Catholic University Law Review

Volume 71
Issue 3 *Summer 2022*

Article 10

6-20-2022

Paving a New (Hua)Wei: A Comparative Analysis of International Approaches to Securing Information and Communication Technology Supply Chains

Jordan Villegas
Catholic University of America (Student), villegasj@cua.edu

PAVING A NEW (HUA)WEI: A COMPARATIVE ANALYSIS OF INTERNATIONAL APPROACHES TO SECURING INFORMATION AND COMMUNICATION TECHNOLOGY SUPPLY CHAINS

Jordan Villegas[+]

Recent amendments to Chinese Intelligence Laws codify affirmative obligations upon domestic companies and citizens alike, namely, that they must assist and support the Chinese Communist Party (CCP) in its intelligence gathering efforts. Coupling these laws with the international prevalence of Huawei, a Chinese telecommunications company comprising two-thirds of 5G equipment outside China, CCP compromised 5G equipment is an unassailable reality. This article explores five intelligence allied nations and how each has respectively addressed the risk posed by Huawei. It argues each nation's policies are deducible to three primary approaches, categorically including: (1) promulgation of law explicitly excluding Huawei 5G equipment; (2) promulgation of law generically improving supply chain risks without any explicit exclusion of Huawei 5G equipment; and (3) no promulgation nor undertaken efforts to address 5G supply chain risks. Various external and domestic factors, including political climates, economic dependencies, and intragovernmental agreement, heavily influence a nation's supply chain risk mitigation efforts. Irrespective of a nation's approach to supply chain risk mitigation, this paper deduces that government action, in and of itself, is insufficient to effectively combat Huawei; it is either incapable of regulating private industries' purchases or, if it is capable, regulatory measures are bogged down by arduous and lengthy procedures such that swift reaction to pervasive security threats is an impracticable option. Thus, the private industry must play a role.

[+] J.D., The Catholic University of America, Columbus School of Law, 2022; B.A., University of California, Los Angeles, cum laude, 2019. I would like to thank Lauren Kravetz and Jeffery Goldthorp for their extensive feedback and guidance on this paper.

INTRODUCTION

"One basic reality should go undisputed: there is nearly zero daylight between the communist government of China and its 'companies.'"[1]

Studies have highlighted that Chinese actors "are the source of more cyber-attacks than in any other country" and "are the world's most active and persistent perpetrators of economic espionage."[2] Against this backdrop, "minimiz[ing] exposure to cyberattacks and espionage" in new technology is vital.[3] Shifting

1. FED. COMMC'NS COMM'N, STATEMENT OF COMMISSIONER MICHAEL O'RIELLY RE: CHINA MOBILE INTERNATIONAL (USA) INC., APPLICATION FOR GLOBAL FACILITIES-BASED AND GLOBAL RESALE INTERNATIONAL TELECOMMUNICATIONS AUTHORITY PURSUANT TO SECTION 214 OF THE COMMUNICATIONS ACT OF 1934, AS AMENDED, ITC-214-20110901-00289 [hereinafter STATEMENT OF COMMISSIONER MICHAEL O'RIELLY].

2. STAFF OF H. PERMANENT SELECT. COMM. ON INTEL., 112TH CONG., INVESTIGATIVE REPORT ON THE U.S. NATIONAL SECURITY ISSUES POSED BY CHINESE TELECOMMUNICATIONS COMPANIES HUAWEI AND ZTE. at 7–8 (Oct. 8, 2012) [hereinafter INVESTIGATIVE REPORT].

3. David Stehlin, *Insight: Telecom Industry Must Develop Trustworthy 5G Equipment Supply Chains*, TELECOMM. INDUS. ASS'N (Nov. 5, 2019), https://tiaonline.org/insight-telecom-industry-must-develop-trustworthy-5g-equipment-supply-chains/.

from 4G to 5G technologies creates new issues and vulnerabilities[4] because 5G technology supports "more connected devices and data than ever before."[5] Vulnerabilities and risks introduced by 5G include "malicious software[,]hardware," and "counterfeit components."[6] Were these risks exploited, the consequences would prove detrimental to 5G network security.

Acquiring 5G products usually involves purchasing from one of four major vendors, each of which provides end-to-end solutions: Huawei Technologies Co., Ltd (Huawei), Ericsson, Nokia, or Samsung.[7] Of these four vendors, Huawei is "cheape[st] to deploy," offering equipment at prices nearly 30 percent lower than its competitors.[8] Headquartered in Shenzhen, China, Huawei owns over two-thirds of 5G equipment outside China,[9] making it the largest telecommunications equipment company in the world.[10] Huawei equipment has been recognized by numerous telecom companies as "good . . . if not better than—competing equipment from Nokia or Ericsson."[11] Huawei's widespread availability, "high-quality," and competitive pricing make it an enticing option for suppliers.[12] However, global concerns regarding Huawei's trustworthiness continue to permeate the international community.

---

4. Kate O'Flaherty, *New 5G Security Threat Sparks Snooping Fears*, FORBES (Nov. 13, 2019, 9:24 AM), https://www.forbes.com/sites/kateoflahertyuk/2019/11/13/new-5g-security-threats-spark-snooping-fears/?sh=75752ac85025.

5. David Stehlin, *Insight: Telecom Industry Must Develop Trustworthy 5G Equipment Supply Chains*, TELECOMM. INDUS. ASS'N (Nov. 5, 2019), https://tiaonline.org/insight-telecom-industry-must-develop-trustworthy-5g-equipment-supply-chains/.

6. *5G Introduces New Benefits, Cybersecurity Risks*, DEP'T OF HOMELAND SEC. (Oct. 15, 2020),https://www.dhs.gov/science-and-technology/news/2020/10/15/feature-article-5g-introduces-new-benefits-cybersecurity-risks.

7. Melanie Hart & Jordan Link, *There is a Solution to the Huawei Challenge*, CENTER FOR AM. PROGRESS (Oct. 14, 2020), https:/www.americanprogress.org/issues/security/reports/2020/10/14/491476/solutions-huawei-challenge/.

8. *Id.*

9. Rita Liao, *Huawei Says Two-Thirds of 5G Networks Outside China Now Use Its Gear*, TECH CRUNCH (June 25, 2019, 10:01 PM), https://techcrunch.com/2019/06/25/huawei-wins-5g-contracts/.

10. *Telecommunication Equipment Companies Ranked By Overall Revenue in 2018 (in Billion U.S. Dollars)*, STATISTA (July 17, 2020), https://www.statista.com/statistics/314657/top-10-telecom-equipment-companies-revenue/; *see also*, Jason Tan, *Huawei Now World's Largest Telecom Equipment-Maker*, CAIXIN (Mar. 19, 2018, 4:59 PM), https://www.caixinglobal.com/2018-03-19/huawei-now-worlds-largest-telecom-equipment-maker-101223256.html.

11. Brian Fung, *How China's Huawei took the lead over U.S. companies in 5G technology*, WASH. POST (Apr. 10, 2019), https://www.washingtonpost.com/technology/2019/04/10/us-spat-with-huawei-explained/.

12. Peter Waldman, Sheridan Prasso, & Todd Shields, *Another Reason U.S. Fears Huawei: Its Gear Works and It's Cheap*, BLOOMBERG (Jan. 24, 2019),https://www.bloomberg.com/news/articles/2019-01-24/huawei-stokes-u-s-fear-with-low-cost-networking-gear-that-works. The chief executive officer and general manager of an Oregon telecommunications company stated, Huawei "makes high-quality networking gear that it sells to rural telecommunications operators for 20 percent to 30 percent less than its competitors do[;]" accordingly, its equipment has helped

The People's Republic of China's (China) 2017 National Intelligence Law has raised international governmental concerns regarding Huawei's allegiance to the Communist Party of China (CCP).[13] Under Chinese intelligence laws, "any organization or citizen shall support, assist, and cooperate with state intelligence work according to law."[14] To achieve this, China "may demand . . . organizations, or citizens provide needed support, assistance, and cooperation."[15] Thus, regardless of whether a Chinese partner company is state or privately owned, "it will have close and increasingly explicit ties to the CCP."[16]

Telecommunications networks' supply chains depend heavily on trust;[17] therefore, the "[u]se of 5G components manufactured by untrusted companies" creates a risk that malicious and counterfeit materials will be introduced in a supply chain.[18] With concerns regarding the use of Huawei equipment in critical infrastructure industries, many U.S. officials have voiced concerns that "the Chinese government's ongoing intelligence activities . . . present[] too great of a risk."[19] A former U.S. National Security Advisor has even considered Huawei "the 'number one concern' for democracy moving forward."[20]

"telecom companies provide landlines, mobile services and high-speed data to many of the poorest and most remote areas in the country." *Id.*

13. Murray Scot Tanner, *Beijing's New National Intelligence Law: From Defense to Offense*, LAWFARE (July 20, 2017, 11:30 AM), https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense. The new law places "ill-defined and open-ended new security obligations and risks not only on U.S. and other foreign citizens doing business or studying in China, but in particular on their Chinese partners and co-workers." *Id.* Most concerningly, the law has effectively shifted the "balance of [] legal obligations from intelligence 'defense' to 'offense' –that is, by creating affirmative legal responsibilities for Chinese, and in some cases, foreign citizens, companies, or organizations operating in China to provide access, cooperation, or support for Beijing's intelligence-gathering activities." *Id.*

14. *Id.*

15. *Id.*; Arjun Kharpal, *Huawei Says It Would Never Hand Data to China's Government. Experts Say It Wouldn't Have a Choice* CNBC, (Mar. 4, 2019, 8:13 PM), https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html.

16. CANADIAN SEC. INTEL. SERV., CHINA AND THE AGE OF STRATEGIC RIVALRY: HIGHLIGHTS FROM AN ACADEMIC OUTREACH WORKSHOP 8 (2018).

