconomic order, in which economic interdependence itself is seen as a security risk, it is no longer possible to separate national security threats from economic issues.[1] Indeed, one of the most striking trends in investment policy over the past decade was that numerous countries have introduced new or reinforced existing national security screening mechanisms for foreign investment.[2] Recent examples include the United Kingdom's National Security and Investment Act 2021,[3] the European Union's framework for screening foreign direct investment,[4] the enhanced investment screening requirements that are embodied in Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) in the United States,[5] and Measures for the Security Review of Foreign Investment adopted in 2020 in China.[6] The COVID-19 pandemic has accelerated this trend in response to new national security concerns about foreign investment.[7]

It is no secret that the upgrading of investment screening mechanisms in some Western countries represents a direct reaction to rising investment from China in sensitive industries and, more broadly, to the transformation of the geopolitical context in which China has emerged as a great power.[8] The Government of China has vehemently criticized national security review of foreign investment from China in some Western countries as discriminatory,

---

[1] Anthea Roberts et al., *Toward a Geoeconomic Order in International Trade and Investment*, 22 J. INT'L ECON. L. 655, 676 (2019).

[2] *See* U.N. CONF. ON TRADE & DEV., NATIONAL SECURITY-RELATED SCREENING MECHANISMS FOR FOREIGN INVESTMENT: AN ANALYSIS OF RECENT POLICY DEVELOPMENTS 4 (Dec. 2019), https://unctad.org/system/files/official-document/diaepcbinf2019d7_en.pdf; Michael E. Leiter et al., *CFIUS Goes Global: New FDI Review Processes Proliferate, Old Ones Expand*, SKADDEN (Jan. 19, 2022), https://www.skadden.com/insights/publications/2022/01/2022-insights/regulation-enforcement-and-investigations/cfius-goes-global.

[3] The National Security and Investment Act 2021, c. 25 (U.K.).

[4] Regulation 2019/452, of the European Parliament and of the Council of Mar. 19, 2019, Establishing a Framework for the Screening of Foreign Direct Investments into the Union, 2019 O.J. (L 79/1).

[5] Foreign Investment Risk Review Modernization Act of 2018, Pub. L. No. 115–132, § 1701, 132 Stat. 2174 [hereinafter FIRRMA].

[6] Measures for the Security Review of Foreign Investment No. 37 (promulgated by the Nat'l Dev. & Reform Comm'n of the People's Republic of China and the Ministry of Com. of the People's Republic of China, Dec. 19, 2020, effective Jan. 18, 2021) (China).

[7] Harlan Grant Cohen, *Nations and Markets*, 23 J. INT'L ECON. L. 793, 796–97 (2020).

[8] Maria Adele Carrai, *The Rise of Screening Mechanisms in the Global North: Weaponizing the Law Against China's Weaponized Investments?*, 8 CHINESE J. COMP. L. 351, 356–62 (2020).

arbitrary, and politicalized. For example, commenting on Australia's decision to block the acquisition of a major Australian construction company by a Chinese state-owned enterprise in 2021, the Chinese Embassy in Canberra accused the Australian government of "weaponizing" national security.[9] China's Ministry of Commerce has also identified the abuse of national security review as a major regulatory hurdle for Chinese investors in the United States.[10]

To respond to the allegedly unfair and arbitrary national security reviews, Chinese investors have resorted to a range of formal and informal mitigating and remedial measures, including lobbying, media campaigns, diplomatic assistance, support from business associations, and contesting national security decisions in domestic courts of host states.[11] However, Chinese investors have rarely challenged national security decisions before international investment arbitral tribunals.[12] The lack of effective use of investor-state dispute settlement (ISDS) by Chinese investors stands in sharp contrast to the number of international investment treaties (IIAs) China has signed, many of which include most of the standard investment protections along with full advance consent to ISDS.[13]

Beneath the apparently calm surface, the situation is stormy. The presence of Chinese investors in ISDS proceedings has been rising fast in recent years. Since 2019, Chinese investors have filed nine investment arbitration cases against foreign host states, more than what Chinese investors had filed for nearly forty years since China entered into the first bilateral investment treaty with Sweden in 1982.[14] Most significantly, the Chinese telecoms giant Huawei filed a formal investment treaty claim against the Government of Sweden before the International Centre for Settlement of Investment Disputes (ICSID) in January 2022. The claim was concerned with Huawei's exclusion from the rollout of 5G

[9] Levi Parsons, *Furious China Accuses Australia of 'Weaponising National Security' by Blocking a $300 Million Takeover of a Major Building Company*, DAILY MAIL AUSTL. (Jan. 12, 2021), https://www.dailymail.co.uk/news/article-9139979/China-accuses-Australia-weaponising-national-security-blocking-300million-takeover.html.

[10] *Ministry of Commerce Regular Press Briefing*, MINISTRY OF COM. CHINA (July 25, 2019), http://english.mofcom.gov.cn/article/newsrelease/press/201908/20190802889887.shtml.

[11] Ji Li, *In Pursuit of Fairness: How Chinese Multinational Companies React to U.S. Government Bias*, 62 HARV. INT'L L.J. 375, 380–87 (2021).

[12] *Id.* at 398–400.

[13] Yuwen Li & Bian Cheng, *China's Stance on Investor-State Dispute Settlement: Evolution, Challenges, and Reform Options*, 67 NETH. INT'L L. REV. 503, 514–23 (2020).

[14] Ming Du, *Explaining China's Approach to Investor-State Dispute Settlement Reform*, 27 EUR. L.J. (forthcoming 2022).

network in Sweden amid national security concerns.[15] It is widely recognized that Huawei's legal challenge of the Swedish ban may be only the tip of the iceberg given that Huawei equipment is currently banned in over a dozen countries and even more countries are considering banning Huawei equipment from their 5G networks.[16]

This article provides the first critical analysis of *Huawei Technologies Co., Ltd. v. Kingdom of Sweden* amid the heated global political debate on how to handle alleged national security concerns about Huawei. International arbitral tribunals have dealt with foreign investors' complaints against national security decisions of host states in a number of disputes.[17] Because of substantial textual variations among IIAs and the lack of an appellate mechanism in ISDS, *ad hoc* arbitral tribunals have so far rendered inconsistent interpretations of even the same investment treaty provisions.[18] Consequently, precisely how investment arbitral tribunals approach national security decisions of host states is a case-by-case exercise.[19] Huawei's challenge to the Swedish ban provides a new opportunity for an investment arbitral tribunal to clarify some long outstanding questions concerning the national security defense in ISDS.

Taking stock of all the public information about Huawei and the whole body of arbitral awards rendered on measures taken for safeguarding national security, this article argues that Huawei is likely to fight an uphill battle in persuading the arbitral tribunal that the Swedish decision is inconsistent with the China-Sweden bilateral investment treaty (BIT). More importantly, this article argues that Huawei's challenge to the national security decision of the government of Sweden is not an isolated incident but an outgrowth of a long-brewing tension between China' party-state capitalism and the liberal international economic

[15] Huawei Tech. Co., Ltd. v. Kingdom of Sweden, ICSID Case No. ARB/22/2 (registered on Jan. 21, 2022).

[16] Joe Panettieri, *Huawei: Banned and Permitted in Which Countries*?, CHANNELE2E (Dec. 27, 2021), https://www.channele2e.com/business/enterprise/huawei-banned-in-which-countries/; Ian Young, *Why a Canadian Ban on Huawei 5G May Come with a Whimper, Not a Bang*, S. CHINA MORNING POST (Nov. 24, 2021), https://www.scmp.com/news/china/diplomacy/article/3157141/why-canadian-ban-huawei-5g-may-come-whimper-not-bang.

[17] At least sixteen national security-related investment cases have been examined by international arbitration tribunals. Most of these cases (ten) involved claims filed by foreign investors against Argentina. *See* U.N. CONF. TRADE & DEV., WORLD INVESTMENT REPORT 2016: INVESTOR NATIONALITY: POLICY CHALLENGES 97 (2017).

[18] Susan D. Franck, *The Legitimacy Crisis in Investment Treaty Arbitration: Privatizing Public International Law Through Inconsistent Decisions*, 73 FORDHAM L. REV. 1521, 1545–46 (2005).

[19] Martins Paparinskis, *Circumstances Precluding Wrongfulness in International Investment Law*, 31 INT'L CENTER SETTLEMENT INV. DISP. REV. 484, 493–96 (2016).

order.[20] Whether the investment arbitral tribunal may handle the dispute adroitly is a litmus test of the resiliency of international investment norms to accommodate systemic friction between heterogeneous political-economic models and rising strategic distrust in the era of geoeconomics.[21]

The article proceeds as follows. Part II explains the driving forces behind the proliferation of national security review in international investment. Using the national security review in the United States as an example, it also illustrates why certain features of national security review are viewed as "weaponized" against Chinese investors. Part III reviews critically how investment arbitral tribunals scrutinize sensitive national security decisions of host states. Part IV provides the first analysis of the *Huawei Technologies Co., Ltd. v. Kingdom of Sweden* dispute, identifying the key legal issues raised by the dispute and analyzing how the arbitral tribunal may approach these issues. Part V concludes the article by suggesting that the outcome of the Huawei dispute will have a lasting effect on shaping the contours of international investment law in the age of geoeconomics.

I. THE WEAPONIZATION OF NATIONAL SECURITY REVIEW IN INTERNATIONAL INVESTMENT LAW

A. Explaining the Proliferation of National Security Review

A number of factors account for the proliferation of national security review mechanisms in national foreign investment laws. To begin with, whereas the concept of national security was traditionally framed in terms of armed attack, civil war, terrorist activity, rioting or other nexus to warfare, the range of issues may be credibly described as national security has expanded exponentially in the 21st century world of complex supply chains and "weaponized interdependence."[22] Diffuse threats such as economic emergencies, infectious disease, cybersecurity, transnational crime, corruption, human rights violations, environmental degradation, and climate change are perceived as national security matters even if there is no military dimension to the threat.[23] As the

[20] Margaret Pearson, Meg Rithmire & Kellee S. Tsai, *Party-State Capitalism in China* 6 (Harv. Bus. Sch., Working Paper No. 21-065, 2020).

[21] KENNETH LIEBERTHAL & WANG JISI, ADDRESSING US-CHINA STRATEGIC DISTRUST 20–33 (2012).

[22] Henry Farrell & Abraham L. Newman, *Weaponized Interdependence: How Global Economic Networks Shape State Coercion*, 44 INT'L SEC. 42, 45 (2019).

[23] J. Benton Heath, *The New National Security Challenge to the Economic Order*, 129 YALE L.J. 1020, 1034–35 (2020).

range of security threats expands, so does the range of industries that may be considered security sensitive. The sensitive sectors are no longer limited to military and defense industries and can encompass, among others, telecommunications, transportation, energy, water and food supply, education, health services, and the media.[24] For example, the national security review of foreign investment in Canada may take into account not only factors related to traditional militarized security, such as the potential effects on Canada's national defense capabilities and sensitive technology with military, intelligence or dual military/civilian applications, but also new national security concerns such as supply of critical goods and services, sensitive personal data, organized crime, and corrupt foreign officials.[25]

Furthermore, technology is a key enabler for economic, political, and military power, and a crucial factor for the international competitiveness of countries.[26] The mastery of cutting-edge technologies and know-how is vital to economic growth, national security, and social stability.[27] Some technological areas, such as artificial intelligence, high-performance computing, biomaterials and the emerging 5G environment, appear to offer the potential for transformative change. Advances in these areas are likely to shape societies, economies, and create new forms of power and influence in the international system.[28] Consequently, states in possession of such assets may have a strong interest in ensuring that they remain in domestic hands. This point was succinctly put by Chinese President Xi Jinping:

> Science and technology innovation has become a critical support for increasing comprehensive national strength . . . whoever holds the key to science and technology innovation makes an offensive move in the chess game and will be able to preempt the rivals and win the advantages.[29]

---

[24] Frédéric Wehrlé & Joachim Pohl, *Investment Policies Related to National Security – A Survey of Country Practices* 23 (OECD Working Papers on Int'l Inv., Paper No. 2016/02, 2016).

[25] Minister of Innovation, Sci. & Ind., *Guidelines on the National Security Review of Investments*, GOV'T OF CAN. (Mar. 24, 2021), https://www.ic.gc.ca/eic/site/ica-lic.nsf/eng/lk81190.html (Can.).

[26] MARTIJN RASSER & MEGAN LAMBERTH, TAKING THE HELM: A NATIONAL TECHNOLOGY STRATEGY TO MEET THE CHINA CHALLENGE 9–11 (2021).

[27] James Manyika et al., *Disruptive Technologies: Advances that will Transform Life, Business, and the Global Economy*, 19 MCKINSEY GLOB. INST. (May 2013).

[28] Office of the Dir. of Nat'l Intelligence, *Global Trends 2040: A More Contested World*, 54–65 (Mar. 2021); MATTHEW DANIELS & BEN CHANG, NATIONAL POWER AFTER AI 13–23 (2021).

[29] XI JINPING, THE GOVERNANCE OF CHINA 132–33 (2014).

At the same time, President Xi highlighted the importance of leading in technology through one's own efforts, adding that:

> Only by holding these technologies in our own hands can we ensure economic security, national security and security in other areas … we will realize the goal that core technologies are self-developed and controllable, and keep the initiative for innovation and development securely in our own hands.[30]

In the same logic, the European Union is investing billions of euros into what it believes are fundamental and core technologies as part of an effort to boost its "technology sovereignty" and reduce its dependency on technologies that come from beyond its borders.[31] With recent supply chain disruptions in the semiconductor and other industries, technological sovereignty is seen as a particularly important issue.[32]

Against this background, it is widely acknowledged that technology competition is central to Sino-American geostrategic competition.[33] It is therefore unsurprising that the FIRRMA expands the scope of "covered transactions" that fall within the national security review to include critical *technologies*; critical *infrastructure*; and security-sensitive personal *data* of U.S. citizens (TID U.S. business).[34] Notably, there is no equity investment threshold that would exclude a "covered transaction" in a TID U.S. business, meaning that a foreign person acquiring even a minority interest in a TID U.S. business would be considered a "covered transaction" if certain rights are granted to foreign investors.[35]

Next, strengthening national security mechanisms is in part also a reaction to the increasing investment activities of state-owned enterprises (SOEs) and sovereign wealth funds. Despite three decades of extensive state reform and

---

[30] Xi Jinping, President of China, Make China a Global Centre for Science and Innovation, Speech at the Joint Session of the 19th Meeting of the Members of the Chinese Academy of Sciences and the 14th Meeting of the Members of the Chinese Academy of Engineering (May 28, 2018).

[31] Sam Shead, *Europe is Focusing on "Tech Sovereignty" as Tensions Flare between the U.S. and China*, CNBC (Mar. 10, 2021), https://www.cnbc.com/2021/03/10/tech-sovereignty-key-issue-for-europe-amid-tensions-between-us-china.html.

[32] European Commission Press Release, Digital Sovereignty: Commission Proposes Chips Act to Confront Semiconductor Shortages and Strengthen Europe's Technological Leadership (Feb. 8, 2022).

[33] Brad Glosserman, *Rethink Power in a New Era of Great Power Competition*, NAT'L INTEREST (Aug. 28, 2021), https://nationalinterest.org/feature/rethink-%E2%80%98power%E2%80%99-new-era-%E2%80%98great-power-competition%E2%80%99%C2%A0-192320.

[34] FIRRMA, *supra* note 5, § 1703(a)(4)(B)(iii).

[35] *Id.* §1703(a)(4).

privatization, sovereign investments remain an important economic force in the global economy.[36] Over the past decade, the share of SOE assets among the world's 2,000 largest firms has doubled to twenty percent. At $45 trillion in 2018, these assets are equivalent to fifty percent of global GDP.[37] According to the OECD, 132 of the world's largest 500 enterprises measured by annual revenues were wholly or majority owned by sovereign governments in 2020, compared to 34 two decades ago.[38] Beyond state ownership in enterprises, some SOEs are directly or indirectly influenced by the state through various means, including their foreign acquisitions being facilitated by financing below market rates provided by the state.[39] SOEs have accounted for five to fifteen percent of annual cross-border acquisitions since 2008.[40]

SOEs are in a unique position to drive economic growth and generate significant spillovers to the rest of the economy given their size and financial power.[41] For example, unlike other types of institutional investors, state-owned investors provide long-term and guaranteed quiet capital in case of future funding needs, and therefore reduce the uncertainty regarding the firm's future financing ability.[42] They also make companies more valuable because they reduce firms' cost of capital as a result of their commanding lower risk premiums.[43]

However, one of the most acute concerns regarding sovereign investments is thatcorporate and investment decisions of sovereign controlled companies may be driven by political and strategic objectives rather than commercial and market

[36] Milan Babic, *State Capital in a Geoeconomic World: Mapping State-led Foreign Investment in the Global Political Economy*, REV. INT'L. ECON. 5 (forthcoming 2022).