17. INVESTIGATIVE REPORT, *supra* note 2, at 1.

> Telecommunications networks are vulnerable to malicious and evolving intrusions or disruptive activities. A sufficient level of trust, therefore, with both the provider of the equipment and those performing managed services must exist at all times. . . . If [a company] cannot be trusted, then the United States and others should question whether the company should operate within the networks of our critical infrastructure.

Id.

18. CYBER AND INFRASTRUCTURE SEC. AGENCY, CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE NOTE, at 1 (2019).

19. China Mobile International (USA) Inc., 34 F.C.C.R. 3361, 13 (2019).

20. Maggie Miller, *Huawei Threat 'No. 1 concern' Moving Forward, Trump National Security Adviser says*, THE HILL (Nov. 16, 2020, 2:11 PM), https://thehill.com/policy/cybersecurity/526165-huawei-threat-no-1-concern-moving-forward-trump-national-security. The former advisor, Robert O'Brien, expanded on such concern, stating

This note examines supply chain risk management (SCRM) policies concerning Huawei and the development of these policies within several nations. By comparatively examining five member nations of the Fourteen Eyes—a signals intelligence-sharing group comprised of fourteen nations[21]—this note addresses and analyzes varying methodologies and actions taken to address Huawei risks. The five nations selected for review are the United States (US), United Kingdom (UK), Canada, Italy, and Germany.

This paper will argue that these five nations can be categorized into three major information and communications technology supply chain risk management (ICT SCRM) policy approaches, which stem from the nations' similar methodologies and shared characteristics. This note focuses on commonalities in the approaches, although each nation within each category may exhibit different characteristics. This categorization will explore the pros and cons of various approaches to ICT SCRM and provide insight for developing future alternatives. This analysis suggests that to effectively reduce the threat from Huawei, both government and private industry action are necessary. Absent industry action, there is a risk that Huawei equipment will not be excluded from private networks, either because Huawei equipment already exists in current networks or will be used for developing new networks.

Part I of this paper provides an overview of global ICT supply chains and narrows into a discussion on Huawei's role in ICT supply chains and a brief discussion of the background of Fourteen Eyes. Part II dissects each of the five selected nations, discussing each nation's individual approach to securing domestic ICT supply chains through legal and policy actions to date. Part III analyzes the five nations by categorizing the nations based on their policy methodologies, shared characteristics, and political overlays. This section also discusses the consequences each approach may have on effectively excluding Huawei equipment from networks and how the private industry is a necessary component to mitigate the risk Huawei poses. This paper's ability to engage in a fulsome discussion of this topic is limited by the amount of publicly available information, as national security policies and intelligence analysis are often non-public or classified. Still, sufficient public sources exist to analyze and arrive at some conclusions regarding how nations perceive the threat from Huawei and the likely paths they will take to remediate the threat.

"[i]f you believe in democracy and you're concerned about our elections, [Huawei is] the number one concern that we've got going forward . . . [because] what China could do with . . . Huawei. . . [is] 'really quite scary.'" *Id.*

21. Sven Taylor, *Five Eyes, Nine, Eyes, 14 Eyes-Explained*, RESTORE PRIV. (Oct. 20, 2021), https://restoreprivacy.com/5-eyes-9-eyes-14-eyes.

I. WHAT ARE INFORMATION AND COMMUNICATIONS SUPPLY CHAINS, WHAT IS HUAWEI, AND WHAT IS HUAWEI'S INVOLVEMENT?

A. Information and Communications Technology Global Supply Chains

Defined by the U.S. National Institute of Standards and Technology (NIST), a "supply chain" is a "set of organizations . . . and resources for creating and moving a product or service from suppliers . . . to an organizations customers."[22] Information and communications technology (ICT) supply chain risks are defined as "[r]isks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations . . . organizational assets, individuals, other organizations, and the Nation."[23]

Vulnerabilities in ICT supply chains may result in an insertion of "counterfeits" and "malicious software and hardware" by actors at many different points, including equipment manufacturers, network integrators, and software maintenance representatives.[24] Since "[ICT] relies on a complex, globally distributed, and interconnected supply chain ecosystem . . . consist[ing] of multiple tiers of outsourcing,"[25] securing them is considered a "global problem."[26] Securing a supply chain requires securing "every individual product of each individual node[,]" in addition to "correctly integrat[ing each node] with all other components up and down the production ladder."[27]

Commentators have stated that because "severe vulnerabilities exist in global supply chains," there is an international consensus "that new ways of tackling these shortcomings are needed."[28] Methods to achieve this goal are influenced

---

22. U.S. GOV'T ACCOUNTABILITY OFF., GAO-12-361, IT SUPPLY CHAIN NATIONAL SECURITY-RELATED AGENCIES NEED TO BETTER ADDRESS RISKS, at 1 n.1 (2012). Information technology is "any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display switching, interchange, transmission, or reception of data or information." *Id.*

23. Jon Boyens at el., NAT'L INST. OF STANDARDS AND TECH., SPECIAL PUBLICATION 800-161, SUPPLY CHAIN RISK MGMT PRACS. FOR FED. INFO. SYSTEMS AND ORGS., at 1 n.2 (2015) [hereinafter NAT'L INST. SUPPLY CHAIN RISK MGMT PRACS.]. A general "supply chain risk" arises from the probability that "an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert . . . an item of supply or a system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of a system." ARMED FORCES COMM'N & ELEC. ASS'N CYBER COMM., SUPPLY CHAIN RISK MGMT AWARENESS (2012) [hereinafter ARMED FORCES COMM'N].

24. NAT'L INST. SUPPLY CHAIN RISK MGMT PRACS., *supra* note 23, at 1.

25. *Id.*

26. ARMED FORCES COMM'N, *supra* note 23, at 3.

27. D. Shoemaker and C. Wilson, *The Weakest Link: The ICT Supply Chain and Information Warfare*, 12 J. INFO. WARFARE 10, 11 (2013).

28. Daniel F. Runde & Sundar R. Ramanujam, *Recovery with Resilience: Diversifying Supply Chains to Reduce Risk in the Global Economy*, CTR. FOR STRATEGIC & INT'L STUD., at 2–3 (Sep. 2020), https://csis-website-prod.s3.amazonaws.com/s3fs-public/production/200904_Ramanujam_GlobalSupply_v4.pdf.

by a variety of factors, including governmental structure, the level of "political interference" in decision-making, and other policy decisions.[29] Also relevant are policies regarding corporate liability and market economics.[30]

There is no internationally unified approach to ICT SCRM policy. Some approaches "incentivize and reward corporate collaboration" with governmental policies, while others "require cooperation [that] directly or indirectly penalize noncollaboration."[31] Some governments have created more stringent requirements, such as "legally or politically binding" agreements that would verify a company's compliance with governmental policies.[32]

B. What is Huawei, and What is its Effect on Global ICT Supply Chains?

Huawei was founded in 1987 by Ren Zhengfei, a former officer with the People's Liberation Army during China's Cultural Revolution.[33] In Huawei's early years, the People's Republic of China's goal was to ensure the entity could acquire the "technical know-how from Western firms" to enable it to "muscle into a market where it previously had no presence."[34] Within just ten years, Huawei's annual revenue quadrupled from $18 billion to over $105 billion.[35]

Huawei's dominance in the 5G market stems from three major factors:

> (1) China provides direct and indirect subsidies—including guaranteed market share within China and cheap credit from Chinese state banks—that reduce Huawei's operational costs, speed time to market for Huawei's products, and allow it to price its products well below prices set by its competitors.
>
> (2) Chinese state banks provide generous financing to Huawei's customers on terms most commercial banks cannot match, making Huawei equipment cheaper to deploy at any price.
>
> (3) Chinese officials interfere in the standardization process at the International Telecommunication Union (ITU) to increase Huawei's

---

29. *Id.* at 4.

30. *See* David Forscey & Herb Lin, '*Just Say No' Is Not a Strategy for Supply Chain Security*, LAWFARE (Mar. 25, 2020, 10:55 AM), https://www.lawfareblog.com/just-say-no-not-strategy-supply-chain-security ("[F]or businesses, market realities are an important factor in risk management decisions.").

31. Ariel Levite, *ICT Supply Chain Integrity: Principles for Governmental and Corporate Policies*, CARNEGIE ENDOWMENT FOR INT'L PEACE (Oct. 4, 2019), https://carnegieendowment.org/2019/10/04/ict-supply-chain-integrity-principles-for-governmental-and-corporate-policies-pub-79974.

32. *Id.* Because such stringent systems "inevitably sour the prospects of objective and widespread collaboration[,]" it is infrequently, and unlikely, that such techniques are adopted. *Id.*

33. Sherisse Pham, *US Judge Rejects Huawei Lawsuit Challenging a Ban on its Products*, CNN BUS. (Feb. 19, 2020 11:23 AM), https://www.cnn.com/2020/02/19/tech/huawei-us-lawsuit-rejected/index.html.

34. Hart & Link, *supra* note 7.

35. *Id.*

> share of the emerging global 5G standard, making Huawei equipment even harder to avoid and setting it up to extend its dominance into 6G and beyond.[36]

Over the years, Huawei has been suspected of various forms of malicious activity. In 2012, for example, the African Union contracted with Huawei to provide a new "desktop cloud solution" for the Union's headquarters.[37] In 2018, the African Union discovered its network had been penetrated, and that nightly for five years, the "organisation's secrets were being [transferred] on to servers in Shanghai."[38] While Huawei denies allegations that it intentionally manufactures its equipment with features which allow it secret access to networks and information, many believe otherwise.[39] U.S. officials claim Huawei "built equipment that secretly gave the company access to networks without the knowledge of the carriers."[40] Additionally, a recent FBI report revealed that Huawei has undertaken efforts to steal U.S. trade secrets and technologies and even launched a "policy instituting a bonus program to award employees who obtained confidential information from competitors."[41]

Huawei's equipment comprises over two-thirds of 5G equipment outside of China.[42] With global transitions to 5G networks and minimal options for vendors, Huawei maintains a large stake in ICT supply chains. However, given security concerns regarding its efforts to steal secrets and information, the effects of Huawei's dominance in ICT global supply chains are likely negative.