[37] *Fiscal Monitor: Policies to Support People During the Covid-19 Pandemic*, IMF (Apr. 2020), https://www.imf.org/en/Publications/FM/Issues/2020/04/06/fiscal-monitor-april-2020.

[38] OECD, TRANSPARENCY AND DISCLOSURE PRACTICES OF STATE-OWNED ENTERPRISES AND THEIR OWNERS 8 (2020).

[39] European Comm'n Staff Working Document, *Impact Assessment Accompanying the Proposal for a Regulation of the European Parliament and of the Council on Foreign Subsidies Distorting the Internal Market*, at 13, SWD (2021) 99 final (May 5, 2021).

[40] U.N. CONFERENCE ON TRADE AND DEVELOPMENT, WORLD INVESTMENT REPORT 2019: SPECIAL ECONOMIC ZONES 26–27 (2019).

[41] *State-owned Enterprises: Understanding Their Market Effects and the Need for Competitive Neutrality*, WORLD BANK, https://thedocs.worldbank.org/en/doc/739371594131714315-0130022020/original/15444WBSOEWEB.pdf.

[42] PATRICK BOLTON ET AL., SOVEREIGN WEALTH FUNDS AND LONG-TERM INVESTING 2 (Columbia Univ. Press, 2012).

[43] Nuno Fernandes, *The Rising Importance of Sovereign Wealth Funds*, 46 HEDGE FUND J. (Apr. 2009), https://thehedgefundjournal.com/the-rising-importance-of-sovereign-wealth-funds/.

considerations.[44] Different from private investors, sovereign investment is not necessarily expected to maximize profits and long-term corporate value. Indeed, the rationale for continued state ownership would often be that state-owned entities are expected to act differently from privately-owned enterprises under some circumstances.[45] That gives rise to concerns that sovereign investment may jeopardize the national security, energy security, economic security, technological edge, or other vital interests of a host country.[46]

Lastly, the upgrading of investment screening mechanisms in some Western countries represents a direct reaction to rising investment from China in strategic industries as well as to the transformation of the geopolitical context. China' practice of the unique state capitalism model has generated a heated debate regarding the merits of state-led development and the crisis of western liberal capitalism.[47] For the first time since 1850 the global capitalist system is experiencing the rapid rise of a continent-size capitalist power that espouses ideas, institutions, interests, and values fundamentally different from those of Anglo-American capitalism.[48] Therefore, China's state-led economic model itself was identified as a key challenge to the liberal international economic order, and in particular, the economic and national security interests of the United States.[49] The U.S. National Defense Authorization Act for 2019 declared that "long-term strategic competition with China is a national security priority that must be addressed through a combination of military, political, and economic means."[50]

[44] Jennifer Lind & Daryl G. Press, *Markets or Mercantilism? How China Secures its Energy Supplies*, 42 INT'L SEC. 170, 204 (2018).

[45] OECD, STATE-OWNED ENTERPRISES AS GLOBAL COMPETITORS: A CHALLENGE OR AN OPPORTUNITY? 27–28 (2016).

[46] European Commission, *Welcoming Foreign Direct Investment While Protecting Essential Interests*, COM (2017) 494 final (Sept. 13, 2017).

[47] JOSHUA KURLANTZI, STATE CAPITALISM: HOW THE RETURN OF STATISM IS TRANSFORMING THE WORLD 72–73 (Oxford Univ. Press, 2016).

[48] Christopher A. McNally, *Sino-Capitalism: China's Reemergence and the International Political Economy*, 64 WORLD POL. 741, 765 (2012).

[49] The U.S.-China Economic and Security Review Commission, *2018 Report to Congress* 29 (Nov. 2018).

[50] John S. McCain, National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, §1261(a) (2018).

B. A Critique of Weaponized National Security Review: The United States as an Example

1. An Overview of National Security and Foreign Direct Investment in the United States

The oversight of foreign investment in the United States has evolved over time, often in response to changing economic and security conditions.[51] In the early 1970s, increased investment in the United States by the Organization of the Petroleum Exporting Countries (OPEC), whose member states were flush with oil money, fostered growing concerns about the prospect of petrodollars flooding America and acquiring control of key American assets. At the time, many feared that, in light of the economically damaging oil embargo launched by OPEC in protest of the American support of the Israeli war effort, the spurt of investment was motivated by political rather than economic considerations.[52] Therefore, President Ford created the Committee on Foreign Investment (CFIUS) in 1975 to serve as a monitor of foreign investment and a coordinator of federal policy towards inbound capital flows.[53] Because CFIUS was established at a time when the United States was actively encouraging inbound foreign investment, it was fairly inactive in its infancy. For instance, between 1975 and 1980, CFIUS met only ten times and seemed unable to decide whether it should respond to the political or the economic aspects of foreign direct investment in the United States.[54] This led to complaints from Congress that CFIUS was falling short of its obligations. This tension between CFIUS taking a passive, investment-friendly approach to review and Congress advocating a more protectionist stance has been a consistent issue at every stage of CFIUS's existence.[55]

Throughout the 1980s, there was growing anxiety in the United States regarding foreign acquisition of U.S. corporations in sensitive industries by Japanese firms, including a bid by computer giant Fujitsu to purchase U.S.-based computer chipmaker Fairchild Semiconductor.[56] Opponents of the

---

[51] Jonathan Masters & James McBride, *Foreign Investment and U.S. National Security*, COUNCIL FOREIGN REL. (Aug. 28, 2018), https://www.cfr.org/backgrounder/foreign-investment-and-us-national-security.

[52] James K. Jackson, Cong. Rsch. Serv., RL33388, The Committee on Foreign Investment in the United States (CFIUS) 7 (2020).

[53] Isaac Lederman, *The Right Rights for the Right People: The Need for Judicial Protection of Foreign Investors*, 61 B.C. L. REV. 703, 707–09 (2020).

[54] Jackson, *supra* note 52, at 6.

[55] Patrick Griffin, *CFIUS in the Age of Chinese Investment*, 85 FORDHAM L. REV. 1757, 1762–63 (2017).

[56] EDWARD M. GRAHAM & DAVID M. MARCHICK, U.S. NAT'L SEC. & FOREIGN DIRECT INV. 41 (2006).

proposed acquisition argued that it would damage U.S. competitiveness and harm national security by giving Japan access to vital U.S. technology and making the United States dependent on Japan for semiconductor production.[57] Amid such concerns, Congress strengthened the CFIUS review process by passing the Exon-Florio amendment to the Defense Production Act of 1950 in 1988, which specified the basic review process of foreign investments.[58] The statute transformed CFIUS into a powerful review body with a broad mandate to advise the President on foreign investment transactions and to recommend that some transactions be suspended or blocked.[59] In 1990, President Bush ordered the China National Aero-Technology Import and Export Corporation (CATIC) to divest its acquisition of the American Corporation MAMCO, a producer of metal parts for civilian aircraft, because MAMCO was in possession of technology that was subject to export controls.[60]

Congress amended Exon-Florio and enacted the Byrd Amendment in 1993.[61] The Byrd Amendment imposed a mandatory forty-five-day investigation for transactions involving foreign government-controlled firms which "could affect" national security.[62] The Byrd Amendment later came under scrutiny as a result of the DP World transaction.[63] Dubai World, a corporation wholly owned by the government of Dubai, attempted in 2006 to purchase the Peninsular and Oriental Steam Navigation Company, a British firm with operations at six major American ports.[64] CFIUS declined to conduct a full forty-five-day investigation into the acquisition because the deal did not pose a national security threat and thus did not meet the second criterion of the Byrd Amendment.[65] However, Congress vociferously disagreed in light of widespread apprehension regarding the Middle East in the aftermath of the terrorist attacks on September 11, 2001.[66]

The CFIUS process was therefore amended again by the Foreign Investment and National Security Act of 2007 (FINSA).[67] FINSA made a number of major

[57] *Id.*

[58] Jackson, *supra* note 52, at 8.

[59] *Id.*

[60] Jim Mendenhall, *United States: Executive Authority to Divest Acquisitions Under the Exon-Florio Amendment - The MAMCO Divestiture*, 32 HARV. INT'L L.J. 286, 289–90 (1991).

[61] Jackson, *supra* note 52, at 9.

[62] *Id.*

[63] *Id.*

[64] *Id.*

[65] *Id.*

[66] Chris Lalonde, *Dubai or not Dubai? A Review of Foreign Investment and Acquisition Laws in the U.S. and Canada*, 41 VAND. J. TRANSNAT'L L. 1475, 1491–92 (2008).

[67] Jackson, *supra* note 52, at 10–11.

changes, including formalizing the CFIUS review system; expanding the legal meaning of "national security" to include critical infrastructure; expanding the composition of CFIUS membership; mandatory investigation of all foreign investment deals in which the foreign investor is owned or controlled by a foreign government; increasing the number of factors the President could consider in making his determination; and greater Congress oversight of CFIUS.[68] With the new mandate under FINSA, CFIUS has transformed from a relatively obscure executive branch committee to a major overseer of foreign entities that seek to acquire American assets.[69] Between 1988 and 2005, CFIUS conducted twenty-five investigations and saw foreign investors voluntarily shelve their plans thirteen times.[70] By comparison, in the seven-year period from 2008 to 2015 after FINSA was enacted, CFIUS carried out 333 investigations, with investors voluntarily withdrawing from 103 transactions.[71]

With the meteoric rise of China as an economic and military power, lawmakers and security officials have become increasingly concerned about the growth of Chinese investments in U.S. companies.[72] Of particular concern is the vulnerability of U.S. technology. Such concerns were clearly expressed by Senator John Cornyn in his testimony before the Senate Committee on Banking, Housing, and Urban Affairs in 2018:

> It's not just that China poses a threat, though, it's that *the kind of threat* is unlike anything the U.S. has ever before faced – a powerful economy with coercive, state-driven industrial policies that distort and undermine the free market, married up with an aggressive military modernization and the intent to dominate its own region and potentially beyond. To close the technology gap with the U.S. and leap-frog ahead of us, China uses both legal and illegal means. One of these tools is investment, which China has weaponized in order to vacuum up U.S. industrial capabilities from American companies that focus on dual-use technologies. China seeks to turn our own technology and know-how against us in an effort to erase our national security advantage.[73]

---

[68] *Id.*

[69] Paul Connell & Tian Huang, *An Empirical Analysis of CFIUS: Examining Foreign Investment Regulation in the United States*, 39 YALE J. INT'L L. 131, 163 (2014).

[70] Lederman, *supra* note 53, at 716.

[71] *Id.*

[72] Masters & McBride, supra note 51.

[73] David R. Hanke, Visiting Fellow, Nat'l Sec. Inst. at George Mason Univ. Antonin Scalia L. Sch., Testimony at Hearing on U.S.-China Relations in 2021: Emerging Risks before the U.S.-China Economic and

In response, Congress passed FIRRMA in 2018, which was widely considered to be the most sweeping overhaul of the CFIUS process in its entire history.[74] First, FIRRMA allows CFIUS to review a wider range of transactions, including any non-passive investment involving critical infrastructure, critical technology, and sensitive personal data.[75] Second, FIRRMA provides for a two-track method for reviewing investment transactions, with some transactions requiring a declaration to CFIUS and receiving an expedited process, while transactions involving investors from countries of special concern would require a written notification of a proposed transaction and would receive greater scrutiny.[76] FIRRMA also lengthens the review period and gives CFIUS greater leeway to suspend transactions.[77] Third, because FIRRMA's reforms substantially increased CFIUS's workload, CFIUS has been provided with additional resources.[78]

The current CFIUS review process is comprised of an informal step and three formal steps. The informal review, usually undertaken prior to filing a transaction with CFIUS, allows individual firms to discuss the transaction with the Committee privately. This gives firms the opportunity to correct any glaring issues with covered transactions and, if such issues cannot be resolved, the opportunity to abandon the deal without incurring negative publicity.[79] Three formal steps include a Declaration or written notice; a National Security Review; and a National Security Investigation.[80] Depending on the outcome of the reviews, CFIUS may forward a transaction to the President for his determination.[81] In some cases, FIRRMA increased the allowable time for reviews and investigations: (1) thirty days to review a declaration or written notification to determine if the transaction involves a foreign person in which a foreign government has a substantial financial interest; (2) a forty-five-day national security review; and (3) forty-five days for a national security

Security Review Commission (Sept. 8, 2021) (transcript available at https://www.uscc.gov/sites/default/files/2021-08/David_Hanke_Testimony.pdf).

74 Jackson, *supra* note 52, at 7.

75 Foreign Investment Risk Review Modernization Act, H.R. Res. 5841, 115th Cong. § 1703(a)(4) (2018) (enacted).

76 *Id.* § 1703(a)(4).

77 *Id.* § 1709.

78 E. Maddy Berg, *A Tale of Two Statutes: Using IEEPA's Accountability Safeguards to Inspire CFIUS Reform*, 118 COLUM. L. R. 1763, 1773–79 (2018).

79 Griffin, *supra* note 55, at 1767.

80 Foreign Investment Risk Review Modernization Act, *supra* note 75, § 1703(a)(4).

81 Id. § 1714.

investigation, with an option for a fifteen-day extension for "extraordinary circumstances," and a fifteen-day presidential determination.[82]

With enhanced screening and more aggressive jurisdiction assertions of CIFUS, there has been a marked increase in the scrutiny of transactions involving foreign investment in the United States.[83] Nevertheless, the data shows that most foreign investment filings to CFIUS were approved, and decisions to block foreign investments on national security grounds have been relatively rare.[84] In 2020, 187 written notices of transactions were filed with CFIUS. CFIUS conducted a subsequent investigation with respect to eighty-eight of those 187 notices.[85] Approximately eighty-nine percent of foreign investment transactions subject to full U.S. filings were cleared without conditions.[86] Another 8.55% of transactions received approval after adopting mitigation measures to resolve CFIUS' national security concerns.[87] The remaining 3.74% of transactions were either abandoned because the parties were unable to mitigate CFIUS's national security concerns (six cases) or formally prohibited by the President (one case).[88] The small number of cases which failed the CFIUS process is a testament to the overall open investment policy of the United States.[89]

On the other hand, CFIUS has heightened scrutiny over deals involving Chinese investors or third-country investors with significant connections to China.[90] Several high-profile Chinese investments were blocked by CFIUS. In several cases, CFIUS has unwound Chinese acquisitions of U.S. businesses

[82] Jackson, *supra* note 52, at 12–14.

[83] *Death by Delay: Greater Scrutiny of FDI Weighs on Inbound U.S. PE Buyouts*, BDO (June 2019), https://www.bdo.com/insights/industries/global/bdo-pitchbook-death-by-delay-greater-scrutiny-of-f.

[84] Harry G. Broadman, *Naivete about CFIUS' National Security Policy Towards Foreign Investment in the U.S.*, FORBES (Feb. 28, 2018), https://www.forbes.com/sites/harrybroadman/2018/02/28/naivete-about-cfius-national-security-policy-towards-foreign-investment-in-the-us/?sh=20865cce1af4.

[85] Committee on Foreign Investment in the United States, Annual Report to Congress, 2020 CFIUS Ann. Rep., at 15.

[86] *Id.*

[87] *Id.*

[88] *Id.* at 15–16.

[89] *Statement by President Joe Biden on the United States' Commitment to Open Investment*, WHITE HOUSE (June 8, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/08/statement-by-president-joe-biden-on-the-united-states-commitment-to-open-investment/.

[90] Blair Wang, *CFIUS Ramps up Oversight of China Deals in the U.S.*, THE DIPLOMAT (Sept. 14, 2021), https://thediplomat.com/2021/09/cfius-ramps-up-oversight-of-china-deals-in-the-us/.

several years following their completion.[91] For example, Ant Financial, a Chinese company owned by Alibaba Group Holding, announced that its proposed acquisition of MoneyGram, a U.S. financial service company, was blocked by CFIUS in 2018. In the following year, CFIUS required gaming company Beijing Kunlun Tech Co. Ltd. to divest its 100% ownership of Grindr, LLC, a dating app. Following the same trend, CFIUS ordered TikTok's owner, ByteDance Ltd., to divest its ownership of American assets in 2020 because of concerns that the app captures a large amount of information from users.[92] More recently, Chinese private equity firm Wise Road Capital and U.S.-based Magnachip Semiconductor Corp. after failing to receive approval from CFIUS.[93] It is also noted that formal presidential decisions to prohibit proposed foreign investments were made in seven cases up to date since the creation of CFIUS, and Chinese investors were directly involved in six of them.[94] In fact, CFIUS has become so hostile to Chinese investors that most now shy away from any investment in the United States that could be perceived as being related to national security.[95] This has resulted in a notable drop in Chinese investments requiring a CFIUS review, from an average of fifty-seven cases per year in the 2016-18 time period to twenty-eight in 2019 and twenty-two in 2020.[96]

---

[91] Jeanne Whalen, *TikTok was Just the Beginning: Trump Administration is Stepping up Scrutiny of Past Chinese Tech Investments*, WASH. POST (Sept. 29, 2020, 3:12 PM), https://www.washingtonpost.com/technology/2020/09/29/cfius-review-past-chinese-investment/.