---

36. *Id.*

37. Angus Grigg, *Huawei Linked to Major Data Breach*, FIN. REV. (July 12, 2018, 11:00 PM), https://www.afr.com/policy/foreign-affairs/huawei-linked-to-major-data-breach-20180712-h12l84.

38. John Aglionby et al., *African Union Accuses China of Hacking*, FIN. TIMES (Jan. 29, 2018), https://www.ft.com/content/c26a9214-04f2-11e8-9650-9c0ad2d7c5b5. Suggested links between Huawei equipment and backdoors allowing breaches have been the subject of high-level, public statements from several individuals, including former U.S. National Security Advisor, Robert O'Brien. O'Brien asserts evidence shows "Huawei has the capability secretly to access sensitive and personal information in systems it maintains and sells around the world[.]" Ishita Chigilli Palli, *US has Evidence of Huawei Backdoor: Report*, BANK INFO SEC. (Feb. 13, 2020), https://www.bankinfosecurity.com/us-has-evidence-huawei-backdoor-access-report-a-13718.

39. AGLIONBY ET AL., *supra* note 38.

40. Palli, *supra* note 38.

41. DEP'T OF JUST., CHINESE TELECOMMUNICATIONS CONGLOMERATE HUAWEI AND SUBSIDIARIES CHARGED IN RACKETEERING CONSPIRACY AND CONSPIRACY TO STEAL TRADE SECRETS (2020). Huawei faces a 16-count idictment stemming from the "long-running practice of using fraud and deception to misappropriate sophisticated technology from U.S. counterparts." *Id.* As revealed by the FBI's investigations, the "misappropriated intellectual property included trade secret information and copyrighted works, such as source code and user manuals for internet routers, antenna technology and robot testing technology." *Id.*

42. Liao, *supra* note 9.

II. VARYING INTERNATIONAL APPROACHES TO SECURING ICT SUPPLY CHAINS

A. The Fourteen Eyes Intelligence Alliance

Since World War II,[43] Britain and the United States have maintained a robust intelligence-sharing partnership with one another.[44] Along with Canada, Australia, and New Zealand, these five nations – the Five Eyes – became a "multilateral intelligence sharing alliance created by the UKUSA Agreement"[45] and serve as the foundation of Western nations' intelligence sharing.[46] Nine additional nations—comprising the "Fourteen Eyes" in aggregate—serve as third parties to the Agreement and participate in SIGINT—signals intelligence—sharing.[47] These additional nations include Denmark, France, Netherlands, Norway, Germany, Belgium, Italy, Sweden, and Spain.[48]

The Fourteen Eyes continue to play a role in developing international strategies as evinced by an unnamed, high-ranking U.S. official's remark "that '[c]onsultations "with our allies . . . on how to resolve China's assertive international strategy have been frequent and are gathering momentum.'"'[49] The concern has been that "if global networks run on Huawei equipment, Beijing could use that equipment to gather intelligence . . . and potentially bring down networks to incapacitate other nations in times of crisis."[50] This paper focuses on the particular approaches to date of the United States, United Kingdom, Canada, Italy, and Germany.[51]

1. The United States of America

The United States has taken a multifaceted approach to secure ICT supply chains. Policy affecting federal government use of Huawei has resulted in

---

43. Dailey J, *The Intelligence Club: A Comparative Look at Five Eyes*, 5 J. POL. SCI. PUB. AFFS. 1, 1 (2017).

44. Braden Couch, *Five Eyes: Unblinking, Unmoving, and Out of Control*, 45 N.C.J. INT'L L. 25, 29 (2019). During the War, the two nations worked closely together to collect signals intelligence and intercept the axis powers' communications. *Id.* at 31–32; *see also* Dailey J., *supra* note 43, at 1.

45. Richie Koch, *What Countries are in the 5 Eyes, 9 Eyes, and 14 Eyes Agreements?*, PROTONVPN (Aug. 30, 2018), https://protonvpn.com/blog/5-eyes-global-surveillance/; *see also* Couch, *supra* note 44, at 26–27.

46. Koch, *supra* note 45.

47. *Id.* While these fourteen parties trade raw data, akin to the primary five nations, the fourteen nations have less access to certain resources, such as the NSA's database. *Id.*

48. Sven Taylor, *Five Eyes, Nine Eyes, 14 Eyes-Explained*, RESTORE PRIV. (Oct. 20, 2021), https://restoreprivacy.com/5-eyes-9-eyes-14-eyes/.

49. Couch, *supra* note 44, at 33 (alteration in original).

50. Hart & Link, *supra* note 7.

51. *See, e.g.*, *Huawei in 5G: Where Do Other Five Eyes Countries Stand?*, FORCES NET (Jan. 28, 2020, 4:05 PM), https://www.forces.net/news/huawei-5g-where-do-other-five-eyes-countries-stand (discussing the several approaches adopted by various nations with respect to exclusionary policies which target Huawei).

excluding Huawei equipment from government networks. Additionally, government policy has begun affecting private consumers by conditioning certain government benefits on complying with exclusions of Huawei equipment. The government has been consistent with its approach towards Huawei in executive, legislative, and regulatory policy.

In 2013, President Obama promulgated Executive Order 13636, "Improving Critical Infrastructure Cybersecurity,"[52] designed to improve the cybersecurity of select entities and critical infrastructure as "cybersecurity incident[s] could . . . result in catastrophic regional or national effects on . . . national security."[53] Although the order directed NIST to develop "a framework to reduce cyber risks to critical infrastructure," it did not directly address supply chains or any specific actor.[54] Commenters opined that the Obama Administration seemed to come to the "defence of Huawei's business practices, corporate governance and intent in expanding its U.S. investments."[55]

The Trump Administration took a much tougher stance. In 2019, President Trump signed Executive Order 13873, "Securing the Information and Communications Technology and Services Supply Chain,"[56] declaring ICT supply chains a matter of "national emergency," and characterizing the concerns as an "unusual and extraordinary threat to the national security . . . of the United States."[57] The Executive Order prohibits "any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service (transaction) by any person . . . where the transaction involves any property in which any foreign country or a national thereof has any interest."[58] It also delegates large roles to the Secretary of Commerce, Secretary of Homeland Security, and the Director of National Intelligence in how to move forward with determining and executing ways to better secure US supply chains.[59] Although President Trump's Executive Order did not specifically label Huawei, the release of the Executive Order occurred on the heels of "months of

52. Exec. Order No. 13636, 78 Fed. Reg. 11739 (Feb. 19, 2013).

53. *Id.*; *see also* TARA BEENY ET AL., SUPPLY CHAIN VULNERABILITIES FROM CHINA IN U.S. FEDERAL INFORMATION AND COMMUNICATIONS TECHNOLOGY, at 9 (Apr. 2018).

54. Exec. Order No. 13636, 78 Fed. Reg. 11739 (Feb. 19, 2013); BEENY ET AL., *supra* note 53, at 9.

55. Simon Montlake, *U.S. Congress Flags China's Huawei, ZTE As Security Threats*, FORBES (Oct. 8, 2012, 12:37 AM), https://www.forbes.com/sites/simonmontlake/2012/10/08/u-s-congress-flags-chinas-huawei-zte-as-security-threats/#525b8e8d784a.

56. Exec. Order No. 13873, 84 Fed. Reg. 22689 (May 15, 2019).

57. *Id.*

58. *Id.*

59. *Id.*

U.S. pressure on Huawei"[60] and at the same time as other actions directed at China.[61]

Pursuant to delegated authority, several executive agencies implemented policies—through standard rulemaking procedures[62]—consistent with the Administration's move to secure ICT supply chains, with some focusing on Huawei.[63] The Bureau of Industry and Security, a sub-agency of the Department of Commerce (DoC), "restricted access by Huawei . . . and its non-U.S. affiliates on the Entity List to items produced domestically and abroad from US technology and software."[64] The Entity List was originally established as an effort to "inform the public of entities who have engaged in activities" threatening or posing risks to various matters, such as weapons of mass destruction programs.[65] Since then, the Entity List has been developed and expanded to include entities with "activities contrary to U.S. national security and/or foreign policy interests."[66] The National Telecommunications and

60. Frank Bajak & Tali Arbel, *Huawei Hit by US Export Controls, Potential Import Ban*, AP (May 16, 2019), https://apnews.com/article/97e72ba36d814c63ad0325688963a9d9.

61. Examples of this include the ongoing war on trade with China, President Trump urging the United Nations to "'hold China accountable' for the coronavirus pandemic," and President Trump's recent executive order banning transactions and activities with eight Chinese companies. Amanda Macias, *Trump Urges UN to Hold China Accountable for the Coronavirus Pandemic*, CNBC (Sep. 22, 2020, 1:40PM), https://www.cnbc.com/2020/09/22/trump-urges-un-to-hold-china-accountable-for-coronavirus-pandemic.html; *see also* Ryan Hass & Abraham Denmark, *More Pain than Gain: How the US-China Trade War Hurt America*, BROOKINGS (Aug. 7, 2020), https://www.brookings.edu/blog/order-from-chaos/2020/08/07/more-pain-than-gain-how-the-us-china-trade-war-hurt-america/; Andrew Shoyer et. al., *Trump Executive Order Blocks Transactions With Certain Chinese Software Applications*, DATA MATTERS (Jan. 8, 2021), https://datamatters.sidley.com/trump-executive-order-blocks-transactions-with-certain-chinese-software-applications.

62. *See* Rules Affecting the Export Administration Regulations, BUREAU INDUS. & SEC., https://www.bis.doc.gov/index.php/federal-register-notices/17-regulations/1541-federal-register-notices-2019; 15 C.F.R. § 744 (2019); 85 Fed. Reg. 41,006 (2020); 41 C.F.R. § 201 (2020).

63. For example, the U.S. Department of Justice pressed charges against Huawei and several of its subsidiaries, alleging that Huawei stole "trade secrets, misled banks about its business[,] and violated U.S. sanctions on Iran." Bajak & Arbel, *supra* note 60. Another example of this is exhibited by the U.S. Department of Energy's decision to prevent electric utility companies from purchasing Chinese equipment. Sonal Patel, *DOE Bans Utility Procurement of Chinese Equipment for Bulk Power System Security*, POWER MAG. (Dec. 18, 2020), https://www.powermag.com/doe-bans-utility-procurement-of-chinese-equipment-for-bulk-power-system-security/.

64. U.S. DEP'T COMM., COMMERCE DEPARTMENT FURTHER RESTRICTS HUAWEI ACCESS TO U.S. TECHNOLOGY AND ADDS ANOTHER 38 AFFILIATES TO THE ENTITY LIST (Aug. 17, 2020). The Department of Commerce defines its entity list as being comprised of "license requirements that it imposes on each listed person." Entity List, BUREAU OF INDUS. & SEC. (last visited Jan. 15, 2021), https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list. The original purposes of the Department publishing an entity list was to "inform the public of entities who have engaged in activities that could result in an increased risk of the diversion of exported . . . items to weapons of mass destruction." *Id.*

65. *Id.*

66. *Id.*

Information Administration (NTIA), also a DoC sub-agency, established the Communications Supply Chain Risk Information Partnership (C-SCRIP),[67] which is designed to "share supply chain risk information with trusted communications providers and suppliers."[68] Another executive effort is illustrated by the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) creation of a SCRM task force.[69] The task force has multiple working groups comprised of both government and non-government participants and works to address various aspects of the supply chain process.[70]

a. Restrictions on Use of Huawei in U.S. Government Networks

Under Title II of the SECURE Technology Act, the Federal Acquisition Supply Chain Security Act of 2018 "established in the executive branch a Federal Acquisition Security Council" (FASC).[71] FASC's purpose is to create recommendations and criteria for information sharing "with executive agencies, other Federal entities, and non-Federal entities with respect to supply chain risk."[72] The head of each executive agency is responsible for an array of duties relating to assessing, prioritizing, and integrating supply chain risk practices to limit, avoid, and mitigate identified risks.[73] These duties "bolster[] the U.S. government's acquisition oversight for critical information and communications technologies."[74] By requiring each department and agency to have a SCRM

67. 85 Fed. Reg. 41006 (July 8, 2020).

68. *NTIA Announces Supply Chain Information-Sharing Program*, NAT'L TELECOMM. INFO ADMIN U.S. DEPT. OF COM. (July 8, 2020), https://www.ntia.doc.gov/blog/2020/ntia-announces-supply-chain-information-sharing-program.

69. CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, INFORMATION AND COMMUNICATION TECHNOLOGY SUPPLY CHAIN RISK MANAGEMENT TASK FORCE: INTERIM REPORT iii (2019).

70. *Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/ict-scrm-task-force; CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, *supra* note 69, at 4. The four working groups cover information sharing, understanding and evaluating supply chain threats, identifying criteria for Qualified Manufacturers, and recommendations for policies regarding ICT purchasing. *Id.*

71. SECURE Technology Act, 41 U.S.C. §1322(a). Members of FASC are to include the Office of Management and Budget, General Services Administration, Department of Homeland Security (including Cybersecurity and Infrastructure Security Agency), Office of the Director of National Intelligence, Department of Justice (including the Federal Bureau of Investigation), Department of Defense (including the National Security Agency), and the Department of Commerce (including National Institute of Standards and Technology). *Id.* at §1322(b)(1).

72. *Id.* at § 1323(a)(2); 41 C.F.R. § 201 (2020). Additionally, FASC is tasked with developing criteria in "[d]etermining the risk to the ICT supply chain[,] [d]isseminating supply chain risk information, and [d]eciding what action to take to mitigate the risk." FED. ACQUISITION SEC. COUNCIL, SUPPLY CHAIN RISK MANAGEMENT (2018).

73. 41 U.S.C. §§ 1326(a)–(b).

74. FED. ACQUISITION SEC. COUNCIL, *supra* note 72.

program, FASC promotes the development of uniform criteria for SCRM,[75] which in turn "arms departments and agencies with [] knowledge" regarding supply chain risks.[76]

Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019 prohibited "executive agencies from entering into, or extending or renewing, a contract with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system."[77] The act, in pertinent parts, defines "covered foreign country [as] the People's Republic of China"[78] and "covered telecommunications equipment or services" as including "[t]elecommunications equipment produced by Huawei Technologies . . . or any subsidiary or affiliate of such."[79]

In an interim rule, published by the General Services Administration, Department of Defense, and National Aeronautics and Space Administration, amendments to Federal Acquisition Regulations were planned to facilitate implementation of Section 889(a)(1)(B).[80] This would apply to the use of covered telecommunications equipment by both the Federal Government and federal contractors in order to avoid any ultimate disruption or delay in the Federal Government's operations.[81]

---

75. *Id.*

76. *Id.*

77. John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115–232, § 889(a)(1)(B), 132 Stat. 1636, 1917 (2018); 85 Fed. Reg. 135 (2020). In March of 2019, Huawei filed suit against the US government, challenging the constitutionality of NDAA's Section 889. *Huawei Sues US Government Over Product Ban*, BBC NEWS (Mar 7, 2019), https://www.bbc.com/news/business-47478587. Huawei argued that, first, the Congressional bill was an unconstitutional bill of attainder, which legislatively punished Huawei without it first being given a fair trial; and second, the bill would restrict Huawei from "engaging in fair competition." *Id.*; *Huawei Sues US Over Equipment Ban, Escalating Legal Clash*, INDUS. WK. (Mar. 7, 2019), https://www.industryweek.com/leadership/article/22027272/huawei-sues-us-over-equipment-ban-escalating-legal-clash. By February of 2020, a U.S. District Judge ruled in favor of the U.S., holding that Congress has the "power to restrict federal agencies from doing business with Huawei and ZTE . . . [c]ontracting with the federal government is a privilege, not a constitutionally guaranteed right." Pham, *supra* note 33. The judge also noted that Huawei faced no broad restrictions on its business endeavors in the US, given that it could "still conduct business with every other company and individual in America as well as the remaining 169 countries and regions it currently does business with." *Id.*

78. John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115–232, § 889(f)(2), 132 Stat. 1636, 1918 (2018).

79. *Id.* at § 889(f)(3)(A).

80. Sean Graves & Suzanne Sumner, *Updated Rule Bans Federal Contractor Use of Huawei and Other Telecommunication Technology*, LEXOLOGY (July 22, 2020), https://www.lexology.com/library/detail.aspx?g=da6d8c76-df81-4360-9023-c4d6f9ebbc7c.

81. Federal Acquisition Regulation: Prohibition on Contracting With Entities Using Certain Telecommunications and Video Surveillance Services or Equipment, 85 Fed. Reg. 42665 (July 14, 2020).

b. Restrictions on Use of Huawei Affecting Private Consumers

Pursuant to Section 3 of the SECURE Technology Act, the Federal Communication Commission's (FCC) Public Safety and Homeland Security Bureau (PSHSB), acting on delegated authority from the Commission, made initial and final designations of Huawei as a "national security threat."[82] Citing Huawei, and another prominent Chinese telecommunications company ZTE, as "a unique threat," PSHSB explained the threat posed "to the security and integrity of the nation's communications networks and communications supply chain because of their size, their close ties to the Chinese government, and the security flaws identified in their equipment."[83] Designating Huawei as a national security threat enabled the FCC, following the standard notice and comment rulemaking process, to forbid private entities who were receiving subsidies through the Universal Service Fund (USF) program from using those funds to purchase equipment from designated national security threat entities, like Huawei.[84] Additionally, the FCC introduced a "rip and replace" order, which offers subsidies to smaller telecom carriers to remove and replace Huawei equipment.[85] Estimated costs of this process, however, are substantial—roughly $1.6 billion.[86]

In December 2017, before the FCC designated Huawei as a national security threat, members of the U.S. Senate and House of Representatives intelligence committees sent the FCC a letter, noting their concerns about Chinese companies in telecommunications networks.[87] Commentators have speculated that this letter pressured AT&T—a dominant US telecommunications carrier—to withdraw from a planned smartphone deal with Huawei.[88] As a consequence of the withdrawal, it has become "very difficult for Huawei to get significant

82. Protecting Against Nat'l Sec. Threats to the Commc'ns Supply Chain through FCC Programs Huawei Designation ZTE Designation, 34 FCC Rcd. 11423, 11424 (2019); Protecting Against Nat'l Sec. Threats to the Commc'ns Supply Chain through FCC Programs – Huawei Designation, 35 FCC Rcd. 6604, 6604 (2020); *see also* 47 C.F.R. § 54.9(b) (2020).

83. Protecting Against Nat'l Sec. Threats to the Commc'ns Supply Chain through FCC Programs – Huawei Designation, 35 FCC Rcd. at 6605.

84. Protecting Against Nat'l Sec. Threats to the Commc'ns Supply Chain through FCC Programs Huawei Designation ZTE Designation, 34 FCC Rcd. at 11424.

85. FED. COMMC'NS COMM'N, WC DOCKET NO. 18-89, PROTECTING AGAINST NATIONAL SECURITY THREATS TO THE COMMUNICATION SUPPLY THROUGH FCC PROGRAMS (2020) (hereinafter "SECOND REPORT AND ORDER").

86. Sarah Barry James, *FCC Approves Telecom Equipment Rip-and-Replace Order Covering Huawei, ZTE,* SPGLOBAL (Dec. 10, 2020), https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/fcc-approves-telecom-equipment-rip-and-replace-order-covering-huawei-zte-61689729.

87. Sijia Jiang, *Huawei's AT&T U.S. Smartphone Deal Collapses*, REUTERS (Jan. 8, 2018, 4:00 PM),
https://www.reuters.com/article/us-at-t-huawei-tech/huaweis-att-u-s-smartphone-deal-collapses-idUSKBN1EX29E.