[92] Chi Hung Kwan, *The China – US Trade War: Deep-Rooted Causes, Shifting Focus and Uncertain Prospects*, 15 ASIAN ECON. POL. REV. 55, 65 (2020).

[93] *U.S. Chipmaker Magnachip, China's Wise Road End $1.4 Billion Merger Deal*, REUTERS (Dec. 13, 2021), https://www.reuters.com/markets/europe/chinas-wise-road-capital-magnachip-call-off-14-billion-deal-2021-12-13/.

[94] The calculation is based on CFIUS annual reports to Congress from 2008 to 2021. U.S. DEP'T OF THE TREAS., CFIUS REPORTS AND TABLES (2021) [hereinafter CFIUS REPORTS], https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-reports-and-tables. Prior to 2008, there was only one case in 1990 when President Bush blocked the sale of an American aircraft manufacturing company to a Chinese SOE. *See* Helene Cooper, *Obama Orders Chinese Company to End Investment at Sites Near Drone Base*, N.Y. TIMES (Sept. 28, 2012), https://www.nytimes.com/2012/09/29/us/politics/chinese-company-ordered-to-give-up-stake-in-wind-farms-near-navy-base.html. The only exception was Singapore chipmaker Broadcom's attempted takeover of U.S. rival chipmaker Qualcomm, blocked by President Trump in 2018. *Id.*

[95] Martin Chorzempa, *Fewer Chinese Investments in the US are Raising National Security Concerns*, PIIE CHARTS (Aug. 18, 2020), https://www.piie.com/research/piie-charts/fewer-chinese-investments-us-are-raising-national-security-concerns.

[96] The calculation is based on CFIUS annual report to Congress from 2008 to 2021. CFIUS REPORTS, supra note 94.

2. *A Critique of U.S. National Security Review of Foreign Direct Investment*

a. The Expansive Concept of National Security

Whereas the concept of national security was once largely framed in terms of warfare, states have increasingly viewed national security in an expansive manner. Like other states, one key feature of U.S. national security screening of foreign investment is that the very concept of national security itself is left undefined.[97] It was purposefully left ambiguous, in theory giving regulators flexibility to deal with future and as yet unforeseen threats.[98] In lieu of defining national security, FINASA sets forth a non-exhaustive list of eleven factors that CIFUS may consider to determine if a proposed transaction threatens to impair U.S. national security, including the potential effects on "critical infrastructure", "critical technologies", and "the long-term projection of the US requirements for sources of energy and other critical resources and materials".[99] The FIRRMA further provides a "sense of Congress" concerning six additional factors that CFIUS should consider.[100] The listed factors have raised interpretation issues, including overly broad and vague elements such as "critical infrastructure" and "critical technology".[101] Further, it is not clear how these factors are assessed, which factors are more important and why, how to weigh and balance the relevant factors, and how to draw a conclusion if different factors point to different inferences.[102] As a result, CFIUS retains almost unlimited discretion to prohibit a proposed investment or requires a foreign investor to undertake onerous commitments to alleviate any national security concerns that CFIUS might have.[103]

The expansive concept of national security is a serious threat to international economic governance. If national security is conceptualized as a fusion of economic, ideological, and technological supremacy, how can one draw the line

---

[97] Cheng Bian, *Foreign Direct Investment Screening and National Security: Reducing Regulatory Hurdles to Investors Through Induced Reciprocity*, 22 J. WORLD INV. TRADE 561, 570 (2021).

[98] Deborah M. Mostaghel, *Dubai Ports World Under Exon-Florio: A Threat to National Security or a Tempest in a Seaport?*, 70 ALB. L. R. 583, 592–93 (2007).

[99] The Foreign Investment and National Security Act of 2007, Pub. L. No. 110-49, § 721(f), 121 Stat. 246, 253–54.

[100] McCain, supra note 50, § 1702 (c)(1)–(6).

[101] FIRRMA, supra note 5.

[102] Ming Du, *The Regulation of Chinese State-Owned Enterprises in National Foreign Investment Laws: A Comparative Analysis*, 5 GLOBAL J. COMP. L. 118, 137 (2016).

[103] *Id.*

between the protection of legitimate security concerns and impermissible protectionism?[104] Without proper oversight, in practice an expansive conceptualization of national security can eat the heart out of the old international economic world order.[105] It may move the norm from economically oriented efficiency and interdependence to security-oriented self-reliance and self-sufficiency.[106]

b. Unpredictable, Discriminatory, and Politicized National Security Review

The decision-making process in the U.S. national security reviews was frequently criticized as unpredictable, untransparent, discriminatory, politicized, and prone to abuse.[107] Firstly, national security reviews may be discriminatory. In *Ralls Corp. v. CFIUS*, a Chinese-owned company Ralls sought to acquire a wind-farm project near a U.S. Navy weapons systems training facility in north-central Oregon.[108] CFIUS issued orders mandating interim mitigation measures and President Obama followed up with an executive order formally blocking the deal.[109] However, the fact that dozens if not hundreds of other foreign-owned and foreign-made wind turbines also operated within the vicinity of the U.S. Navy installation was conveniently ignored.[110] The FIRMMA has further legalized the discriminatory practice by allowing CFIUS to discriminate among foreign investors in reviewing investment transactions by labeling some countries as "a country of special concern" — a country that "has a demonstrated or declared strategic goal of acquiring a type of critical technology or critical infrastructure that would affect United States leadership in areas related to national security".[111] Given that the FIRRMA's unique momentum stemmed from concerns about increasing Chinese investment in American businesses, Chinese investors are most likely targets of the discriminatory treatment. In fact, the FIRRMA requires the Secretary of Commerce to submit to Congress and

104 Joel Slawotsky, *The Fusion of Ideology, Technology and Economic Power: Implications of the Emerging New United States National Security Conceptualization*, 20 CHINESE J. INT'L L. 3, 60–61 (2021); Anthea Roberts et al., *Geoeconomics: The U.S. Strategy of Technological Protection and Economic Security*, LAWFARE (Dec. 11, 2018), https://www.lawfareblog.com/geoeconomics-us-strategy-technological-protection-and-economic-security.

105 *Id.*

106 Roberts, *supra* note 104.

107 Berg, *supra* note 78, at 1792–1800; Bian, supra note 97, at 584–85.

108 Ralls Corp. v. Comm. on Foreign Inv., 758 F.3d 296, 304 (D.C. Cir. 2014).

109 Id. at 305–06.

110 Id. at 305.

111 FIRRMA, *supra* note 5, § 1702(c)(1).

CFIUS a detailed report on foreign direct investment transactions made by Chinese investors in the United States every two years after the enactment of the FIRRMA until 2026.[112]

Secondly, secrecy marks a key feature of CFIUS. The CFIUS process shields the inner workings of its members from public knowledge and even from the foreign investors affected by the review.[113] Information submitted to CFIUS is confidential and with limited exceptions, not subject to information disclosure requirements.[114] The lack of transparency creates hidden barriers for foreign investors in practice.[115] Combined with CFIUS's broad power, the national security review process has become so unpredictable that some commentators called it a "lottery" for foreign investors.[116]

Thirdly, the CFIUS process is vulnerable to politicization.[117] As a profoundly contested political issue, national security review of high-profile M&A transactions can easily fall prey to congressional outcry, media sensationalism, and public hysteria.[118] The evidence shows that almost all major deals involving Chinese acquirers are subject to politicization by the media, members of Congress, the security community, domestic industry incumbents, and groups generally critical of China.[119] Consequently, rather than addressing real national security concerns, political interference based on political gamesmanship, emotion, and even xenophobia create huge uncertainties for Chinese investors.[120]

The botched attempt by China's fourth-largest steelmaker and state-owned Anshan Iron & Steel Group to acquire a minority stake in the U.S.-based Steel

---

112 *Id.* § 1719(b).

113 In *Ralls Corp.*, for example, the court found that U.S. Government did not provide Ralls with advance notice, access to the unclassified evidence supporting the decision, and an opportunity to rebut that evidence. *Ralls Corp.*, 758 F.3d at 319; Kevin Granville, *CFIUS, Powerful and Unseen, is a Gatekeeper on Major Deals*, N.Y. TIMES (Mar. 5, 2018), https://www.nytimes.com/2018/03/05/business/what-is-cfius.html.

114 FIRRMA, *supra* note 5, § 1713. On the other hand, assessing the proper standard of transparency in relation to national security review requires taking into account the sensitivity of the information at issue. *Id.*

115 Xing Xing Li, *National Security Review in Foreign Investments: A Comparative and Critical Assessment on China and U.S. Laws and Practices*, 13 BERKLEY BUS. L. R. 255, 272–73 (2015).

116 *Id.* at 272.

117 GRAHAM & MARCHICK, *supra* note 56, at 123.

118 DANIEL H. ROSEN & THILO HANEMANN, AN AMERICAN OPEN DOOR? MAXIMIZING THE BENEFITS OF CHINESE FOREIGN DIRECT INVESTMENT 62 (2011).

119 *Id.*

120 Yiheng Feng, *We Wouldn't Transfer Title to the Devil: Consequences of the Congressional Politicization of Foreign Direct Investment on National Security Grounds*, 42 N.Y.U. J. INT'L L. & POL. 253, 280–83 (2009).

Development Co. in July 2010 was a typical example.[121] Fifty members of the U.S. Congress representing the Congressional Steel Caucus urged CFIUS to scrutinize the proposed investment.[122] In its letter to Secretary Timothy Geithner, the Congressional Steel Caucus stated that the investment could give the Chinese "access to new steel production techniques and information regarding American national security infrastructure project".[123] Anshan announced that it had decided, given the opposition from members of Congress, to put its investment on hold, notwithstanding the absence of any decision by CFIUS.[124] However, it is impossible to see how Anshan's investment would create any national security concerns. To begin with, the "new steel production technologies" referred to in the letter were developed in Italy.[125] It is not proprietary to the United States and can be bought on the open market. [126] Moreover, Anshan would only take a fourteen percent minority equity in the joint venture.[127] Finally, the joint venture was expected to generate less than three tenths of one percent of total U.S. rebar production. A Forbes reporter called the national security concerns about Anshan's investment "idiocy" and "utter nonsense".[128]

Likewise, many observers were surprised by the CFIUS decision to block Ant Financial's proposed acquisition of MoneyGram.[129] Ant Financial had received CFIUS clearance in previous transactions and MoneyGram arguably did not deal with particularly sensitive information from a national security perspective.[130] Nor does MoneyGram operate in the defense sector or deal with

[121] Yu Hongyan & Ren Jie, *Ansteel Cements Steel Moves in US*, CHINADAILY (Sept. 16, 2010), https://www.chinadaily.com.cn/business/2010-09/16/content_11310945.htm.

[122] Mark Feldman, *China's Outbound Foreign Direct Investment: The U.S. Experience*, 13 INT'L J. PUB. POL. 304, 311 (2017).

[123] *Id.*

[124] *Id.* at 315.

[125] *US Steel Sector Falls out over Anshan-SDC Joint Venture*, FASTMARKETS (Dec. 29, 2010), https://www.metalbulletin.com/Article/2740763/REVISITED-US-steel-sector-falls-out-over-Anshan-SDC-jv.html.

[126] *Id.*

[127] *Id.*

[128] Stan Abrams, *The Curious Case of Anshan Steel and the Space-Age Rebar Technology*, FORBES (July 7, 2010), https://www.forbes.com/sites/china/2010/07/07/the-curious-case-of-anshan-steel-and-the-space-age-rebar-technology/?sh=396014a84305.

[129] Olga Torres, *CFIUS Review of Chinese Investment in the United States: The Good, the Bad, and the Ugly*, TORRES TRADE L. INSIGHTS (Sept. 22, 2020), https://www.torrestradelaw.com/posts/CFIUS-Review-of-Chinese-Investment-in-the-United-States%3A—The-Good%2C-the-Bad%2C-and-the-Ugly/218.

[130] *Id.*

critical infrastructure such as semiconductors.[131] Additionally, both MoneyGram and Ant Financial offered several amended proposals to help mitigate the concerns of CFIUS.[132] Ultimately, the proposed transaction was denied because of the close ties between Ant Financial and the Chinese government, and it was feared that the financial data held by MoneyGram could be used by the Government of China.[133]

Finally, to challenge a national security decision in the U.S. domestic courts is usually fruitless because judicial review on such decisions is limited.[134] In particular, a presidential decision to suspend or prohibit deals is not subject to judicial review.[135] In *Ralls Corp. v. CFIUS*, Ralls sued both the CFIUS order and the presidential veto.[136] The Court of Appeals for the D.C. Circuit confirmed that Ralls could not challenge the merits of the President's decision.[137] However, the Court held that the presidential veto deprived Ralls of constitutionally protected property interests without procedural due process because the government did not provide Ralls with advance notice, access to the unclassified evidence supporting the decision, and an opportunity to rebut that evidence.[138] The D.C. Circuit's decision represents a major change because before *Ralls Corp.*, the law provided no remedy whatsoever to investors injured by CFIUS or the President.[139]

Nevertheless, the thrust of the *Ralls Corp.* ruling proves to be of little use to prospective investors.[140] If anything, *Ralls Corp.* confirms that foreign investors face severe hurdles in challenging a CFIUS decision, much less a presidential blocking order.[141] To start with, as CFIUS screens foreign investment, it works with classified or privileged information.[142] It is not possible for CFIUS to share sensitive information with foreign entities that could pose a national security

131 Louise Lucas et al., *Data Take Central Stage as Ant Financial Fails in MoneyGram Bid*, FIN. TIMES (Jan. 3, 2018), https://www.ft.com/content/fd22dd9c-f06d-11e7-b220-857e26d1aca4.

132 Torres, *supra* note 129.

133 Ana Swanson & Paul Mozur, *MoneyGram and Ant Financial Call Off Merger, Citing Regulatory Concerns*, N.Y. TIMES (Jan. 2, 2018), https://www.nytimes.com/2018/01/02/business/moneygram-ant-financial-china-cfius.html.

134 *Ralls Corp.*, 758 F.3d at 308.

135 *Id.* at 311.

136 *Id.* at 308.

137 *Id.* at 311.

138 *Id.* at 319.

139 Lederman, *supra* note 53, at 720.

140 *Id.*

141 *Id.* at 719.

142 *Id.* at 720.

risk.[143] Furthermore, although foreign investors may challenge procedures of a CFIUS review, i.e., whether investors were afforded procedural due process, courts will not question the outcome of a CFIUS review.[144] Lastly, even if in the highly unlikely scenario that a court rules that CFIUS exceeded its authority in recommending the transaction be prohibited, once CFIUS refers the matter to the President, the presidential order blocking the deal is non-appealable.[145] In fact, *Ralls Corp.* remains the only foreign investor who has ever gone to court to challenge a CFIUS review.[146]

II. CHALLENGING NATIONAL SECURITY DECISIONS BEFORE INTERNATIONAL INVESTMENT TRIBUNALS

To respond to the allegedly unfair and arbitrary national security reviews, Chinese investors have resorted to a range of formal and informal mitigating and remedial measures.[147] Importantly, host states do not regulate foreign investment in a legal void. Chinese investors may contest national security decisions both in domestic courts of host countries as well as before international investment tribunals. To what extent national security decisions are subject to administrative or judicial review differs across countries, as does the extent of possible remedies.

Although many argue that national security decisions should be nonjusticiable,[148] most countries allow foreign investors to contest security-related decisions through either judicial appeal or administrative reconsideration, or both.[149] In practice, national security concerns are primarily relevant in connection with the establishment of new investments.[150] However, prospective foreign investors rarely use domestic judicial processes to challenge national security decisions made at the pre-establishment stage.[151] This is

143 Chang Liu, *Ralls v. CFIUS: The Long Time Coming Judicial Protection of Foreign Investors' Constitutional Rights against Government's National Security Review*, 15 J. INT'L BUS. & L. 361, 375 (2016).

144 *Ralls Corp.*, 758 F.3d at 311; Shannon Tiezzi, *Chinese Company Wins Court Case against Obama*, THE DIPLOMAT (July 17, 2014), https://thediplomat.com/2014/07/chinese-company-wins-court-case-against-obama/.