88. *Id.*

[market shares] in the U.S."[89] Following AT&T's decision, Verizon—another prominent US carrier—dropped its plans to sell Huawei phones.[90]

c. Other U.S. Government Attempts to Reduce the Prevalence of Huawei

The recent NDAA FY21, passed by Congress over a Presidential veto, included the "Wireless Supply Chain Innovation and Multilateral Security,"[91] "direct[ing] the [NTIA] to begin issuing competitive grants . . . that promote" and "enhance competitiveness in the supply chains of Open RAN 5G Networks."[92] Section 9202(a) grants security funding for communications technology and permits funds to "[a]ccelerat[e] commercial deployments of open interface standards-based compatible, interoperable equipment . . . such as the O-RAN Alliance [or] the Open-RAN Software Community."[93] "Open-RAN" is defined as "the Open Radio Access Network approach to standardization adopted by the O-RAN Alliance."[94] As a concept, Open RAN "creates standardized and interoperable interfaces between systems in the radio access network[,]" which would substitute for traditional telecommunication networks interfaces that are "either proprietary or optimized by the individual vendor, and are often tied to the underlying hardware layer."[95] Thus, opening interfaces with Open RAN would provide operators the opportunity to "integrate components from a variety of vendors" and enable companies in the telecom industry to "specialize in sub-components rather than end-to-end solutions."[96]

---

89. *Id.*

90. Rachel England, *Verizon Follows AT&T in Dropping Huawei Smartphones*, ENGADGET (Jan. 30, 2018), https://www.engadget.com/2018-01-30-verizon-follows-atandt-in-dropping-huawei-smartphones.html. Some commentators have speculated that Verizon's decision to exclude Huawei resulted from the pressure it felt once AT&T decided to exclude Huawei. *Id.*

91. National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 3388 § 9202.

92. Ron Westfall, *Open RAN 5G Bill: Congress Ups 5G Stakes with Passage of $750 Million Open RAN 5G Bill*, FUTURUM (Nov. 23, 2020), https://futurumresearch.com/research-notes/open-ran-5g-bill-congress-ups-5g-stakes-with-passage-of-750-million-open-ran-5g-bill/. The bill was unanimously passed by the House of Representatives and aimed to target $750 million in funding to help spur Open RAN industry developments. *Id.*

93. National Defense Authorization Act (NDAA) for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 3388 § 9202(a)(1)(C)(ii) (2021). This bill also sets up a "Multilateral Telecommunications Security Fund to support the development and adoption of secure and trusted telecommunications technologies." *Id.* § 9202(a)(2)(B).

94. *Id.* § 9202(b)(5).

95. Melissa K. Griffith, *Open RAN and 5G: Looking Beyond the National Security Hype*, WILSON CTR. (Nov. 2, 2020), https://www.wilsoncenter.org/article/open-ran-and-5g-looking-beyond-national-security-hype. Commentators have opined that Open RAN has received much attention because the concept has "been framed as a national security imperative and an important tool for keeping untrusted vendors (namely Huawei and ZTE) out of 5G networks at home and abroad." *Id.*

96. *Id.*

"[A]dvocates for Open RAN claim" the diversity and innovation of the system "will muscle out Chinese companies like Huawei whose relative advantage is in providing proprietary, vertically integrated networks at low cost."[97] In addition, "U.S. policy makers view Open RAN as an avenue for U.S.-based 5G suppliers to compete more effectively against China-based supplier[] Huawei."[98]

Overall, the United States is engaging in a "'whole of government' approach" to minimize Huawei's presence in ICT supply chains, citing Huawei as a national security concern. Executive, legislative, and regulatory actions are chipping away at Huawei's access both to the substantial amount of equipment and services purchased by the federal government and services purchased by providers for businesses and consumers.[99]

2. The United Kingdom

As of late 2021, the UK has no ICT SCRM policy targeting Huawei that carries the force of law. However, the UK is on track to imitate the US's efforts through pending legislation in the House of Commons. If passed, the legislation would echo that of the US by designating Huawei as a national security threat. UK's policy on Huawei shifted in 2020, from originally permitting the equipment in certain communications networks to excluding its equipment completely. This policy shift was concurrent with the deterioration of political relations between the UK and China. Government officials' stances and statements in the UK mirror the domestic shifts, indicating a tougher, more stringent position on Huawei. Overall, UK's ICT SCRM proposed legislation targets Huawei explicitly rather than targeting national security threats and envisions a framework that would curtail the use of Huawei products.

---

97. *Id.* In October of 2020, under leadership by former Chairman Ajit Pai, the Federal Communications Commission hosted an event on Open RAN technologies. *Id.* During this event, much attention was given to the economic benefits brought by Open RAN, and to the security implications associated with the presence of Chinese equipment in 5G networks. *Id.* This event received much attention in both the government and private industries, as a keynote speaker of this event was former Secretary of State, Mike Pompeo, who stressed that Open RAN is a "crucial tool for 'addressing the China challenge' the U.S. now faces." *Id.* This intragovernmental appearance from a key executive member at an independent regulatory event emphasizes "the recent geopolitical weight that has been given to Open RAN in the U.S." *Id.*

98. Westfall, *supra* note 92.

99. Laura H. Phillips et al., *Current "Whole of Government" Approach to Perceived National Security Risks from Chinese Technology Reflected in the FCC's Latest Universal Service Fund Order* FAEGRE DRINKER (Dec. 4, 2019), https://www.faegredrinker.com/en/insights/publications/2019/12/current-whole-of-government-approach-to-perceived-national-security-risks-from-chinese-technology-__?utm_source=Drinker_Communications&utm_medium=Email&utm_campaign=Current-Whole-of-Government-Approach-to-Perceived-National-Security-Risks-from-Chinese-Technology-Reflected-in-the-FCCs-Latest-Universal-Service-Fund-Order (discussing the U.S.'s combined government efforts via FCC action to unanimously ban Huawei from all projects funded by the Universal Service Fund).

The UK's approach to securing ICT supply chains can be characterized as one of patchwork. A July 2019 "UK Telecoms Supply Chain Review Report," issued to Parliament by the Department for Digital, Culture, Media, and Sport, stated that the government was "not yet in a position to make a final decision on individual high risk vendors and the additional controls that will be applied to them."[100] The Intelligence and Security Committee of Parliament stated that the effects of this delay were beginning to "caus[e] serious damage to [their] international relationships" and because of this, "a decision [needed to] be made as a matter of urgency."[101] The Secretary of State for Digital, Culture, Media & Sport stated that the UK would "legislate to put the telecoms security requirements on a statutory footing, strengthen the powers of the regulator . . . to enforce the security requirements, and provide new national security powers for government to respond to supply chain risks in the future."[102]

In January 2020, Prime Minister (PM) Boris Johnson permitted "'high-risk vendors' such as Huawei . . . in[] the non-sensitive parts of the 5G network[,]" at a cap of 35 percent.[103] High-risk vendors were excluded from sensitive core and critical networks.[104] Britain defended this position, claiming Five Eyes intelligence-sharing would not be jeopardized, as there is a fundamental difference between constructing 5G and sharing classified data.[105] This stance remained the UK's position until July 14, 2020.[106]

In mid-July, following a meeting of the U.K. National Security Council, PM Johnson announced his decision to restrict Huawei from 5G telecom networks and to remove Huawei equipment from current systems by 2027.[107] The U.K.

---

100. DEP'T FOR DIGIT., CULTURE, MEDIA & SPORT, UK TELECOMS SUPPLY CHAIN REVIEW REPORT 7 (2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819469/CCS001_CCS0719559014-001_Telecoms_Security_and_Resilience_Accessible.pdf.

101. INTEL. AND SEC. COMM. OF PARLIAMENT, STATEMENT ON 5G SUPPLIERS, https://isc.independent.gov.uk/wp-content/uploads/2021/01/20190719_ISC_Statement_5G Suppliers_Web.pdf.

102. DEP'T FOR DIGIT., CULTURE, MEDIA & SPORT, *supra* note 100, at 1.

103. Paul Sandle & Jack Stubbs, *Defying Trump, UK's Johnson Refuses to Ban Huawei 5G,* REUTERS (Jan. 27, 2020, 7:38 PM), https://fr.reuters.com/article/us-britain-usa-huawei-idUSKBN1ZR02G. Former U.S. White House National Security Council Senior Director, Tim Morrison, emphasized "[i]f Huawei is allowed into any part of your network, it is allowed into every part of your network." *Id.* A separate Trump administration official also stated, relatedly, that "[t]here is no safe option for untrusted vendors to control any part of a 5G network." *Id.*

104. *Id.*

105. *Id.*

106. Stuart Seidel, *US-UK to Remove Huawei from UK 5G Networks by 2027, Bans Huawei from Supplying New 5G Equipment*, BAKER MCKENZIE (July 17, 2020), https://www.internationaltradecomplianceupdate.com/2020/07/17/us-uk-to-remove-huawei-from-uk-5g-networks-by-2027-bans-huawei-from-supplying-new-5g-equipment/.

107. *Id.*

Secretary of State claimed the change in course as a result of the significantly different landscape following the US's sanctions on Huawei.[108] He stated his uncertainty regarding Huawei's presence in the supply chain and that "the UK [could] no longer be confident it [could] guarantee the security of future Huawei 5G equipment."[109] Additionally, Parliament's Defence Committee reported a finding of "clear evidence" that Huawei "colluded with the Chinese state," prompting it to adopt the position that the UK "may need to remove all Huawei equipment earlier than planned."[110]

Timing of the UK's shift correlates with the increasing tension between the UK and China over China's actions in Hong Kong.[111] On June 30, 2020, the implementation of China's new National Security law in Hong Kong severed the territorial agreement between the UK and China, under which China was not yet to effectuate the CCP within Hong Kong.[112] As tensions rose, the UK announced its decision to ban Huawei from U.K. communications networks two weeks before the official severance.[113]

Concurrent with the announcement that Huawei equipment and services would be banned from U.K. communications networks, a new Telecoms (Security) Bill, which would amend the U.K.'s Communications Act 2003, was under consideration.[114] The new bill "plac[es] strengthened telecoms security duties on telecoms providers, [and] provid[es] new powers for the government

---

This announcement, appearing in a Press Release issued by both the Department for Digital, Culture, Media & Sport and the National Cyber Security Centre, stated there was to "be a ban on the purchase of new Huawei kit[s] for 5G" and that Huawei equipment "will be completely removed from 5G networks by the end of 2027." Huawei to be removed from UK 5G networks by 2027 (July 14, 2020), https://www.gov.uk/government/news/huawei-to-be-removed-from-uk-5g-networks-by-2027.

108. Hadas Gold, *UK Bans Huawei From its 5G Network in Rapid About-Face*, CNN BUS. (July 14, 2020, 1:12 PM), https://www.cnn.com/2020/07/14/tech/huawei-uk-ban/index.html.

109. *Id.*

110. *UK Parliament Committee says Huawei Colludes with the Chinese State*, REUTERS (Oct. 8, 2020, 3:46 AM),
https://www.reuters.com/article/us-britain-huawei/uk-parliament-committee-says-huawei-colludes-with-the-chinese-state-idUSKBN26T144.

111. *See* Hilton Yip, *China's Surging Nationalism Has Claimed Hong Kong*, FOREIGN POL'Y (May 28, 2020, 12:52 PM), https://foreignpolicy.com/2020/05/28/hong-kong-nationalism-china-security-law-protests/.

112. *Id.* In effect, the law eviscerates "Hong Kong's autonomy under the 'one country, two systems' arrangement that has been in place since 1997." *Id.*

113. *Id.*

114. *See* Factsheet 2: New Telecoms Security Framework (Nov. 24, 2020), https://www.gov.uk/government/publications/telecommunications-security-bill factsheets/factsheet-2-new-telecoms-security-framework. Acknowledging the "lack of incentives for telecoms providers to apply security best practices" and the "tensions between commercial priorities and commercial concerns," the UK government introduced a new telecoms security framework through the Telecommunications (Security) Bill which "imposes new statutory duties and requirements for the UK's public telecoms providers." *Id.*

to set out specific security requirements."[115] At the time of writing this article, the bill had passed the House of Commons stages and was set for its third and final reading in the House of Lords in late 2021 through early 2022.[116] This bill will introduce a stronger telecoms security framework by "placing strengthened telecoms security duties on public telecoms providers" and "introduc[ing] new national security powers for the government to manage risks posed by high risk vendors."[117] The bill also "places new obligations on public telecoms service providers to share information with Ofcom [the telecom regulator] that is necessary to assess the security of their networks" and "introduces financial penalties for non-compliance."[118] Lastly, "[t]he Bill creates new powers for the Secretary of State to designate vendors for the purpose of . . . imposing controls on [public communications providers'] use of those designated vendors' goods."[119] This designation occurs only when the Secretary deems it "necessary in the interests of national security."[120]

While the bill has not yet become law and no other legislation or regulatory actions have limited the use of Huawei equipment or services in the U.K. communications network, the UK has taken non-legislative measures to recommend ICT SCRM practices that would exclude Huawei equipment. Chief among these actions is the U.K.'s National Cyber Security Centre (NCSC) report identifying Huawei by name and offering recommendations for risk mitigation security practices.[121] NCSC is "the national technical authority for information assurance and the lead Government operational agency on cyber security,"[122] which is part of the Government Communications Headquarters, and "acts as a bridge between industry and government, providing a unified source of advice, guidance and support on cyber security."[123] The NCSC's original January 28,

115. *Id.*

116. Telecommunications (Security) Act 2021, c. 31 (UK), https://bills.parliament.uk/bills/2806). After the third reading in the House of Lords, it passes to its final stages of "consideration of amendments" and "royal assent." *Id.*

117. Factsheet 1: Overview (Nov. 24, 2020), https://www.gov.uk/government/publications/telecommunications-security-bill-factsheets/factsheet-1-overview.

118. *Id.*

119. *Id.*

120. *Id.*

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

122. HUAWEI CYBER SECURITY EVALUATION CENTRE (HCSEC) OVERSIGHT BOARD ANNUAL REPORT 2020: A REPORT TO THE NATIONAL SECURITY ADVISER OF THE UNITED KINGDOM (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 (hereinafter "HCSEC OVERSIGHT ANNUAL REPORT 2020").

123. NCSC (National Cyber Security Centre) (last visited Mar. 13, 2022), https://www.gov.uk/government/organisations/national-cyber-security-centre.

2020 report did not go as far as to specifically identify Huawei, but the July 14, 2020 update, which came after the release of the U.S. Entity List, did.[124]

Reflecting the UK's shift towards tougher policies on Huawei, the Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board issued a 2020 annual report to the National Security Adviser of the UK.[125] HCSEC, belonging to Huawei Technologies, was founded in 2010 to serve as a liaison between Huawei and Her Majesty's Government to identify and mitigate risks arising in the UK's critical national infrastructure.[126] The 2020 report raised issues regarding Huawei's "poor coding practices" as it continues to fail to follow "its own internal secure coding guidelines."[127]

While UK law is undergoing review and finalization, private telecom companies, in the meantime, have discovered alternative vendors and solutions to Huawei. One example of this occurred in November 2020 when Vodafone, a British mobile operator, announced it would not be contracting with Huawei but instead would explore alternative technology, such as Open RAN.[128] Switching to Open RAN, even without the UK's legislation officially in place, indicates the hesitance of private telecom operators to voluntarily continue using Huawei equipment.

In sum, the UK's shift to prohibiting Huawei products in U.K. communications networks, coupled with assessments in Parliament and other oversight boards, reflects the UK's decreasing tolerance for Huawei equipment

---

124. NAT'L CYBER SEC. CTR., *supra* note 121. The July update echoed the U.S.'s approach toward Huawei, addressing the following factors:

> (a) Huawei has a significant market share in the UK already, which gives it a strategic significance; (b) It is a Chinese company that could, under China's National IntelligenceLaw of 2017, be ordered to act in a way that is harmful to the UK; (c) We assess that the Chinese State (and associated actors) have carried outand will continue to carry out cyber attacks against the UK and our interests; (d) Our experience has shown that Huawei's cyber security and engineeringquality is low and its processes opaque. . .; and (e) A large number of Huawei entities have been included on the US Entity listfor over 12 months now.

Id.

125. HCSEC OVERSIGHT ANNUAL REPORT 2020, *supra* note 122.

126. *Id.*

127. *Id.* The 2020 report stated, because Huawei failed to address and assess the security risks raised by NCSC in its previous report, the UK was left exposed to such risks. *Id.* Causes of these risks were considered ongoing, but inclusive of the following:

> Huawei had inadequate component management and did not align end-of-life dates of components with end-of-life date of products. Furthermore, Huawei did not identify the issue themselves. Once identified by NCSC, Huawei did not remediate the issue promptly. It took 18 months for network remediation to begin.Remediation of nationally distributed access networks, including productreplacement where necessary, takes time and is resource intensive. The issue has been compounded by Huawei being placed on the U.S.Entity List.

Id.

128. Joe Devanesan, *Is OpenRAN the 5G Alternative to Huawei?*, TECHHQ, (Nov. 20, 2020), https://techhq.com/2020/11/is-openran-the-5g-alternative-to-huawei/.

in 5G deployment. This shift is reflected through both the recent proposal of the Telecoms Bill and through the independent actions of private industry. Though the legislation remains pending, the U.K. appears credible in prohibiting all Huawei products in the near future.

3. Canada

Canada has not adopted a law or policy to restrict Huawei equipment. Canada's action in ICT SCRM policy has been limited and inconsistent throughout its governance. While some agencies of the Canadian government have produced guidance documents and action plans for ICT SCRM, none approach a level of detail capable of restricting products from any specific entity. Furthermore, Canadian government officials have not indicated, neither through public statements nor policy proposals, any government plan to secure supply chains. Commentators opine that the silence from high-level officials and the government is indicative of a "do nothing" approach to securing supply chains.[129]

Some attribute the silence to the fact that Canadian intelligence does not have any "cabinet committee dedicated exclusively to S&I [Security and Intelligence] . . . [nor] parliamentary oversight mechanism which can consistently monitor the [intelligence] community."[130] Consistent with this state of affairs, Canada remains the only Five Eyes member to neither ban nor restrict usage of Huawei 5G equipment in its domestic networks.[131]

Canada recently adopted a comprehensive approach to coordinated national security policy. Public Safety Canada (Public Safety) was established "in 2003 to ensure coordination across all federal departments and agencies responsible for national security and the safety of Canadians."[132] Public Safety's Minister, Ralph Goodale, claims the agency is currently examining, "with a great deal of care[,]" the security and technical issues involved, and assures, their final decisions "will not compromise [their] national security."[133]

The department adopted a Cyber Security Strategy 2018 and, in 2019, released a 2019-2024 National Cyber Security Action Plan (Action Plan), which recognized that, for the future innovation and prosperity of Canada, there was a

---

129. Tom Jowitt, *Canada To Be Final 'Five Eyes' Member to Exclude Huawei – Report*, SILICON (Aug. 26, 2020, 11:34 AM), https://www.silicon.co.uk/5g/canada-exclude-huawei-347312#:~:text=Five%20Eyes%20Ban,5G%20equipment%20in%20that%20ban.

130. Dailey, *supra* note 43, at 4.

131. Robert Fife, et al., *Canada is now the Only Five Eyes Member to not Ban or Restrict use of Huawei 5G Equipment*, GLOBE & MAIL (July 15, 2020), https://www.theglobeandmail.com/politics/article-canada-now-only-member-of-five-eyes-alliance-to-have-not-banned-huawei/.

132. *About Public Safety Canada*, (last visited Nov. 12, 2020), https://www.publicsafety.gc.ca/cnt/bt/index-en.aspx.