145 Jackson, supra note 52, at 23.

146 Liu, *supra* note 143.

147 Li, *supra* note 11, at 380–87.

148 Adam Tomkins, *National Security and the Role of the Court: A Changed Landscape?*, 126 L. Q. R. 543, 543–44 (2010).

149 Wehrlé & Pohl, *supra* note 24, at 40–42.

150 LUCIA RETTER ET AL., RELATIONSHIPS BETWEEN THE ECONOMY AND NATIONAL SECURITY: ANALYSIS AND CONSIDERATIONS FOR ECONOMIC SECURITY POLICY IN THE NETHERLANDS 39 (2020).

151 Wehrlé & Pohl, supra note 24, at 41.

because disagreements between the authorities and prospective foreign investors are mostly settled in the course of the national security review process itself.[152] "Insofar as authorities signal to investors that their investment is unlikely to meet with approval, investors face strong incentives to either submit a revised proposal aimed at accommodating the regulatory concerns or withdraw from the process."[153]

Nevertheless, national security review may also affect established investments. Compared to prospective investors, established investors are more likely to seek judicial remedy in domestic courts.[154] For example, Chinese investors TikTok and WeChat filed lawsuits challenging the legality of President Trump's executive order banning their use in the U.S. market.[155] Similarly, Huawei filed lawsuits challenging the ban on their products in the U.S. and Swedish courts.[156] Even if domestic courts have jurisdiction to review national security decisions, they frequently show considerable deference to the decisions of the relevant government agencies.[157] In particular, domestic courts normally do not determine the case upon its merits. Rather, courts may only review the procedural grounds leading to the national security decision and a victory for the plaintiff foreign investor will lead to a renewed review rather than a reversal of the previous decision.[158] *Ralls Corp.* discussed above was a typical example.

That said, domestic courts are still available to serve as a powerful check against executive actions. This is particularly the case outside the CFIUS context. TikTok's successful challenge of the national security decision in U.S.

---

[152] OECD, ACCOUNTABILITY FOR SECURITY-RELATED INVESTMENT POLICIES 6 (2008).

[153] *Id*.

[154] Szilárd Gáspár-Szilágyi, *Let Us Not Forget about the Role of Domestic Courts in Settling Investor-State Disputes*, 18 L. & PRAC. INT'L CTS. & TRIBUNALS 389, 403 (2020).

[155] Jeanne Whalen & Ellen Nakashima, *Biden Revokes TikTok and WeChat Bans, but Sets up a Security Review of Foreign-owned Apps*, WASH. POST (June 9, 2021), https://www.washingtonpost.com/technology/2021/06/09/tiktok-ban-revoked-biden/.

[156] Demetri Sevastopulo, *Huawei Challenges its Designation as a Threat to US Security*, FIN. TIMES (Feb. 9, 2021), https://www.ft.com/content/b7c2294d-9207-4fae-8fed-d63a80c99618; Finbarr Bermingham, *Huawei 5G Ban is Upheld by Swedish Court in Further Blow to Chinese Telecoms Giant's European Plans*, S. CHINA MORNING POST (June 23, 2021), https://www.scmp.com/news/china/article/3138369/huawei-5g-ban-upheld-swedish-court-further-blow-chinese-telecoms-giants.

[157] Craig Forcese, *Through a Glass Darkly: The Role and Review of National Security Concepts in Canadian Law*, 43 ALBERTA L. R. 963, 999 (2006); Dominic McGoldrick, *The Boundaries of Justiciability*, 59 INT'L & COMP. L.Q. 981, 1011–14 (2010).

[158] OECD - ACCOUNTABILITY, *supra* note 152, at 6.

courts is telling.[159] In August of 2020, President Trump issued Executive Order 13942, which relies on the International Emergency Economic Powers Act (IEEPA) and the National Emergencies Act, alleges that TikTok, the video-sharing app owned by the Chinese company ByteDance Ltd. (ByteDance), threatens to "allow the Chinese Communist Party access to Americans' personal and proprietary information–potentially allowing China to track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage."[160] To mitigate these risks, the President directed the Secretary of Commerce to identify and list prohibited transactions with ByteDance and its subsidiary TikTok, and ordered ByteDance to divest itself of TikTok's U.S. operations.[161] In response, TikTok filed a lawsuit alleging that the government's prohibitions violate the Administrative Procedure Act (APA), exceeded the President's and Commerce Secretary's authority under IEEPA, and were unconstitutional under the First and Fifth Amendments and the Takings Clause.[162] Siding with TikTok, Judge Nichols found the government's actions likely exceeded the scope of authority granted by IEEPA, and Commerce's failure to consider viable alternative mitigations likely violated the requirements of the APA. Accordingly, Judge Nichols issued a preliminary injunction barring the federal government from enforcing a ban.[163]

Where domestic remedies prove to be inadequate, foreign investors may also seek remedies through ISDS mechanisms embodied in IIAs, which may impose obligations on host states for the establishment, protection, promotion, and regulation of foreign investment.[164] Depending on the circumstances of each case, national security decisions may lead to a breach of the obligations of host states under BITs to accord foreign investors national treatment, most-favored-nation treatment (MFN), and fair and equitable treatment (FET) at the pre-

[159] Dave Perera, *TikTok Proves Elusive Target for Trump Administration as US Court Orders Another Halt on Prohibitions*, MLEX (Dec. 7, 2020), https://mlexmarketinsight.com/news/insight/tiktok-proves-elusive-target-for-trump-administration-as-us-court-orders-another-halt-on-prohibitions.

[160] Exec. Order No.13942, 85 Fed. Reg. 48, 637 (Aug. 6, 2020).

[161] *Id*.

[162] TikTok Inc. v. Trump, 490 F. Supp. 3d 73, 73 (D.D.C. 2020).

[163] *Id*. at 83, 86.

[164] Ioannis Glinavos, *Which Way Huawei? ISDS Options for Chinese Investors*, in HANDBOOK OF INTERNATIONAL INVESTMENT LAW AND POLICY 2451, 2468–71 (Julien Chaisse et al. eds., 2021); Lizzie Knight & Tania Voon, *The Evolution of National Security at the Interface between Domestic and International Investment Law and Policy: The Role of China*, 21 J. WORLD INV. & TRADE 104, 131 (2020).

establishment phase.[165] Moreover, if national security measures are taken at the post-establishment stage, they may contravene provisions in IIAs on expropriation, non-discrimination, FET, full protection and security, the freedom of capital transfers, and the umbrella clause.[166] For instance, in *Global Telecom Holding S.A.E. v. Canada*, the claimant alleged that Canada had breached the FET obligation in the Canada-Egypt BIT by subjecting it to an arbitrary, unreasonable, baseless, and nontransparent national security review.[167]

However, IIAs normally allow host states to adopt measures for the protection of certain public policy concerns, including "essential security interests."[168] The national security defense may either be listed as one of the nonconforming measures that a contracting party wishes to main or prescribed as an independent exception clause in IIAs. For example, Article 10.15 of the Regional Comprehensive Economic Partnership Agreement (RCEP), to which China is a signatory, provides:

> Nothing in the [investment] Chapter shall be construed to: … (b) preclude a Party from applying measures that it considers necessary for: (i) the fulfilment of its obligations with respect to the maintenance or restoration of international peace or security; or (ii) the protection of its own essential security interests.[169]

Unless otherwise prescribed in the relevant IIA, a successful invocation of the national security exception clause would exempt a host state from liability

---

[165] Mark McLaughlin, *State-owned Enterprises and Threats to National Security under Investment Treaties*, 19 CHINESE J. INT'L L. 283, 302–16 (2020). Whether there is a violation of the relevant BIT must be considered on the case-by-case basis. Some BITs do not apply to the pre-establishment phase of an investment. Moreover, even if a BIT grants establishment rights, the parties may still use a negative list or a positive list to exclude certain sectors or activities from the pre-establishment obligations. Under both circumstances, market entry restrictions based on national security grounds, including discriminatory treatment to foreign SOEs, do not violate the BIT. *See* Lu Wang, *Non-Discrimination Treatment of State-Owned Enterprises investors in International Investment Agreements?*, 31 ICSID REV. 45, 48–49 (2016).

[166] UNCTAD, THE PROTECTION OF NAT'L SECURITY IN IIAS 31 (2009).

[167] Glob. Telecom Holding S.A.E. v. Canada, ICSID Case No. ARB/16/16, Award, ¶¶ 573–82 (Mar. 27, 2020) [hereinafter Global Telecom Award].

[168] OECD, INTERNATIONAL INVESTMENT PERSPECTIVES: FREEDOM OF INVESTMENT IN A CHANGING WORLD 105 (2007). Most IIAs that include a security exception use the term "essential security interests" or "national security" to describe a situation where the exception may be invoked. Several tribunals considered that, by including the expression 'essential', the term 'essential security interests' is narrower than the more general term security interest. It may generally be understood to refer to those interests relating to the quintessential functions of the state, namely, the protection of its territory and its population from external threats, and maintenance of law and public order internally. *Id.*

[169] Regional Comprehensive Economic Partnership Agreement, art. 10.15 (emphasis added) [hereinafter RCEP].

for compensation.[170] In this section, I will first provide an overview of how national security clauses were interpreted by investment arbitral tribunals. Then I will inquire why, despite the fact that Chinese investors have complained about national security reviews, they have rarely challenged national security decisions through ISDS mechanisms provided in IIAs.

A. The National Security Exception before Investment Tribunals

International arbitral tribunals have dealt with complaints against national security decisions in a number of investment disputes.[171] There are several key trends in arbitral awards that can be identified in relation to national security clauses in IIAs.[172] First, the scope of "essential security interests" is flexible but not unlimited. In several ISDS cases brought against Government of Argentina by foreign investors concerning measures undertaken during the financial crisis in the 2000s, all arbitral tribunals concurred that a severe economic crisis could constitute an "essential security interest". However, tribunals disagreed on whether Argentina's economic crisis was severe enough to qualify as a national security issue. For the tribunals in the *CMS*, *Enron*, and *Sempra* cases, only an economic crisis imperiling a state's very existence and independence, such as a total economic and social collapse, would be of a sufficient scale to fulfil the requirement. They denied that such a dire situation existed in Argentina.[173] By contrast, the *LG&E* and the *Continental Casualty* tribunals agreed that the devastating economic, political, and social conditions in Argentina triggered the protections afforded under the national security exception clause.[174]

More recently, in *Devas v. India* and *Deutsche Telekom v. India*, a pair of investors claimed that India's annulment of a contract for a satellite telecommunications spectrum on national security grounds violated their treaty

[170] CMS Gas Transmission Co. v. Argentina, ICSID Case No. ARB/01/8, Annulment, ¶ 146 (Sept. 25, 2007) [hereinafter CMS Annulment]; LG & E v. Argentina, ICSID case no. ARB/02/1, Decision on Liability, ¶ 264 (Oct. 3, 2006) [hereinafter LG & E Award].

[171] At least sixteen national security-related investment cases have been examined by international arbitration tribunals. Most of these cases (ten) involved claims filed by foreign investors against Argentina. *See* UNCTAD, WORLD INVESTMENT REPORT 2016: INVESTOR NATIONALITY: POLICY CHALLENGES 97 (2017).

[172] PRABHASH RANJAN, ESSENTIAL SECURITY INTERESTS IN INTERNATIONAL INVESTMENT LAW: A TALE OF TWO ISDS CLAIMS AGAINST INDIA (Chaisse et al. eds., 2020).

[173] CMS Gas Transmission Co. v. Argentina, ICSID Case No. ARB/01/8, Award, ¶ 355 (May 12, 2005) [hereinafter CMS Award]; Sempra Energy Int'l v. Argentina, ICSID Case No ARB/02/16, Award, ¶ 348 (Sept. 28, 2007) [hereinafter Sempra Award]; Enron Corp. v. Argentina, ICSID Case No ARB/01/3, Award, ¶¶ 306–07 (May 22, 2007) [hereinafter Enron Award].

[174] LG & E Award, *supra* note 170, ¶ 237; Cont'l Cas. Co. v. Argentina, ICSID case no. ARB/03/9, Award, ¶ 180 (Sept. 5, 2008).

rights. The Indian government stated that the spectrum was reacquired for national needs, including the needs of defense, para-military forces, and other public utility services as well as for societal needs. Although the genuineness of India's national security claim was questioned,[175] both tribunals stated that they should grant a wide margin of deference to India in the determination of essential security interests.[176] As the tribunal in *Devas v. India* stated:

> An arbitral tribunal may not sit in judgment on national security matters as on any other factual dispute arising between an investor and a State. National security issues relate to the existential core of a State. An investor who wishes to challenge a State decision in that respect faces a heavy burden of proof, such as bad faith, absence of authority or application to measures that do not relate to essential security interests.[177]

Consequently, even if there was no imminent military or security threat, the Government of India's declaration that the satellite spectrum was reacquired for military or paramilitary use was sufficient for the tribunals to hold that the measure was directed at the protection of India's essential security interests.[178]

On the other hand, the scope of essential security interests is not unlimited. The tribunal in *Deutsche Telekom v. India* stressed that the term "essential security interests" cannot be "stretched beyond [its] natural meaning."[179] In both *Devas v. India* and *Deutsche Telekom v. India*, the tribunals made a clear differentiation between military needs and public or societal interests.[180] Although they showed significant deference to India's asserted military needs, both tribunals held that public utilities services and social needs for which the satellite spectrum was to be used—such as train tracking, emergency communication and disaster warnings, crop forecasting, rural communications,

---

[175] The tribunal in *Deutsche Telekom v. India* found that four years after the annulment of contract, Indian Government was still debating how to use the appropriated satellite spectrum. There was only possibility but no guarantee that the spectrum would be allocated for military use. *See* Deutsche Telekom AG v. India, PCA Case No. 2014-10, Interim Award, ¶¶ 286-287 (Perm. Ct. Arb. 2017) [hereinafter Deutsche Interim Award]; *see also* Devas v. India, PCA Case No. 2013-09, Award on Jurisdiction and Merit, ¶ 96 (Perm. Ct. Arb. 2016) (Haigh, Mr., dissenting) [hereinafter Devas Award on Jurisdiction and Award].

[176] Devas Award on Jurisdiction and Award, *supra* note 175, ¶ 245; Deutsche Interim Award, *supra* note 175, ¶ 235.

[177] Devas Award on Jurisdiction and Award, *supra* note 175, ¶ 245; Deutsche Interim Award, *supra* note 175, ¶ 235.

[178] Deutsche Interim Award, *supra* note 175, ¶ 281; Devas Award on Jurisdiction and Award, *supra* note 175, ¶ 335.

[179] Deutsche Interim Award, *supra* note 175, ¶ 236.

[180] *Id.* ¶ 281.

telemedicine, tele-education, did not constitute "essential security interests."[181] The effort to put some control on the nebulous concept of national security was also apparent in other international fora. For example, an ECHR decision refused to accept the contention that drug trafficking was a matter of national security.[182] More recently, Russia and India blocked a U.N. Security Council draft resolution that for the first time would have defined climate change as a security threat to world peace.[183]

Article XXI Security Exceptions of GATT 1994 has been incorporated into many IIAs.[184] In *Russia – Traffic in Transit*, a World Trade Organization (WTO) Panel ruled that it is generally left to every WTO Member to define what it considers to be its essential security interests because such a determination will depend on the particular situation and perceptions of the state in question, and can be expected to vary with changing circumstances.[185] However, the discretion of a WTO Member is limited by its obligation to interpret and apply the essential security interests exception in good faith.[186] For the Panel, the obligation of good faith requires that Members not use the security exception as a means to circumvent their WTO obligations.[187] The Panel concluded that the invoking Member should articulate the essential security interests it seeks to protect.[188] This obligation, for the panel, is "crystallized in demanding that the measures at issue meet *a minimum requirement of plausibility* in relation to the proffered essential security interests, i.e., that they are not implausible as measures protective of these interests."[189] On the surface, the investment tribunals' approach to interpret "essential security interests" is less deferential compared with that of the WTO panels. For instance, the tribunals in *Devas v. India* and *Deutsche Telekom v. India* seem to suggest that the line between security

[181] *Id*. ¶¶ 281–84; Devas Award on Jurisdiction and Award, *supra* note 175, ¶ 354.

[182] *C.G. and Others v. Bulgaria*, EUR. CT. H.R., Application No. 1365/07, Final Judgment, ¶ 43 (July 24, 2008).

[183] Rick Gladstone, *Russia Blocks U.N. Move to Treat Climate as Security Threat*, N.Y. TIMES (Dec. 13, 2021), https://www.nytimes.com/2021/12/13/world/americas/un-climate-change-russia.html.