133. Marrian Zhou, *Canadian Ban on Huawei's 5G Tech will Trigger 'Repercussions,' says China*, CNET (Jan. 18, 2019, 12:11 PM), https://www.cnet.com/news/canadian-ban-on-huaweis-5g-tech-will-trigger-repercussions-says-china/.

robust need for improved cyber security.[134] This Action Plan was to serve as a "blueprint for the implementation of [Canada's 2018] Strategy."[135] The 2018 Strategy addressed Canada's move toward greater cyber security measures by discussing new funding for the Canadian Centre for Cyber Security (Cyber Centre) and the creation of the National Cybercrime Coordination Unit.[136] The Plan, however, like the 2018 Strategy, lacks any discussion on mitigating threats to ICT supply chains.[137]

The Cyber Centre was established in 2018, within the Communications Security Establishment (CSE), by Canada in an attempt to coordinate cyber security expertise and offer guidance and support on cyber security for the private and public sectors.[138] Cyber Centre "leads the government's response to cyber security events [and] work[s] to protect and defend the country's valuable cyber assets[,]" serving as "Canada's authority on cyber security."[139] In 2018, it released a "National Cyber Threat Assessment," which stated efforts would be taken to "help[] mitigate supply chain threats to the telecommunications sector."[140] On closer examination, this assessment was only a set of broad conclusions that did not suggest any substantive methodologies to address ICT SCRM or indicate that any were forthcoming.[141]

The Canadian Security Intelligence Service (CSIS) "is at the forefront of Canada's national security system" with the authority to "take measures to reduce threats to" and investigate "activities suspected of constituting threats to the security of Canada."[142] While CSIS has reportedly pushed for Huawei's ban from Canadian infrastructure, the group has not released formal documentation regarding this stance.[143] The only public statement related to security concerns emanates from an academic outreach workshop—"China and the Age of

---

134. PUB. SAFETY CAN., NATIONAL CYBER SECURITY ACTION PLAN 2019-2024, 3–4, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/ntnl-cbr-scrt-strtg-2019-en.pdf.

135. *Id.*

136. *Id.* at II–III.

137. *Id.*

138. *Id.* at 20–21; *About the Cyber Centre* (last visited Nov. 12, 2020), https://cyber.gc.ca/en/about-cyber-centre. The Communications Security Establishment is a member of Canada's security and intelligence community, which provides the Government with information technology security and foreign signals intelligence services. *About Us*, COMMC'NS SEC. ESTABLISHMENT (last visited Apr. 2, 2021), https://www.cse-cst.gc.ca/en/about-apropos.

139. *About the Cyber Centre*, *supra* note 138.

140. *National Cyber Threat Assessment 2018*, CAN. CTR. FOR CYBER SEC. (last visited Nov. 12, 2020), https://cyber.gc.ca/sites/default/files/publications/national-cyber-threat-assessment-2018-supply-chain-e.pdf.

141. *Id.*

142. *Canadian Security Intelligence Service*, (last visited Nov. 12, 2020) https://www.canada.ca/en/security-intelligence-service.html.

143. *See* Roger Jordan, *Canada's Military Top Brass Joins CSIS in Demanding Huawei Ban*, WSWS (Feb. 12, 2020), https://www.wsws.org/en/articles/2020/02/12/huaw-f12.html.

Strategic Rivalry"—in which CSIS organized but did not participate.[144] The workshop and publication of papers by leading—though unnamed—experts expressed many concerns regarding China's influential role in the development of technology and infrastructure that would, without doubt, penetrate and compromise national security.[145]

The Canadian Security Telecommunications Advisory Committee (CSTAC) was established in 2010 in response to several National Strategies and Action Plans for Critical Infrastructure that "called for government and industry cooperation to ensure the security of Canada's critical infrastructure."[146] CSTAC is comprised of five government members, including but not limited to, Public Safety Canada, Cyber Centre, CSIS, and twelve industry members.[147] CSTAC's mission is to "improve the overall security" of the critical infrastructure in Canadian telecom.[148] CSTAC has released several guidance and best practices papers, but none of these documents carry the force of law nor any weight beyond being informal guidelines. Additionally, as indicated above, none of the government members involved in this Committee have separately regulated with the force of law on ICT supply chains.

Conservative Members of Parliament heavily criticize the lack of governmental action, arguing that, as the only "Five Eyes [nation] to [] not take[] action to mitigate the security risk of using Huawei[,]" this has been "an abject failure on the Trudeau government's part to protect [Canada's] national security," by ultimately threatening the future of Canada's privy to "intelligence-sharing."[149] The leader of the Bloc Québecois argued Canada's reluctance "to ban Huawei" is likely an attempt "to avoid a further strain in relations with China at a time when . . . Chinese trade sanctions" resulted after Canadian forces arrested a Huawei executive officer.[150] Links between Canada's silence on Huawei and political tensions between the two countries are well recognized, with diplomatic sources claiming that "[i]f it weren't for [the arrests], Canada would have already said it would not be using Huawei 5G technology."[151]

---

144. CANADIAN SEC. INTEL. SERV., CHINA AND THE AGE OF STRATEGIC RIVALRY: HIGHLIGHTS FROM AN ACADEMIC OUTREACH WORKSHOP (2018).

145. *Id.* at 65–66, 110. One excerpt reads: CCP leader "Xi Jinping highlighted the country's ambition to transform itself into a 'science and technology superpower[.]'" *Id.* at 125.

146. CAN. SEC. TELECOMM. ADVISORY COMM. (CSTAC), SECURITY BEST PRACTICES FOR CANADIAN TELECOMMUNICATIONS SERVICE PROVIDERS (TSPS) 2 (2013).

147. *Canadian Security Telecommunication Advisory Committee (CSTAC)*, (last visited Jan. 15, 2020), https://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/h_sf10727.html.

148. CAN. SEC. TELECOMM. ADVISORY COMM., *supra* note 146, at 2.

149. Fife, et al., *supra* note 131.

150. *Id.* After Huawei executive Wanzhou was arrested on Canadian soil, Beijing responded by arresting two Canadians and halting agricultural imports from Canada for the following months. *Id.*

151. David Ljunggren, *Canada has Effectively Moved to Block China's Huawei from 5G, but Can't Say so*, REUTERS (Aug. 25, 2020, 12:30 PM), https://uk.reuters.com/article/us-canada-

Canada's inaction is condemned by military officials, who argue allowing Huawei "a role in 5G [will] threaten national security."[152] Public Safety maintains, however, that Canada is closely working and communicating with its Five Eyes partners "to ensure that its approach to strengthening critical infrastructure resilience considers the global context and leverages best practices from trusted allies."[153] Despite these assertions, as of July 2020, a cabinet member stated privately that only one discussion on Huawei had occurred, and nothing indicates Canada will be announcing a path soon.[154]

Many believe the delay in formalizing a decision has resulted in a de facto ban from private networks and that eventually, Canada's "absence of a solution will [] settle all problems."[155] Because "do[ing] nothing" may allow Canada to avoid being at the crossroads between the US and China, some commentators argue this approach is strategic by upsetting neither country.[156] Yet, merely choosing not to adopt a policy as a strategy to upset neither country appears instead likely ineffective, as it may lead the US to place pressure on Canada, thereafter causing havoc for the latter's relationship with China.

Illustrative of this pressure, on the one side, a former Chinese Ambassador to Canada[157] asserted, "[i]f the Canadian government does ban Huawei from participating in the 5G network, then . . . there will be repercussions."[158] On the other side, President Trump asserted, if "countries 'want to do business with us, they can't use' technology from Huawei."[159] U.S. members of Congress have also threatened that intelligence sharing will come to a halt with any country that

---

huawei-analysis/canada-has-effectively-moved-to-block-chinas-huawei-from-5g-but-cant-say-so-idUKKBN25L26S.

152. Stephen Wicary, *Military wants Huawei Banned from 5G in Canada: Report*, BNN BLOOMBERG (Feb. 10, 2020), https://www.bnnbloomberg.ca/military-wants-huawei-banned-from-5g-in-canada-report-1.1387769.

153. PUB. SAFETY CAN., 2018-2020 ACTION PLAN FOR CRITICAL INFRASTRUCTURE 4 (2018).

154. Fife, et al., *supra* note 131.

155. Jowitt, *supra* note 129. Exemplifying these effects, "two of the biggest Canadian mobile operators – Bell Canada and Telus – signed up with Sweden's Ericsson and Finland's Nokia to build 5G networks, dropping Huawei despite using its kit for their 4G networks." *Id.*

156. *Id.*

157. *See* Keegan Elmer, *China's 'Outspoken' Lu Shaye Leaves Canada to Become Ambassador to France*, S. CHINA MORNING POST (Aug. 9, 2019, 11:00 PM), https://www.scmp.com/news/china/diplomacy/article/3022175/chinas-outspoken-lu-shaye-leaves-canada-become-ambassador.

158. Zhou, *supra* note 133.

159. Fife et al., *supra* note 131. With a recent shift from the Trump to the Biden administration, the question remains whether President Biden will adopt his predecessors' approach. While still the early days of Biden's administration, executive efforts thus far remain largely consistent with those under President Trump; some nuances nevertheless exist, such as broader efforts being taken to adopt a more wholistic, comprehensive approach to supply chain security. *See* Justin Sherman, *The U.S. Is Continuing Its Campaign Against Huawei*, LAWFARE (July 20, 2021, 11:58 AM), https://www.lawfareblog.com/us-continuing-its-campaign-against-huawei.

uses Huawei technology.[160] Given Canada's role in the Five Eyes alliance, permitting Huawei to remain in its 5G networks could prove extremely challenging for the future of Canada's intelligence-sharing relationship with the US and, possibly, with the other Five Eyes countries.

Despite Canada's ambiguous policy on ICT SCRM, private industry has begun to shift away from Huawei of its own accord. In June 2020, two of Canada's largest telecom providers, Bell Canada and Telus Corp, announced new 5G telecom deals with Ericsson and Nokia.[161] Rogers Communications, another "dominant [Canadian] telecoms operator" had "already partnered with Ericsson."[162] These three providers account for a substantial portion of 5G telecom contracts in Canada, and none of these contracts involve Huawei for the future of 5G networks.