[184] For instance, Article 16.3 of the China-Australia Free Trade Agreement (2015). Article XXI of GATT 1994 provides: "Nothing in this Agreement shall be construed …(b) to prevent any contracting party from taking any action which it considers necessary for the protection of its essential security interests…". The China–Australia Free Trade Agreement (ChAFTA), Austl.–China, Dec. 20, 2015, https://www.dfat.gov.au/sites/default/files/chafta-agreement-text.pdf.

[185] Panel Report, *Russia – Measures Concerning Traffic in Transit*, WT/DS512/R (Apr. 5, 2019), ¶ 7.131 [hereinafter *Russia – Traffic in Transit*].

[186] *Id.*

[187] *Id.*

[188] *Id*. ¶¶ 7.133–7.134.

[189] *Id*. ¶ 7.138 (emphasis added).

interests and public or societal interests can be clearly drawn. But it is at least disputable why some public or social needs, such as disaster response, cannot be considered as national security interests.[190]

To conclude, national security is not static but an evolving concept that may encompass not just military threats but also political and economic dimensions. Investment arbitral tribunals have jurisdiction to review host states' invocation of national security exception and they grant a wide margin of deference to host states with regard to the existence of an essential security interest. Nevertheless, such deference cannot be unlimited. The legitimacy of essential security interests claimed by host states should be determined case-by-case in each dispute.

Second, national security exception clauses in IIAs normally contain a nexus requirement such as "necessary" or "directed to."[191] The significance of the nexus requirement is in establishing the degree of connection between the adopted measure and the security objective that the measure seeks to achieve. A nexus requirement of "necessary" to protect security interest is stricter compared with "directed to."[192] Earlier investment arbitral tribunals conflated the "necessary" requirement in the security exception clause with the customary international law defense of necessity provided in Article 25 of the International Law Commission's Articles on the Responsibility of States for Internationally Wrongful Acts (ILC Articles), which requires that, for a measure to be "necessary," it must be the "only way" for the state to safeguard an essential interest against a grave and imminent peril.[193] More recently, however, arbitral tribunals clarified that the treaty defense of necessity is different from the customary international law defense of necessity.[194] To assess the necessity of the measures to protect a state's essential security interests, the tribunal in *Deutsche Telekom v India* laid down a two-prong test.[195] First, whether the measure was "principally targeted" to protect the essential security interests at stake.[196] Second, whether the measure was objectively required in order to

190 Heath, *supra* note 23, at 1045.

191 Deutsche Interim Award, supra note 175, ¶ 288.

192 *Id.*

193 CMS Award, *supra* note 173, ¶ 323; Sempra Award, *supra* note 173, ¶¶ 350–51; Enron Award, *supra* note 173, ¶¶ 309–310.

194 Deutsche Interim Award, *supra* note 175, ¶ 228; CMS Annulment, *supra* note 170, ¶ 129; Sempra v. Argentina, ICSID Case No. ARB/02/16, Annulment ¶ 198 (29 June 2010); LG & E v. Argentina, supra note 126, ¶ 245; Cont'l Cas. Co. v. Argentina, *supra* note 174, ¶ 167.

195 Deutsche Interim Award, supra note 175, ¶ 239.

196 *Id.*

achieve that protection, taking into account whether the state had reasonable alternatives that are less in conflict or more compliant with its international obligations.[197] The tribunal found that the Government of India's annulment of contract was not "necessary" because the two conditions were not met.[198]

Third, all investment arbitral tribunals held that, absent specific wording in the applicable BITs that grants complete discretion to a host state to decide how to protect its security interests, national security exception clauses are not self-judging.[199] The typical formulation of a self-judging security exception clause allows a host state to adopt such measures "which it considers" necessary for protecting essential security interests.[200] Under a self-judging clause, once it has been determined that the threat in question falls under the security exception as such, it is the exclusive prerogative of host country authorities to determine how to react to this threat.[201] However, a self-judging national security exception in IIAs does not provide a complete shield from judicial scrutiny as States remain subject to the general obligation to carry out their treaty commitments in good faith, as required by Article 26 of the Vienna Convention on the Law of Treaties.[202] This view is nevertheless contested as critics argued that there is no explicit textual warrant for a good faith view of security measures; that the good faith test in international law is ambiguous; and that investment tribunals may impose significant constraints on sovereign states to take security measures.[203]

Until now there has not been a specific case dealing with self-judging national security clauses in IIAs. Nevertheless, the WTO panel in *Russia-Transit Measures* held that the obligation of good faith applies not only to the respondent's articulation of its essential security interests, but also to the nexus

197 *Id.*

198 *Id.* ¶¶ 286–290. The tribunal found that the annulment of contract was not "principally targeted" at achieving the security objective because there was no clarity as regards the usage of the spectrum even years after the contract had been annulled. Moreover, reasonable, and least restrictive alternative measures were clearly available to India. *Id*.

199 CMS Award, *supra* note 173, ¶¶ 371–73; Devas Award on Jurisdiction and Award, *supra* note 175, ¶ 219.

200 UNCTAD, THE PROTECTION OF NATIONAL SECURITY IN IIAS 39 (2009).

201 *Id.*

202 William Burke-White & Andreas von Staden, *Investment Protection in Extraordinary Times: The Interpretation and Application of Non-precluded Measures in Bilateral Investment Treaties*, 48 VA. J. INT'L L. 307, 370 (2007); Robyn Briese & Stephan Schill, *If the State Considers: Self-Judging Clauses in International Dispute Settlement*, 13 MAX PLANCK Y.B. U.N. L. 61, 120 (2009).

203 Ji Ma, *International Investment and National Security Review*, 52 VAND. J. TRANSNAT'L L. 899, 933–37 (2021); Jose E. Alvarez & Kathryn Khamsi, *The Argentine Crisis and Foreign Investors: A Glimpse into the Heart of the Investment Regime*, *in* Y.B. INT'L INV. LAW & POLICY 379, 425–26 (Oxford Univ. Press, Karl P. Sauvant ed., 2009).

requirement.[204] As discussed above, this is an a highly deferential standard of review as it only requires a minimum requirement of plausibility in relation to the proffered essential security interests.[205] Specifically, a panel must determine "whether the measures are so remote from, or unrelated to, the … emergency that it is implausible that [the respondent state] implemented the measures for the protection of its essential security interests".[206] Following this legal standard, the Panel concluded in *Saudi Arabia–IPRs* that the non-application of criminal procedures and penalties to an intellectual property pirate company did not have any plausible relationship to Saudi Arabia's protection of its essential security interests.[207]

For non-self-judging national security exception clauses, arbitral tribunals are entitled to make their own assessment as to whether such a measure can be justified on national security grounds.[208] This includes an evaluation of whether there is a threat to national security, and whether the host state's measures are a necessary response to the threat.[209] Still, a non-self-judging security provision does not give arbitration tribunals the authority to completely ignore the assessment of the host state invoking the exception, nor to dictate which measures a host state should take.[210] As the tribunal in *Deutsche Telekom v India* explains:

> Whether a measure is 'necessary' … is subject to review by the Tribunal, as the clause is not self-judging. In that review, the Tribunal will undoubtedly recognize a margin of deference to the host state's determination of necessity, given the state's proximity to the situation, expertise and competence. Thus, the Tribunal would not review de novo the state's determination… On the other hand, the deference owed to the state cannot be unlimited, as otherwise unreasonable invocations of [the exception clause] would render the substantive protections contained in the treaty wholly nugatory.[211]

---

204 *Russia – Traffic in Transit*, *supra* note 185, ¶ 7.139.

205 *Id.*

206 *Id.*

207 Panel Report, *Saudi Arabia – Measures Concerning the Protection of Intellectual Property Rights*, WT/DS567/R (June 16, 2020), ¶ 7.293.

208 Deutsche Interim Award, *supra* note 175, ¶ 238.

209 *Id.*

210 *Id.*

211 *Id.*

B. Why didn't Chinese Investors Challenge National Security Decisions before Arbitral Tribunals?

Since its first BIT with Sweden in 1982, China has signed 145 BITs (107 in force) and twenty-four treaties with investment provisions (nineteen in force) by June 2022.[212] The new generation Chinese BITs include most of the standard investment protections, along with full advance consent to ISDS.[213] However, Huawei is the only Chinese investor to file an investment treaty claim against the national security decision of a host state up to date. A number of reasons may explain why few Chinese investors chose to challenge national security reviews before investment arbitral tribunals.

To begin with, empirical evidence shows that a large percentage of Chinese investors and their legal advisors know very little of how to protect their rights through ISDS.[214] Lack of knowledge begets skepticism about the efficacy of the institution,[215] which was only made worse by the legitimacy crisis of the ISDS system in recent years.[216] The deficiencies of the current ISDS system , such as lack of stability and predictability in arbitral awards, complex, slow and costly arbitral proceedings, no opportunity for appeal, and tribunals constituted mainly of lawyers who are not industry experts, are not helpful in boosting Chinese investors' confidence in investment arbitration as an effective remedy.[217]

Second, early Chinese BITs are limited in the scope of protection provided to foreign investors. For instance, they apply only to the period *after* an investment was made and they do not address the pre-establishment period of investment.[218] Therefore, a host State may engage in screening of proposed foreign investment without much concern about its treaty obligations. In addition, due to skepticism of international dispute resolution as only serving the interests of Western countries and being a capital-importing country with scarce

---

[212] Investment Policy Hub, UNCTAD, https://investmentpolicy.unctad.org/international-investment-agreements/countries/42/china.

[213] Li & Cheng, *supra* note 13, at 514–23.

[214] Li, *supra* note 11, at 399–400.

[215] *Id.* at 400.

[216] Daniel Behn et al., *Introduction: The Legitimacy Crisis and the Empirical Turn*, in THE LEGITIMACY OF INVESTMENT ARBITRATION: EMPIRICAL PERSPECTIVES 4 (Daniel Behn, Ole Kristian Fauchald and Malcolm Langford eds., 2022).

[217] *Id.* at 4–8.

[218] *E.g.*, China-Germany Bilateral Investment Treaty, arts. 2(1), 2(3), China-Ger., Jan 12, 2003, https://investmentpolicy.unctad.org/international-investment-agreements/treaty-files/736/download; Agreement on Encouragement and Reciprocal Protection of Investments, arts. 2, 3(2), China-Neth., Nov. 26, 2001, https://investmentpolicy.unctad.org/international-investment-agreements/treaty-files/763/download.

overseas foreign investment at the time, China took a conservative attitude towards ISDS until the late 1990s.[219] Early Chinese IIAs provide either no ISDS provisions at all or a narrowly constructed ISDS clause that only admits disputes "involving the amount of compensation resulting from expropriation" to arbitration.[220] Some tribunals, such as the tribunal in *China Heilongjiang International Economic & Technical Cooperative Corp. v. Mongolia*, adopted an extremely narrow construction of the ISDS provision that the only arbitrable matter was the amount of compensation for an expropriation. The tribunal therefore lacked jurisdiction with regard to whether an expropriation had actually occurred.[221] Even if a liberal interpretation is adopted, the scope of the ISDS clause remains narrow as the only arbitrable matter under the BIT would be expropriation and compensation.[222]

Third, national security decisions are often carved out as non-conforming measures, sheltered by self-judging national security exception clauses, or simply prescribed as non-justiciable in some Chinese BITs. For example, national security decisions taken under the auspices of the Investment Canada Act (ICA) are not subject to any dispute settlement provisions in the Canada-China BIT.[223] On August 9, 2021, the Canadian government ordered the telecom company China Mobile International (CMI), a wholly owned subsidiary of the central Chinese SOE China Mobile, to either divest itself entirely of or wind up

[219] Chi Manjiao & Wang Xi, *The Evolution of ISA Clauses in Chinese IIAs and its Practical Implications: The Admissibility of Disputes for Investor-State Arbitration*, 16 J. WORLD INV. & TRADE 869, 874 (2015).

[220] For example, Article 13.3 of the China-Singapore BIT (1985) and Article 11.2 of the China-Japan BIT (1988). Stephan W. Schill, *Tearing Down the Great Wall: The New Generation Investment Treaties of the People's Republic of China*, 15 CARDOZO J. INT'L & COMP. L. 73, 90–91 (2007).

[221] China Heilongjiang Int'l Econ. & Tech. Coop. Corp. et al. v. Mongolia, PCA Case No. 2010-20, Award, ¶¶ 435–54 (Perm. Ct. Arb. 2017). In contrast, the tribunals in *Tza Yap Shum v. Peru* and *Sanum v. Laos* adopted a different interpretation when faced with the same question. They found that a limitation of the ISDS clause solely over the amount of compensation for expropriation would deprive the clause of its *effect utile*. Tza Yap Shum v. The Republic of Peru, ICSID Case No. ARB/07/6, Award, ¶ 148 (July 7, 2011); Sanum Inv. Ltd. v. Lao People's Democratic Republic, PCA Case No. 2013-13, Award on Jurisdiction, ¶¶ 239–42 (Perm. Ct. Arb. 2013) (finding that a limitation of the ISDS clause solely over the amount of compensation for expropriation would deprive the clause of its *effect utile*).

[222] China Heilongjiang Int'l Econ. & Tech. Coop. Corp. et al. v. Mongolia, *supra* note 221, at 149–50, 154.

[223] Bilateral Investment Treaty, Annex D.34, Can.-China, Sept. 9, 2012 (providing: "A decision by Canada following a review under the *Investment Canada Act*, an Act respecting investment in Canada, with respect to whether or not to: (a) initially approve an investment that is subject to review; or (b) permit an investment that is subject to national security review; shall not be subject to the dispute settlement provisions under Article 15 and Part C of this Agreement.").

the Canadian business based on a national security review in pursuance of the ICA.[224] The national security concern of the CMI was stated as follows:

> As the Investor is a state-owned enterprise ultimately controlled by the Chinese state, this investment could result in the Canadian business being leveraged by the Investor's ultimate controller for non-commercial purposes, such as the compromise of critical infrastructure and foreign interference, to the detriment of Canada's national security.[225]

The CMI filed a legal challenge to the order before the federal court but lost the battle.[226] The CMI Canada thereafter ceased operations on January 5, 2022.[227] Because the decision was made under the ICA, it is not possible for the CMI to invoke the ISDS clause in the Canada-China BIT.

Likewise, in the China-Australia free trade agreement (ChAFTA), Australia reserves the right to adopt or maintain any measure when it considers necessary for the protection of essential security interests with respect to proposals by foreign persons and foreign government investors to invest in Australia.[228] Australia's treaty obligations with respect to market access, national treatment and MFN treatment do not apply to such decisions.[229] Moreover, the ChAFTA incorporates WTO Article XXI's national security exception.[230] The same is true with the new mega-regional free trade agreements that China has recently concluded, such as the Regional Comprehensive Economic Partnership Agreement (RCEP), or aspires to join, such as the Comprehensive and Progressive Trans-Pacific Partnership.[231] China signing up for the restrictive,

---

[224] Alexandra Posadzki & Steven Chase, *Ottawa Says China Mobile must Divest Telecom Business*, GLOBE & MAIL (Sept. 14, 2021), https://www.theglobeandmail.com/business/article-ottawa-says-china-mobile-must-divest-telecom-business/.

[225] China Mobile Commc'ns Group Co., Ltd et al & Can. Att'y Gen. et al., Application for Jud. Rev. under Section 18.1 of the Fed. Ct. Act (Can.), Ct. File No. T-1377-21 (Sept. 7, 2021), ¶ 27.

[226] Jim Bronskill, *Chinese Telecom Firm Loses Court Battle against Order to Divest Canadian Subsidiary*, NAT'L POST (Dec. 7, 2021), https://nationalpost.com/news/canada/chinese-controlled-firm-loses-court-bid-to-pause-ottawas-divestment-order.

[227] Shailaja Pai, *China Mobile Leaving Canada*, DEVELOPING TELECOMS (Dec. 29, 2021), https://developingtelecoms.c om/telecom-business/operator-news/12595-china-mobile-leaving-canada.html.

[228] *ChAFTA Fact Sheet: Investment and Investor State Dispute Settlement*, AUSTL. GOV'T DEP'T FOREIGN AFF. & TRADE, https://www.dfat.gov.au/sites/default/files/chafta-fact-sheet-investor-state-dispute-settlement.pdf (last updated 2018).

[229] Free Trade Agreement, China-Austl., Annex 3, § B, June 17, 2015 [hereinafter ChAFTA].

[230] *Id.* art. 16.3 (providing "Article XXI of GATT 1994 and Article XIV bis of GATS are incorporated into and made part of this Agreement, mutatis mutandis.").

[231] RCEP, *supra* note 169; Comprehensive & Progressive Agreement for Trans-Pacific Partnership art. 29.2, Dec. 30, 2018 [hereinafter CPTPP].

self-judging national security exception clause is also a reflection of China's own approach to national security review of inbound foreign investment.[232]

Finally, the Chinese culture also plays an important role in shaping Chinese investors' ambivalence about ISDS.[233] China's deeply rooted Confucian philosophy emphasizes harmony and conflict avoidance and sees that the optimal resolution of disputes should be achieved, not by the exercise of legal power, but by moral persuasion.[234] As a cultural predisposition, Chinese investors usually prefer informal and non-adversarial methods to resolve their disputes with host states.[235]

III. A CRITICAL ANALYSIS OF HUAWEI TECHNOLOGIES CO., LTD. V. KINGDOM OF SWEDEN

A. Huawei and National Security Concerns

Founded in 1987 by a former military engineer Ren Zhengfei, Huawei has transformed from a small trader selling phone switches in Shenzhen to the world's largest seller of smartphones and telecommunications equipment and a leader in 5G network infrastructure within a span of three decades.[236] With almost 200,000 employees and operations in more than 170 countries, Huawei boasts twenty-eight percent of the global market for telecom equipment.[237] In 2021, Huawei reported $99.9 billion in revenue, more than half of which were from its international market sales.[238] As the crown jewel of China's booming technology industry, Huawei is the national symbol of China's technological innovation and embodiment of China's dream of becoming a global technology

[232] Foreign Investment Law (promulgated by the Nat'l People's Cong., Jan 1, 2020, effective Mar. 15, 2019) art. 35 (China) (stipulating that the decision of security review shall be final, which means that the decision may not be administratively reconsidered or challenged in court in China).

[233] Danny McFadden, *The Growing Importance of Regional Mediation Centers in Asia*, in MEDIATION IN INTERNATIONAL COMMERCIAL AND INVESTMENT DISPUTES 160–81 (Catharine Titi & Katia F. Gómez eds., 2019).

[234] Melland Schill, *Cultural Element in International Law*, Lecture at Univ. of Manchester (May 5, 2016) (transcript available at the Univ. of Manchester Library).

[235] Wang Guiguo, *Chinese Mechanisms for Resolving Investor-State Disputes*, 1 JINDAL J. INT'L AFF. 204, 205, 209, 213, 222–23 (2011); Dae Un Hong & Ju Yoen Lee, *Why Are There So Few Investor-State Arbitrations in China? A Comparison with Other East Asian Economies*, 35 CHINA & WTO REV. 2018 42–44.

[236] YUN WEN, THE HUAWEI MODEL: THE RISE OF CHINA'S TECHNOLOGY GIANT 30, 32, 36–39, 48–49, 101–02, 130–32, 183 (2020).

[237] HUAWEI INVESTMENT & HOLDING CO., LTD. 2021 ANNUAL REPORT 48 (2022), https://www-file.huawei.com/minisite/media/annual_report/annual_report_2021_en.pdf?version=0401.

[238] Zhao Shiyue, *Huawei Remains Top Global Player in Telecom Equipment*, CHINA DAILY (Mar. 17, 2022), https://global.chinadaily.com.cn/a/202203/17/WS6232fe2fa310fd2b29e5192d.html.

leader.[239] Concomitant of its impressive success, Huawei is also the focus of scrutiny by Western governments which see its global expansion as a security threat.[240] In 2012, a report released by the House Permanent Select Committee on Intelligence concluded that using equipment made by Huawei and ZTE, another Chinese telecommunications company, could "undermine core U.S. national security interests."[241] In 2018, six U.S. intelligence chiefs, including the directors of the CIA and FBI, advised Americans not to use products or services from Huawei, warning that the company could maliciously modify or steal information and conduct undetected espionage.[242]

But precisely how does Huawei present national security concerns to the United States? Allegations were made about Huawei's cyber espionage, intellectual property theft, violations of international sanctions, complicated ownership structure, and the influence the Chinese Communist Party had over Huawei.[243] The main concern was that Huawei may be used by the Chinese Communist Party as an instrument for spying purposes.[244] All firms in China, "irrespective of their ostensibly private, commercial status, are subject to a deep and pervasive system of Party control."[245] It is impossible for a business enterprise to resist State- and Party-manipulable pressures and incentives in China. [246] Article 7 of China's National Intelligence Law further stipulates that "All organizations and citizens shall, in accordance with the law, support, cooperate with, and collaborate in state intelligence work, and guard the secrecy of state intelligence

239 WEN, *supra* note 175, at 52, 87, 89, 122, 131–32, 180.

240 Mike Rogers et al., Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE, 112th Cong., at 6, 7, 10 (2012).

241 HOUSE PERMANENT SELECT COMM. ON INTEL., INVESTIGATIVE REPORT ON THE U.S. NATIONAL SECURITY ISSUES POSED BY CHINESE TELECOMMUNICATIONS COMPANIES HUAWEI AND ZTE, 112th Sess., at 11–16, 21–44 (2012).

242 Sara Salinas, *Six Top US Intelligence Chiefs Caution Against Buying Huawei Phones*, CNBC (Feb. 13, 2018, 12:22 PM), https://www.cnbc.com/2018/02/13/chinas-hauwei-top-us-intelligence-chiefs-caution-americans-away.html.

243 HOUSE PERMANENT SELECT COMM. ON INTEL., *supra* note 241, at 2–3, 13–16, 22–24, 31–33.

244 Christopher A. Ford, Assistant Sec'y, Bureau of Int'l Sec. & Nonproliferation, Remarks at the Multilateral Action on Sensitive Technologies Conference: Huawei and Its Siblings, the Chinese Tech Giants: National Security and Foreign Policy Implications 4–6 (Sept. 11, 2019), https://2017-2021.state.gov/huawei-and-its-siblings-the-chinese-tech-giants-national-security-and-foreign-policy-implications/index.html.

245 Christopher A. Ford, *Huawei and its Siblings, the Chinese Tech Giants: National Security and Foreign Policy Implications*, U.S. DEP'T OF STATE (Sept. 11, 2019), https://2017-2021.state.gov/huawei-and-its-siblings-the-chinese-tech-giants-national-security-and-foreign-policy-implications/index.html.

246 Ford, supra note 244, at 7–8, 11.

work they are aware of."[247] Therefore, it is alleged that Huawei may be legally compelled to install "backdoors" or other vulnerabilities in the equipment it manufactures and supplies, which can be used for intelligence and data gathering, potentially giving Beijing the capability to shut down key digital networks in the event of war.[248] Other circumstantial evidence frequently advanced include Huawei has a close link with the Chinese military and China's state security apparatus. The linkage is often traced back to Zhengfei, who worked as a soldier and then an officer in the People's Liberation Army Engineering Corps between 1974 and 1983, as well as Huawei's involvement in defense-related research and development.[249] Huawei's murky ownership structure, easy access to financing, and high levels of government subsidies are not helpful in assuaging the concerns either.[250]

At the heart of national security concerns is 5G, the next generation of cellular networks, which will provide faster download speeds for smartphones, connect devices in smart cities, and support autonomous vehicles and robots.[251] As 5G networks will be the most critical infrastructure in societies that we have ever seen, the consequences of potential sabotage and espionage also increase significantly.[252] To complicate matters, certain technical aspects in 5G technology make it more vulnerable to be misused for espionage and sabotage than previous generations of mobile telecoms networks.[253] For example, the complex technical nature of the 5G systems makes investigating of electronic equipment at the time of

[247] William Evanina, Director, NCSC, Keynote Address at the International Legal Technology Association (June 4, 2019).

[248] Yongjin Zhang, *"Barbarising" China in American Trade War Discourse: The Assault on Huawei*, 42 THIRD WORLD Q. 1436 (Mar. 22, 2021), https://www.tandfonline.com/doi/abs/10.1080/01436597.2021.1894120?journalCode=ctwq20.

[249] Robert Mendick, *Huawei Staff CVs Reveal Alleged Links to Chinese Intelligence Agencies*, THE TELEGRAPH (July 5, 2019), https://www.telegraph.co.uk/news/2019/07/05/huawei-staff-cvs-reveal-alleged-links-chinese-intelligence-agencies/.

[250] Christopher Balding & Donald C. Clarke, *Who Owns Huawei*? SSRN (Apr. 17, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3372669; Chuin-Wei Yap, *State Support Helped Fuel Huawei's Global Rise*, WALL ST. J. (Dec. 25, 2019), https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736.

[251] *What is 5G and What Will It Mean for You?*, BBC NEWS (Jan. 28, 2020), https://www.bbc.co.uk/news/business-44871448.

[252] Tom Wheeler & David Simpson, *Why 5G Requires New Approaches to Cybersecurity: Racing to Protect the Most Important Network of the 21st Century*, BROOKINGS (Sept. 3, 2019), https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/.

[253] Karsten Friis & Olav Lysne, *Huawei, 5G and Security: Technological Limitations and Political Responses*, 52 DEV. & CHANGE 1174, 1179 (Oct. 3, 2021).

purchase futile.[254] Stopping malicious functionality from entering through software updates appears to be impossible, and one should be careful not to assume that exploitation of undesired functionality in the 5G equipment will always be detected.[255]

Given the alleged national security threat, U.S. Congress and the executive branch have initiated a swift and brutal strike to limit Huawei's access to international supply chains, telecommunications systems, and markets.[256] In May 2019, the U.S. Department of Commerce placed Huawei and 68 of its affiliates to the Entity List, to which U.S. companies may not sell components without government approval. On the same day, President Trump issued an executive order declaring a national emergency due to the threat of foreign adversaries exploiting vulnerabilities in U.S. information and communications technology and services, clearly aimed at China and Huawei. Subsequently, major U.S. technology companies, such as Google, Broadcom, Intel, Qualcomm and Xilinx, announced that they would no longer supply equipment or services to Huawei.[257] In August 2020, the Department of Commerce expanded its restrictions to limit Huawei's use of chips made using American software and equipment, and also added thirty-eight Huawei affiliates to its Entity List.[258] In December 2020, the Federal Communications Commission upheld the order designating Huawei as posing a national security threat to the safety of communications networks and banned the use of support from the Commission's Universal Service Fund—$8.3 billion a year—to purchase equipment or services from Huawei.[259] In other legal actions, the U.S. has pursued criminal charges against Huawei and its Chief Financial Officer for stealing U.S. technology, conspiracy, wire fraud, bank fraud, racketeering, and helping Iran to evade sanctions, amongst other charges.[260]

---

254 *Id.* at 1184.

255 *Id.* at 1182–84.

256 STEPHEN P. MULLIGAN & CHRIS D. LINEBAUGH, CONG. RSCH. SERV., R46693, HUAWEI AND U.S. LAW (2021).

257 Nadeem Badshah & Lily Kuo, *Google Blocks Huawei Access to Android Updates after Blacklisting*, THE GUARDIAN (May 20, 2019), https://www.theguardian.com/technology/2019/may/19/google-huawei-trump-blacklist-report.

258 Press Release, Michael R. Pompeo, Sec'y of State, The United States Further Restricts Huawei Access to U.S. Technology (Aug. 17, 2020), https://2017-2021.state.gov/the-united-states-further-restricts-huawei-access-to-u-s-technology/index.html.

259 Press Release, Fed. Commc'ns Comm'n, FCC Affirms Designation of Huawei as National Security Threat (Dec. 10, 2020), https://www.fcc.gov/document/fcc-affirms-designation-huawei-national-security-threat.

260 David McCabe et al., *U.S. Charges Huawei with Racketeering, Adding Pressure on China*, N.Y. TIMES (July 14, 2020), https://www.nytimes.com/2020/02/13/technology/huawei-racketeering-wire-fraud.html.

Moreover, the U.S. has been pressuring its allies to follow suit, even threatening to stop sharing intelligence with them if Huawei equipment is used in their telecommunication system, as part of a larger crackdown on Huawei.[261] Bowing to U.S. pressure, the United Kingdom announced that it would ban Huawei equipment from the UK's 5G telecoms infrastructure beginning in 2021, reversing its previous stance only six months earlier that Huawei would be banned from the core of its telecoms network, although its hardware would be allowed in up to thirty five percent of peripheral parts of the network.[262] Other countries such as Australia, Japan, Romania, and Canada followed.[263] More countries, including India, Germany, the Netherlands, and New Zealand, are considering bans of Huawei equipment.[264] Experts warned that tensions between the United States and China over technology could lead to a "digital iron curtain", which would compel foreign governments to decide between doing business with the U.S. or China.[265]

As a technical matter, there is no public evidence that Huawei equipment presents a national security threat.[266] Nor is there evidence to indicate that Huawei is in any way under the orders of the Chinese government, or that Beijing has any plans to dictate business plans and strategy at Huawei—particularly when it comes to spying.[267] There are doubts that Washington has shared much evidence in private with its allies. According to the media reports, a "dossier" on Huawei presented by a delegation of senior U.S. officials to their counterparts in the United Kingdom in January 2020 contained "no smoking

[261] Stu Woo & Kate O'Keeffe, *Washington Asks Allies to Drop Huawei*, WALL ST. J. (Nov. 23, 2018), https://www.wsj.com/articles/washington-asks-allies-to-drop-huawei-1542965105.

[262] Billy Perrigo, *Bowing to U.S. Pressure, U.K. Bans 5G Equipment from China's Huawei over Security Concerns*, TIME (July 14, 2020), https://time.com/5866643/uk-huawei-5g-ban/.

[263] Annabelle Liang, *Canada to Ban China's Huawei and ZTE from its 5G Networks*, BBC NEWS (May 20, 2022), https://www.bbc.co.uk/news/business-61517729; Radu Marinas, *Romanian President Signs Bill into Law to Ban Huawei from 5G*, REUTERS (June 11, 2021), https://www.reuters.com/business/media-telecom/romanian-president-signs-bill-into-law-ban-huawei-5g-2021-06-11/.

[264] Reality Check Team, *Huawei: Which Countries are Blocking its 5G Technology*, BBC NEWS (May 18, 2019), https://www.bbc.co.uk/news/world-48309132.

[265] Simon Duke, *A Digital Iron Curtain is Descending as China and America Tussle over Huawei*, THE TIMES (May 28, 2020), https://www.thetimes.co.uk/article/a-digital-iron-curtain-is-descending-as-china-and-america-tussle-over-huawei-gktcxw6l0.

[266] *Huawei is at the Centre of Political Controversy*, THE ECONOMIST (Apr. 27, 2019), https://www.economist.com/briefing/2019/04/27/huawei-is-at-the-centre-of-political-controversy; Lindsay Maizland & Andrew Chatzky, *Huawei: China's Controversial Tech Giant*, COUNCIL FOREIGN RELATIONS (Aug. 6, 2020), https://www.cfr.org/backgrounder/huawei-chinas-controversial-tech-giant.

[267] Karishma Vaswani, *Huawei: The Story of a Controversial Company*, BBC NEWS (Mar. 6, 2019), https://www.bbc.co.uk/news/resources/idt-sh/Huawei.

gun" incriminating Huawei.[268] Huawei has long protested that actions by western governments against it are hiding the desire to address the competitive disadvantages of its western competitors. As the most audited and inspected company in the tech industry, Huawei contends that it has never had a major cyber security incident, nor has anyone ever produced evidence of any security problems with Huawei equipment.[269]

B. Why did Huawei Bring ISDS Proceedings against Sweden?

On April 17, 2020, the Swedish Post and Telecom Agency (PTS) invited all major Mobile Network Operators (MNOs) on the Swedish market to an auction in the Swedish 5G network. In the press release PTS issued for the bidding invitation, it highlighted that, since the 5G development is an important part of Sweden's digitalization, great focus will be put on ensuring that the use of 5G network does not cause harm to Swedish national security. On October 20, 2020, PTS issued a decision authorizing four MNOs to participate in the auction with the mandatory requirement that all future licensees awarded through the auction are prohibited from using any equipment or services from Huawei for new installation and implementation of central functions of 5G networks. In addition, where existing infrastructure for central functions will be used for the provision of 5G services, Huawei equipment and services are to be phased out by no later than January 1, 2025.[270] Huawei had attempted to challenge the PTS Decision before the Administrative Court of Stockholm but ultimately failed in June 2021. Huawei is currently appealing the Swedish court decision to uphold a ban on its 5G equipment before the European Court of Justice.[271]

As explained above, Chinese investors are generally reluctant to challenge national security decisions of host states. However, several unique features of Huawei's investment in Sweden may explain why Huawei has chosen to formally challenge the Government of Sweden's national security decision before the ICSID. First, the China-Sweden BIT, originally signed in 1982 and

[268] Gordon Corera, *Huawei: 'No Smoking Gun' in US's 5G Dossier*, BBC NEWS (Jan. 14, 2020), https://www.bbc.com/news/technology-51112232.

[269] *Is Safety the Real Reason to Ban Huawei*, HUAWEI (Feb. 14, 2019), https://huawei.eu/story/safety-real-reason-ban-huawei.

[270] E-mail from Zhao Minglu, Legal Representative of Huawei Technologies Co., Ltd., to Stefan Löfven, Prime Minister of Sweden (Dec. 31, 2020) [hereinafter Huawei's Written Notification] (available at https://www.italaw.com/sites/default/files/case-documents/italaw170044.pdf).

[271] Laurens Cerulus, *Huawei Seeks EU Court Involvement in Swedish Ban*, POLITICO (Oct. 6, 2021), https://www.politico.eu/article/huawei-sweden-china-5g-court-case-european-union/.

then amended in 2004, does not contain a national security exception clause.[272] Back in 2019, Huawei warned the Czech Republic of potential international arbitration in relation to assertions by the Czech cybersecurity agency that Huawei's technologies and equipment pose a national security threat.[273] Similar to the China-Sweden BIT, there is no national security exception clause in the China-Czech BIT.[274] Some argued that the absence of a national security exception clause would give an arbitral tribunal much more leeway to assess the genuineness and necessity of Sweden's national security claim.[275] However, the absence of an explicit national security exception clause does not necessarily mean that a host state is precluded from invoking it as a defense for national security review, a point which will be discussed in detail in part IV.C below.

Second, Huawei would suffer heavy financial loss and other adverse effects due to the national security decision of the Swedish government. Huawei is an established investor with significant investments in Sweden, employing more than 600 people and Huawei Sweden generated revenues of approximately SEK 5 billion (about $530 million USD) in 2019. Because of the national security decision, Huawei claims that its immediate revenue loss is estimated at SEK 5.2 billion for the 2021 to 2025 period alone. As the national security decision refers to a period of twenty-five years, the total estimated revenue losses would be substantially larger. [276] Clearly, sunk costs and lost prospective profits would be high if Huawei were banned from lucrative 5G business or even forced to divest. The potential for substantial financial remedy through ISDS would make Huawei's legal challenge appealing.

Finally, since formal domestic litigation and administrative appeals have proven to be a dead end, to challenge the Swedish ban before an international investment arbitral tribunal is the last resort for Huawei. Considering that more

[272] Agreement on Mutual Protection of Investments between the Government of the Kingdom of Sweden and the Government of the People's Republic of China, China-Swed., Mar. 29, 1982, 1350 U.N.T.S. 22733 (amended Sept. 27, 2004).

[273] Marc Santora, *Huawei Threatens Lawsuit Against Czech Republic After Security Warning*, N.Y. TIMES (Feb. 8, 2019), https://www.nytimes.com/2019/02/08/business/huawei-lawsuit-czech-republic.html.

[274] Agreement between the Czech Republic and the People's Republic of China on the Promotion and Protection of Investments, China-Czech, Dec. 8, 2005 (agreement does not have a security exception clause).

[275] Jarrod Hepburn & Luke Eric Peterson, *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?*, INV. ARB. REP. (Feb. 19, 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/.

[276] Huawei's Written Notification, *supra* note 270.

countries are currently weighing the option of excluding Huawei equipment from their 5G network, Huawei's resort to ISDS may also have a deterrent effect because the move will force host countries to evaluate potentially draconic legal liability arising from the breach of IIAs.

If this analytical approach is correct, it is highly likely that Huawei may consider initiating an ISDS against Canada as well for its decision to ban Huawei from supplying technology and equipment to build Canada's 5G wireless networks, depending on the outcome of *Huawei v. Sweden*.[277] First, Huawei appears to have significant investments in Canada. It ranked 18th among Canada's Top one hundred corporate research and development spenders in 2020, reaching $261.6 million in Fiscal 2019.[278] The ban will have a hugely negative impact on Huawei's investment in Canada.[279] Second, different from the CMI order discussed earlier, any ban on the use of Huawei equipment in 5G networks will not be made under the ICA since Huawei first came to Canada more than a decade ago and its investment was approved under the ICA. Consequently, if Huawei chose to challenge the ban, the dispute would not be excluded from the ISDS clause in the Canada-China BIT.[280] Lastly, the Canada-China BIT does not contain a broad national security exception. Article 33(5) allows a contracting party to take any actions that it considers necessary for the protection of its essential security interests but goes on to define those interests narrowly in military terms, citing traffic in arms, nuclear weapons, and war or other emergency in international relations.[281] It is unlikely that banning Huawei equipment from the 5G networks is designed to address an "emergency in international relations". Thus, Canada does not seem to have an explicit foothold for mounting a broad essential security interest defense.

C. The Prospect of Huawei v. Sweden

Huawei argued that Sweden's measures leading to and including the PTS decision, which were adopted without any transparency and have unlawfully targeted and discriminated Huawei, directly violate Sweden's international

[277] Janyce McGregor, *Banning Huawei from Canada's 5G Networks Could be Costly for Taxpayers*, CBC (Feb. 17, 2019), https://www.cbc.ca/news/politics/huawei-canada-china-fipa-1.5021033.

[278] *Huawei Canada Ranks 18th Overall in Corporate R&D Spending in Canada*, HUAWEI (Jan. 15, 2021), https://www.huawei.com/ca/news/ca-en/huawei-canada-ranks-18th-overall-in-corporate-spending-in-canada.

[279] Nic Fildes, *Huawei's UK Revenue and Profit Shrink After 5G Ban*, FIN. TIMES (June 13, 2021), https://www.ft.com/content/cb58f6bb-b12f-405d-9c10-20b6aa06765f.

[280] Agreement Between the Government of Canada and the Government of the People's Republic of China for the Promotion and Reciprocal Protection of Investments, Can.-China, 2012, at Annex D.34.

[281] *Id*. art. 33.5.

obligations under the China-Sweden BIT, in particular the FET (Article 2(1)); MFN treatment (Article 2(2)); and not to expropriate, nationalize or take any other measure having a similar effect with respect to an investment made by Chinese investors (Article 3).[282] As mentioned above, the China-Sweden BIT does not contain a national security exception clause. Therefore, it is not possible for Sweden to rely on national security exception clause and the arbitral tribunal will have full power to assess the legality of Sweden's national security claim under the China-Sweden BIT.

As a legal strategy, Sweden is likely to put on two defenses. First, Sweden will argue that its decision to ban Huawei equipment from 5G network does not violate FET, MFN or otherwise constitutes an expropriation. In other words, Sweden could seek to avoid responsibility through arguments related to interpretation and application of investment protection obligations themselves. Second, it is also possible for Sweden to argue that any wrongfulness of the decision could be precluded because it is the only way for Sweden to safeguard an essential interest against a grave and imminent peril. This necessity defense is permitted in customary international law embodied in Article 25 of the ILC Articles, even if the China-Sweden BIT does not contain a national security exception clause.[283] It will be to the great advantage of Sweden if it could persuade the arbitral tribunal that the exclusion of Huawei equipment from its 5G network did not violate any substantive treaty obligations because it is widely acknowledged that the elements of the necessity defense in Article 25 of the ILC Articles are extraordinarily difficult to satisfy in the realm of foreign investment law.[284]

Granted, there is only limited public information about security risks of Huawei equipment and much of this information is not verified. This is of course unsurprising because it is standard practice to keep information relating to national security confidential. Moreover, it would be cautious to take the media comments with a pinch of salt. For example, it has been said that there was "no smoking gun" in the dossier on Huawei prepared by the U.S. government to share with its allies.[285] But there are no details about how the media reached its

[282] Huawei's Written Notification, *supra* note 270.

[283] *See* EDF International SA & Others v. Argentina, ICSID Case No. ARB/03/23, Decision on Annulment, ¶ 319 (Feb. 5, 2016).

[284] Andrea K. Bjorklund, *Emergency Exception to International Obligations in the Realm of Foreign Investment: The State of Necessity and Force Majeure as Circumstances Excluding Wrongfulness*, in OXFORD HANDBOOK OF INT'L. INV. LAW 460, 520–21 (Peter Muchlinski et al. eds., 2008).

[285] Gordon Corera, *Huawei: 'No Smoking Gun' in US's 5G Dossier*, BBC NEWS (Jan. 14, 2020), https://www.bbc.com/news/technology-51112232.

conclusion, and other reports point to a different conclusion.[286] Therefore, the analysis below is primarily aimed at providing an analytical framework, rather than speculating the outcome of the dispute. When more facts emerge from *Huawei v. Sweden*, we will be in a better position to perform the latter task.

1. Does the Huawei Ban Violate Substantive Treaty Obligations in China-Sweden BIT?

The relevant legal standards of FET, MFN, and expropriation in international investment law are extensively discussed in the arbitral awards and academic literature.[287] For the purpose of this Article, it is sufficient to say that any analysis of whether substantive treaty obligations in China-Sweden BIT were breached must focus on two issues. First, is the *purpose* of the Swedish decision to exclude Huawei equipment from 5G network the protection of national security? Second, is the Swedish decision justifiable, i.e., reasonable, non-discriminatory, and proportional for the purpose of preventing national security risks? If the Swedish decision was for the purpose of national security and the decision was justifiable, then it would not violate FET, MFN, or constitute expropriation. Specifically, if the two conditions were met, the ban would not constitute expropriation but a legitimate non-compensable government regulation, falling within police powers of Sweden;[288] the ban would not violate FET because it was not arbitrary or discriminatory;[289] and the ban would not violate MFN because different treatment in like circumstances may be justified by pursuing the legitimate public interest of national security.[290]

---

[286] *See* HUAWEI CYBER SECURITY EVALUATION CENTRE OVERSIGHT BOARD ANNUAL REPORT ¶¶ 6.8–6.9 (2020) [hereinafter HCSEC ANNUAL REPORT 2020], https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/923309/Huawei_Cyber_Security_Evaluation_Centre__HCSEC__Oversight_Board-_annual_report_2020.pdf.

[287] *Accord* Rudolf Dolzer, *Fair and Equitable Treatment: Today's Contours*, 12 SANTA CLARA J. INT'L L. 7–33 (2014); Stephen Vasciannie, *The Fair and Equitable Treatment Standard in International Investment Law and Practice*, 70 BRITISH Y. B. INT'L L, 99–164 (2000); Ying Zhu, *Do Clarified Indirect Expropriation Clauses in International Investment Treaties Preserve Environmental Regulatory Space*, 60 HARV. INT'L L.J. 377, 377–416 (2019); Caroline Henckles, *Indirect Expropriation and the Right to Regulate: Revisiting Proportionality Analysis and the Standard of Review in Investor-State Arbitration*, 15 J. INT'L ECON. L. 223, 230–37 (2012).

[288] *See* Tecnicas Medioambientales Tecmed S.A. v. The United Mexican States (*Tecmed v. Mexico*), ICSID Case No. ARB(AF)/00/2, Award, ¶ 96 (May 29, 2003); *see also* OECD, *"Indirect Expropriation" and the "Right to Regulate" in International Investment Law* 16–19 (Working Paper on International Investment 2004/04).

[289] CMS Award, *supra* note 173, ¶ 290; Jacob Stone, *Arbitrariness, the Fair and Equitable Treatment Standard, and the International Law of Investment*, 25 LEIDEN J. INT'L L. 77, 77–107 (2012).

[290] Todd J. Grierson-Weiler & Ian A. Laird, *Standards of Treatment*, in THE OXFORD HANDBOOK OF INT'L. INV. LAW 261, 291 (Peter Muchlinski, Federico Ortino & Christoph Schreuerp eds, 2012); Pope & Talbot v. Canada, Award on the Merits of Phase 2 (Apr. 10, 2001) [hereinafter Pope & Talbot Award], at 9–37.

For the first question, this article argues that the tribunal is likely to accept Sweden's argument that the decision to exclude Huawei equipment from its 5G network was taken to protect national security unless Sweden cannot produce any plausible evidence that Huawei 5G equipment presents a national security risk. Given the ubiquitous high-speed connectivity of 5G and its potential to transform military capabilities as well as the fact that 5G networks will be integrated into future military operations,[291] there is little doubt that a threat to the security of 5G networks constitutes a national security risk. Moreover, a clear trend emerging from the case law is that arbitral tribunals usually grant a wide margin of deference to the host country in determining the existence of a national security risk precisely because national security issues relate to the existential core of a state. Such deference cannot be unlimited, but it proves to be very difficult for a foreign investor to challenge the assessment of a host country. The tribunal in *Devas v. India* stated that an investor who wishes to challenge a State's national security decision faces a heavy burden of proof, such as "bad faith, absence of authority or application to measures that do not relate to essential security interests".[292] The tribunal in *Deutsche Telekom v. India* stated that the Government of India's declaration that the satellite spectrum was reacquired for military or paramilitary use was sufficient for the tribunal to hold that the measure was directed at the protection of India's essential security interests, even though the tribunal openly expressed serious doubt of the genuineness of India's national security claim.[293] The tribunal in *Global Telecom Holding S.A.E v. Canada* did not even assess the genuineness or rationality of Canada's security concerns and considered only how the national security review process was conducted.[294]

Finally, to allay fears that Huawei equipment might pose a security risk to the UK's networks, Huawei entered into an agreement with the British government to allow extensive security reviews of Huawei's hardware and software in November 2010.[295] The Huawei Cyber Security Evaluation Centre (HCSEC) is controlled by an oversight board that reports to the UK's National

[291] Steven Walker et al., *Why the World's Militaries are Embracing 5G*, IEEE SPECTRUM (Nov. 11, 2021), https://spectrum.ieee.org/lockheed-martin-5g.

[292] Devas Award on Jurisdiction and Award, *supra* note 175, ¶ 245; Deutsche Interim Award, *supra* note 131, ¶ 235.

[293] Deutsche Interim Award, *supra* note 175, ¶¶ 281–87.

[294] Global Telecom Award, *supra* note 167, ¶ 607.

[295] HUAWEI CYBER SECURITY EVALUATION CENTRE OVERSIGHT BOARD ANNUAL REPORT ¶¶ 2.3 (2021), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1004291/2021_HCSEC_OB_REPORT_FINAL__1_.pdf

Cyber Security Centre.[296] Over the years of operation of the HCSEC, British inspectors have never found a backdoor.[297] However, the oversight board has consistently identified "significant, concerning issues" in Huawei's approach to software development that require ongoing management and mitigation.[298] In other words, the potential national security risk of Huawei equipment cannot be completely overruled even if mitigation measures were undertaken.

The second question is whether the Swedish ban on Huawei equipment is rational, non-discriminatory, and proportional for the purpose of safeguarding national security. First, the Swedish authority singled out and banned Huawei equipment but permitted Huawei's business competitors to supply a similar product for its 5G networks. Apparently, the Swedish decision affords Huawei a differential and less favorable treatment compared to other investors in the same business sector. Nevertheless, whether the differential treatment violates the MFN treatment embodied in Article 2(2) of the China-Sweden BIT depends on whether the differential treatment is unreasonable or lacking proportionality to achieve an otherwise legitimate objective of the state.[299] If, for example, Huawei presents a higher national security risk to Sweden than Huawei's competitors such as Samsung, then a differential treatment may be justified. Similarly, if the Swedish decision is reasonable and proportional, it will not be inconsistent with the FET obligation or constitute indirect expropriation.[300]

The burden of proof falls on the Swedish government to explain why the difference in treatment between Huawei and its competitors is justified.[301] It was reported that the Swedish ban was based on national security concerns raised by Sweden's security services and armed forces.[302] However, the detailed analysis of why Huawei was afforded a differential treatment was not disclosed. Since Sweden is not the only country that banned Huawei equipment from 5G network, it would be useful to review why other countries, such as the U.S. and

296 HCSEC ANNUAL REPORT 2020, *supra* note 286, ¶¶ 1.2–1.3.

297 *Huawei is at the Centre of Political Controversy*, *supra* note 266.

298 HCSEC ANNUAL REPORT 2020, *supra* note 286, ¶¶ 6.8–6.9.

299 *See* Parkerings-Compagniet v. Republic of Lithuania, ICSID Arbitration Case No. ARB/05/8, Award, ¶ 368 (Sept. 11, 2007); *see also* Grierson-Weiler & Laird, *supra* note 290, at 291; Julian Arato et al., *The Once and Future Law of Non-Discrimination*, 112 Proceedings of the American Society of International Law Annual Meeting 61, 62–65 (2018).

300 *See* OECD - *Indirect Expropriation*, *supra* note 288, 16–19; *see also* Stone, *supra* note 222, at 77–107 (discusses if the Swedish decision is reasonable and proportional).

301 *See* Pope & Talbot Award, *supra* note 290, at 35–36.

302 Johan Ahlander & Supantha Mukherjee, *Swedish Court Upholds Ban on Huawei Selling 5G Network Gear*, REUTERS (June 22, 2021), https://www.reuters.com/technology/swedish-court-upholds-ban-huawei-selling-5g-network-gear-2021-06-22/.

UK, treated Huawei differently from other ICT vendors. It is highly likely that Sweden will use the same reasons as other countries to justify its decision.

In the UK, Huawei has always been considered as posing a higher national security risk by the UK government and it is designated as a high-risk vendor by the National Cyber Security Centre (NCSC), the UK's lead technical authority on cyber security. The reasons why the NCSC continues to consider Huawei a high-risk vendor include at least that:[303]

- Huawei has a significant market share in the UK already, which gives it a strategic significance;
- Huawei could, under China's National Intelligence Law of 2017, be ordered to act in a way that is harmful to the UK;
- the NCSC assesses that the Chinese State (and associated actors) have carried out and will continue to carry out cyber attacks against the UK and the UK interests;
- Huawei's cyber security and engineering quality is low and its processes opaque. For example, the HCSEC Oversight Board raised significant concerns about Huawei's engineering processes.
- A large number of Huawei entities have been included on the US Entity List. Those restrictions keep tightening in a way that is likely to have an impact on future availability and reliability of Huawei's products.

Similarly, the U.S. government has accused Huawei of potential cyber espionage, intellectual property theft, violations of international sanctions, complicated ownership structure, relationship with the Chinese intelligence agencies and the Chinese military and being influenced by the Chinese Communist Party.[304]

Huawei has vigorously denied many of the allegations, and the denials are not without merits.[305] For example, Huawei's attorneys have issued a legal opinion before the Federal Communications Commission arguing that Huawei is not obligated to cooperate with any request by the Chinese government to use their systems or access them for malicious purposes under the guise of state

303 *NCSC Advice on the Use of Equipment from High Risk Vendors in UK Telecoms Networks*, NAT'L CYBER SEC. CENTRE [hereinafter NCSC], https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks (last updated July 14, 2020).

304 HOUSE PERMANENT SELECT COMM. ON INTEL., *supra* note 241, at 11–34; Ford, *supra* note 244.

305 *See* Zhang, *supra* note 248, at 1446–49.

security, nor is the Chinese government authorized to order Huawei to hack into products they make to spy on or disable communications.[306] China's ministry of foreign affairs has officially clarified that no law in China requires any company to install mandatory back doors[307] Zhengfei has publicly asserted that Huawei has never spied for the Chinese government and never would.[308] Huawei has also tried to explain that it is controlled by its employees through a trade union, not the Chinese government.[309] Moreover, there is no hard evidence that Huawei's equipment is inherently riskier than its competitors' equipment.[310]

The central question is: how would the arbitral tribunal approach competing claims of the rationality of the Swedish decision? As the tribunal in *Deutsche Telekom v India* states, the tribunal will recognize a margin of deference to the host state's determination, given the state's proximity to the situation, expertise, and competence. Thus, the tribunal would not review *de novo* the state's determination.[311] It is unlikely for the tribunal to ask a State to show that the existence of a national security risk was unanimously accepted, which will often be an almost impossible task to meet, especially in areas of scientific uncertainty or new technology. Instead, the tribunal will focus on whether the reasons provided by Sweden are reasonable or rational, for instance, supported by at least some respectable security experts.[312] Given that there is strong voice from highly qualified technical experts questioning the security of Huawei equipment in the 5G network[313], it is possible for the tribunal to refrain from second guessing a sovereign state's good faith regulatory choice.

---

306 Jihong Chen & Jianwei Fang, *Declaration before the Federal Communications Commission* (May 27, 2018), https://thechinacollection.org/wp-content/uploads/2019/03/Huawei-Declaration.pdf. But Huawei's legal opinion is disputed in particular because the law has never been tested. *See* Yuan Yang, *Is Huawei Compelled by Chinese Law to Help with Espionage*, FIN. TIMES (Mar. 5, 2019).

307 *Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on July 13, 2020*, MINISTRY OF FOREIGN AFFS. PEOPLE'S REPUBLIC CHINA (July 13, 2020), https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/202007/t20200713_693288.html.

308 Dan Strumpf & Josh Chin, *Huawei's Mysterious Founder Denies Spying for China, Praises Trump*, WALL ST. J. (Jan. 15, 2019, 12:00 PM), https://www.ft.com/content/282f8ca0-3be6-11e9-b72b-2c7f526ca5d0.

309 Yuan Yang, *Huawei Says Employees Control Company through 'Virtual Shares'*, FIN. TIMES (Apr. 25, 2019), https://www.ft.com/content/22fdb0ea-6742-11e9-a79d-04f350474d62.

310 *See* Colin Lecher & Russell Brandom, *Is Huawei a Security Threat? Seven Experts Weigh in*, THE VERGE (Mar. 17, 2019, 2:00 PM), https://www.theverge.com/2019/3/17/18264283/huawei-security-threat-experts-china-spying-5g.

311 *See* Deutsche Interim Award, *supra* note 175, ¶ 238.

312 *See* Nigel Blackaby & Alex Wilbraham, *Practical Issues Relating to the Use of Expert Evidence in Investment Treaty Arbitration*, 31 ICSID REV. 655, 661–63 (2016).

313 NCSC, *supra* note 303; *see also* Lecher & Brandom, *supra* note 310.

It would also be challenging for Huawei to argue that the Swedish ban is not proportional to the risks presented by Huawei 5G kit. One important feature of the Swedish decision is that it is *not* a complete exclusion of Huawei equipment. It only prohibited Huawei equipment from central functions of 5G network.[314] The Swedish decision is a reminder of the United Kingdom's initial decision that Huawei would be banned from the core of its telecoms network, although Huawei equipment would be allowed in up to thirty-five percent of peripheral parts of the network. The United Kingdom's network operators and intelligence officials believed that it was possible to design a system architecture in which the sensitive parts of the network known as its "core" are protected from interference.[315] Related, Huawei has long complained that host countries did not consider the steps that Huawei had taken to guard against state interference and exploitation of its technology and equipment.[316]

However, many contended that as 5G evolves, the current distinction between core/central and non-core/peripheral parts will be lost as more and more sensitive operations are carried out closer to users.[317] The 2012 report released by the House Permanent Select Committee on Intelligence concluded that it is virtually impossible to find and eliminate every significant vulnerability given the complexity of the information and telecommunications system, in particular, when flaws were intentionally inserted by a determined and clever insider.[318] In the same vein, due to areas of concern exposed through the proper functioning of the mitigation strategy and associated oversight mechanisms, the oversight board of the HCSEC in the United Kingdom has consistently concluded since 2018 that it can provide only limited assurance that the long-term security risks can be managed in the Huawei equipment currently deployed in the United Kingdom.[319] Based on this assessment, the United States and Australia claim it will no longer be possible to keep Huawei, and by extension the Chinese state, out of the network's most sensitive areas.[320] Given that the Swedish decision is arguably even more generous than the initial UK decision, as it did not specify the percentage of peripheral parts of the network that Huawei may

[314] Huawei's Written Notification, *supra* note 270.

[315] Perrigo, *supra* note 262.

[316] Hepburn & Peterson, *supra* note 275.

[317] Wheeler & Simpson, *supra* note 252.

[318] The Permanent Select Committee on Intelligence, *supra* note 304, at 4–7.

[319] HCSEC ANNUAL REPORT 2020, *supra* note 286, ¶ 6.8.

[320] Leo Kelion, *Huawei Set for Limited Role in UK 5G Networks*, BBC NEWS (Jan. 28, 2020), https://www.bbc.co.uk/news/technology-51283059.

provide, it is possible that the Swedish decision could pass a proportionality assessment.

In summary, considering the available public information about Huawei and the whole body of arbitral awards, it is likely that the arbitral tribunal will substantially defer to Sweden's national security decision and find that the Swedish decision on Huawei may not violate FET, MFN, or otherwise constitute indirect expropriation. Still, more facts relating to the security of Huawei equipment and the circumstances relating to the Swedish ban are needed to reach a conclusion.

2. The Necessity Defense

Alternatively, Sweden can invoke the customary international law doctrine of necessity to defend its decision. Article 25 of the ILC Articles, which reflects customary international law on the point, provides:

> 1. Necessity may not be invoked by a State as a ground for precluding the wrongfulness of an act not in conformity with an international obligation of that State unless the act: (a) is the only way for the State to safeguard an essential interest against a grave and imminent peril; and (b) does not seriously impair an essential interest of the State or States towards which the obligation exists, or of the international community as a whole.
>
> 2. In any case, necessity may not be invoked by a State as a ground for precluding wrongfulness if: (a) the international obligation in question excludes the possibility of invoking necessity; or (b) the State has contributed to the situation of necessity.[321]

In order to invoke the necessity defense, Sweden has to demonstrate that all the requirements prescribed above are met. As there is no evidence that Sweden has contributed to the situation of necessity, or that the international obligation in the China-Sweden BIT excludes the possibility of invoking necessity, or that Sweden's invocation of the necessity defense would seriously impair an essential interest of China or of the international community as a whole, the analysis below will focus on two issues. First, was the Swedish ban imposed for the purpose of safeguarding "an essential interest" against "a grave and imminent peril"? Second, was the ban "the only way" for Sweden to "safeguard" the "essential interest"?

[321] International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, art. 25, 2001, Supplement No. 10 (A/56/10).

For the first question, it is highly likely that the arbitral tribunal will hold that the security of 5G network is "an essential interest." In *LG & E Energy v. Argentina,* the tribunal noted that necessity under customary international law is triggered whenever the State is threatened by a serious danger to the possibility of maintaining its essential services in operation.[322] In *AWG Group v. Argentina* and *Impregilo v. Argentina*, the tribunals considered the provision of water distribution and waste water treatment services was vital to the health and well-being of nearly ten million people and was therefore "an essential interest" of the Argentine State.[323]

The requirement that the essential interest be threatened by a "grave and imminent peril" is seldom discussed separately in the arbitral awards.[324] In *Enron v. Argentina*, the tribunal took the view that the Argentine financial crisis was not a "grave and imminent peril" because there was no convincing evidence that the events were "out of control or had become unmanageable."[325] By comparison, in the *Gabcikovo-Nagymaros* case, the International Court of Justice outlined a less stringent standard. It ruled that for a peril to be "imminent," it must not be a mere possibility; instead, it must be duly established, certain and inevitable. This is not to say that the peril must have already manifested itself. A State is perfectly entitled to take measures in response to the peril from the moment that it becomes certain, even though the realization of that peril may be far off.[326] Given that there is no smoking-gun evidence that Huawei has previously rigged its equipment at the behest of the Chinese government, it would be challenging for Sweden to argue that the national security risk posed by Huawei is "certain and inevitable," even less "out of control or had become unmanageable."

To justify its decision due to the doctrine of necessity, Sweden must also show that the decision it took was "the only way" for it to protect the essential interest against the peril posed by Huawei. In *CMS v. Argentina*, the tribunal concluded that as long as Argentina had other options available to it, even if they may be costly or less convenient, the "only way" requirement would not be

322 LG & E Energy Corp., LG & E Cap. Corp. & LG & E Int'l, Inc. v. Argentine Republic, ICSID Case No. ARB/02/1, Decision on Liability, ¶ 246 (Oct. 3, 2006).

323 AWG Group Ltd. v. Argentine Republic, ICSID Case No. ARB/03/19, Decision on Liability, ¶ 260 (July 30, 2010); *see also* Impregilo S.p.A. v. Argentine Republic, ICSID Case No. ARB/07/17, Award ¶ 346 (June 21, 2011).

324 Dimitrios Katsikis, *Necessity Due to Covid-19 as a Defense to International Investment Claims*, 36 ICSID REV. 46, 55 (2021).

325 Enron Award, *supra* note 173, ¶ 307.

326 Gabcikovo-Nagymaros Project (Hungary/Slovakia), Judgment, 1997 I.C.J. Rep. 42 ¶ 54 (Sept. 25).

met.[327] Other tribunals in the *Sempra* and *Enron* arbitrations adopted a similar approach.[328] This is a highly stringent standard as theoretically there are always alternatives that could be adopted to protect the essential interest at stake. For example, Huawei has offered to sign no-spy agreements with governments of host countries to commit to making Huawei equipment meet the no-spy, no-backdoors standard.[329] In addition, Huawei has put a lot of effort into demonstrating transparency in its systems and is open to investigations of its 5G equipment. In 2018, it announced the opening of an information security lab in Germany where operators and regulators could review the source code that went into Huawei equipment.[330] A similar center of HCSEC has already been operational in the United Kingdom since 2010. Hypothetically, there are other possible ways for the Swedish government to enhance surveillance of 5G security without banning Huawei equipment out of central functions.

The problem with the current approach of most tribunals is that the question of whether the measure taken by the State is the "only way" cannot be asked in the abstract. On almost every occasion there will be other options, other courses of action that a State could have conceivably taken. The real question that must be asked is whether the "essential interest" could be adequately protected by other alternatives.[331] Tribunals in *Urbaser SA et al. v. Argentina* and *AWG Group v. Argentina* seem to support this view.[332] If this approach was taken, Sweden may argue that excluding Huawei equipment from central functions of 5G network is the "only way" to ensure national security as alternatives may fail to achieve its objective. It is unclear whether this argument may be accepted by the arbitral tribunal.

In practice, very rarely could a State satisfy the cumulative requirements of necessity doctrine in customary international law.[333] Arbitral tribunals seem to have adopted an extremely intrusive standard of review in scrutinizing the

[327] CMS Award, *supra* note 173, ¶¶ 323–24.

[328] Sempra Award, *supra* note 173, ¶¶ 350–351; *see also* Enron Award, *supra* note 173, ¶ ¶ 309–10.

[329] Owen Churchill & Nectar Gan, *Huawei Will Commit to No-spy Agreements to Win Government Contracts, Chairman Says Amid US Pressure on Allies Over 5G Fears*, S. CHINA MORNING POST (May 15, 2019, 2:23 AM), https://www.scmp.com/news/world/europe/article/3010230/huawei-will-commit-no-spy-agreements-win-government-contracts.

[330] Huawei, *Huawei Opens Security Innovation Lab in Bonn*, FIN. TIMES (Nov. 16, 2018), https://sciencebusiness.net/network-news/huawei-opens-security-innovation-lab-bonn.

[331] Katsikis, *supra* note 324, at 61.

[332] Urbaser SA et al. v. Argentine Republic, ICSID Case No. ARB/07/26, Award, ¶ 716 (Dec. 8, 2016); *see also* AWG Group Ltd. v. Argentine Republic, *supra* note 323, ¶ 235.

[333] C. L. LIM, JEAN HO & MARTINS PAPARINSKIS, INTERNATIONAL INVESTMENT LAW & ARBITRATION: COMMENTARY, AWARDS AND OTHER MATERIALS 485–86 (2nd ed. 2021).

necessity of measures at issue. It would be a challenge for Sweden to rely on the necessity defense in customary international law to justify the exclusion of Huawei equipment from its 5G network.

CONCLUSION

The rise of Chinese investors as active global players presents to host countries a vexing policy dilemma. The positive economic and political ramifications of foreign direct investment are widely accepted. But due to their strong political ties with the Chinese government and concentration in strategic and sensitive sectors, Chinese investors are perceived as raising some unique national security challenges to host states. Huawei is a case in point.

To be sure, the heated political debate on how to handle alleged national security concerns about Huawei is not merely a technical issue. It should be seen in the broader context of American securitization of China in general.[334] At its core, what Huawei presents is a political and a geopolitical challenge. As FBI Director Chris Wray testified before the Senate Intelligence Committee in 2018:

> We're deeply concerned about the risks of allowing any company or entity that is beholden to foreign governments that don't share our values to gain positions of power inside our telecommunications networks.[335]

But a weaponized national security regime not only damages foreign investors' perception of the investment environment in a host country, but also runs the risk of breaching a host country's investment treaty obligations if a national security decision was not made on genuine national security concerns but under the influence of misinformed populism, protectionism, and xenophobia.[336] This concern leads us to enquiry whether modern international investment norms are resilient enough to balance the competing interests of safeguarding genuine national security concerns and preventing the abuse of national security exception as a pretext for protectionism or even a tool of great power rivalry. It is submitted that Huawei's request for arbitration against Sweden is a testing ground and the outcome of the case will have a lasting effect

[334] Andrew Stephen Campion, *From CNOOC to Huawei: Securitization, the China Threat, and Critical Infrastructure*, 28 ASIAN J. POL. SCI. 47, 56–59 (2020).

[335] Salinas, *supra* note 179.

[336] *See* Maira Goes de Moraes Gavioli, *National Security or Xenophobia: The Impact of the Foreign Investment and National Security Act in Foreign Investment in the U.S.*, 2 WM. MITCHELL L. RAZA J. 1, 42–43 (2011).

on shaping the contours of international investment law in the age of geoeconomics.