While the largest Canadian communications providers have shifted away from Huawei, the Canadian government has not yet taken a concrete policy stance on the future of Huawei equipment. Dominant telecommunications providers, rather than government policy, appear to be the force behind the pressure for Canadian providers to opt for non-Huawei products.

4. The European Union

"[D]edicated to achieving a high common level of cybersecurity across Europe[,]" the European Agency for Cybersecurity (ENISA) was established in 2004.[163] ENISA, "strengthened by the EU Cybersecurity Act[,] . . . contributes to EU cyber policy, enhances the trustworthiness of ICT products, . . . [and] cooperates with Member States and EU bodies."[164] In January 2020, ENISA published the EU toolbox of risk-mitigating measures ("the Toolbox").[165] The

160. *See* Sean Keane, *Huwaei Ban timeline: Detained CFO Makes Deal with the US Justice Department*, CNET (Sept. 30, 2021, 8:10 AM), https://www.cnet.com/tech/services-and-software/huawei-ban-timeline-detained-cfo-makes-deal-with-us-justice-department/; *see also* Stephanie Condon, *Senator Unveils Bill to Stop the US from Sharing Intel with Countries using Huawei 5G*, ZDNET (Jan. 9, 2020), https://www.zdnet.com/article/senator-unveils-bill-to-stop-the-us-from-sharing-intel-with-countries-using-huawei-5g/ (discussing Senator Tom Cotton's proposed legislation to prohibit the U.S. from sharing intelligence with any country permitting Huawei 5G equipment within its borders).

161. Moira Warburton & Neha Malara, *Canadian telcos tap Ericsson, Nokia for 5G gear, ditching Huawei*, REUTERS (June 2, 2020, 3:01 PM), https://www.reuters.com/article/us-bell-canada-ericsson-5g/canadian-telcos-tap-ericsson-nokia-for-5g-gear-ditching-huawei-idUSKBN2391ZV.

162. *Id.*

163. *About ENISA – The European Union Agency for Cybersecurity*, https://www.enisa.europa.eu/about-enisa (last visited Feb. 2, 2022).

164. *Id.*

165. NIS Coop. Grp., *Cybersecurity of 5G Networks EU Toolbox of Risk Mitigating Measures*, 3, CG Pub. 01/2020 (Jan. 2020).

Toolbox recommends member states either exclude or restrict high-risk vendors from their core 5G networks.[166]

The Toolbox does not specify which entities qualify as high-risk vendors, leaving the responsibility to member states to make this determination.[167] Critics of this approach argue that, while the EU identified the need to address cyber security very early, it has allowed trading interests with China to prevail over addressing identified security threats.[168] The interplay between policy development and concern for international trade is particularly apparent with Germany, as Germany "is more dependent on foreign trade than many other EU member states."[169]

a. Germany

Germany has adopted regulations with the force of law that nominally strengthen the security standards for companies in ICT infrastructures,[170] but on further examination, the regulations merely create a self-certification regime, whereby suppliers, such as Huawei, declare their trustworthiness as a condition of supplying products for use in German communications networks.[171] While recent reports have discussed proposals for tighter security legislation, for the foreseeable future, the only requirement in force is minimal, and private industry has little incentive to abstain from pursuing relationships and contracts with Huawei.[172]

Adopting stronger requirements is further complicated by the opposing views of the former German Chancellor and other government agencies. The former

166. Luke Baker & John Chalmers, *As Britain bans Huawei, U.S. Pressure Mounts on Europe to Follow Suit*, REUTERS (July 14, 2020, 10:42 AM), https://www.reuters.com/article/us-britain-huawei-europe/as-britain-bans-huawei-u-s-pressure-mounts-on-europe-to-follow-suit-idUSKCN24F1XG. In response to these recommendations, a EU senior diplomat stated that member states raised concerns over these guidelines not reaching "far enough to limit dependence on Huawei, and [that] the [Toolboox's] distinction between 'core' . . . and 'non-core' was 'not as robust' as" anticipated. *Id.*

167. *Id.*

168. *See* Daniel Leisegang, *Knock, Knock! Huawei's there*, THE GER. TIMES (Mar. 2020), http://www.german-times.com/knock-knock-huaweis-there/. With trade volumes amounting to roughly 600 billion euros, trade levels of this magnitude influence the EU's actions given the Union's tremendous interest in not "jeopardizing its relationship with [its] . . . economic partner[,]" China. *Id.*

169. *Id.*

170. Council Directive 2015/1535, of September 17, 2015, Catalogue of Requirements in Accordance with § 109(6), 2015 O.J. (L. 241) [hereinafter Catalogue].

171. *Id.* at § 3.

172. *See* Samuel Stolton, *US Praises German Moves to Sideline Huawei from 5G Networks*, EURACTIV (Jan. 13, 2021), https://www.euractiv.com/section/digital/news/us-praises-german-moves-to-sideline-huawei-from-5g-networks/ (discussing reports surfacing regarding proposals for a two-stage procedure for ensuring 5G network security, "involv[ing] technical tests of components to be used in 5G infrastructure, alongside a 'political assessment' of the trustworthiness of manufacturers").

Chancellor, Angela Merkel, advocated resisting the international and domestic pressures to completely exclude Huawei, stating that even though issues and concerns have "increased substantially," they must "keep trying to find solutions, even if it's a millimeter at a time."[173] Merkel's stance faces public criticism from two major governmental bodies: the German intelligence agencies, claiming Huawei's "ties to the Chinese communist party pose a risk to information security,"[174] and the Chair of the Foreign Affairs Committee of the Bundestag, claiming Germany must recognize Huawei's security risks.[175] Nevertheless, Merkel rejects a blanket ban in favor of "strict security requirements that should be constantly reviewed."[176]

The self-certification regime emanates from September 2020 action of the telecommunications regulatory authority, the Bundesnetzagentur ("Federal Network Agency for Electricity, Gas, Telecommunications, Post, and Railway" or "Federal Network Agency"),[177] which issued a "[c]atalogue of security requirements for operating of telecommunications and data processing systems" in accordance with Section 109 of the Telecommunications Act.[178] The catalogue directs the Federal Network Agency, in consultation with the Federal Office for Information Security, to create guidelines for networks and establish "[a]dditional security requirements for network components with an increased risk potential."[179] It also requires public telecom network operators and providers to "appropriately select manufacturers and sellers or suppliers of critical components before purchasing them[,]" and "obtain a comprehensive

---

173. Patrick Donahue, *Merkel Resists Full Ban on Huawei, Making Germany an Outlier*, BLOOMBERG (Sept. 30, 2020, 6:10 PM), https://www.bloomberg.com/news/articles/2020-09-22/merkel-resists-full-ban-on-huawei-making-germany-an-outlier.

174. *Id.*

175. Patrick Wintour, *Europe Divided on Huawei as US Pressure to Drop Company Grows*, THE GUARDIAN (July 13, 2020, 9:52 AM), https://www.theguardian.com/technology/2020/jul/13/europe-divided-on-huawei-as-us-pressure-to-drop-company-grows.

176. Andrea Thomas, Bundesnetzagentur schließt Huawei nicht pauschal vom 5G-Ausbau aus [*The Federal Network Agency Does not Exclude Huawei from the 5G Expansion Across the Board]*, DOW JONES NEWSWIRES (Aug. 11, 2020, 12:24 PM), https://www.finanznachrichten.de/nachrichten-2020-08/50419271-bundesnetzagentur-schliesst-huawei-nicht-pauschal-vom-5g-ausbau-aus-015.htm&prev=search&pto=aue. Chancellor Angela Merkel's refusal to exclude any single company from the 5G expansion is shared by Peter Altmaier, the Federal Minister of Economics. *Id.*

177. *About the Bundesnetzagentur*, https://www.bundesnetzagentur.de/EN/General/Bundesnetzagentur/About/AboutTheBundesnetzagentur_node.html (last visited Feb 11, 2022).

178. Catalogue, *supra* note 170, at § 2.

179. *Id.* at Annex 2. "The Catalogue of the Bundesnetzagentur has the status of 'soft law,' which means that it is an interpretation of binding statutory law by the Bundesnetzagentur . . . The Bundesnetzagentur . . . mentioned that it can audit the security measures of [networks] affected[.]" Sven-Erik Heun, et. al, *New IT Security Requirements for Telecommunications Services and Networks in Germany*, BIRD & BIRD (Oct. 2019), https://www.twobirds.com/en/news/articles/2019/global/new-it-security-requirements-for-telecommunications-services-and-networks-in-germany.

declaration from the supply source to demonstrate its trustworthiness."[180] While these requirements apply "across all networks and communications infrastructure . . . [and] vendors[,]"[181] it is criticized for "lack[ing] teeth"[182] because its "forensic approach . . . [still] allows for companies like Huawei to operate in the country."[183]

Huawei publicly maintains that it will "'continue to work transparently with regulators, customers[,] and industry organizations' to 'ensure the security of mobile networks.'"[184] Germany's Economic Minister met with Huawei's CEO and stated for the record "that [Germany] expect[s] all operators to fulfill . . . security requirements and that it is now Huawei's duty to show us that they are able to do so."[185] Whether and how Germany enforces that duty remains to be seen.

In late September 2020, reports surfaced regarding the government's move toward a new IT Security Act, "seeking to introduce new rules to ensure the security of 5G networks, that would de facto amount to an 'exclusion' of Huawei."[186] This new IT Security Act, the "IT-SiG 2.0," aims to "clos[e] legal loopholes and expand[] the existing regulatory framework [with an] . . . overarching objective [] to enhance IT security standards by amending several existing German laws."[187] To date, however, the legislation has not been formally proposed, drawing criticism from German lawmakers.[188] The bill, as currently proposed, would create "bureaucratic obstacles that could prove insurmountable" and effectively create "an outright ban on Huawei" as a

180. *Catalogue*, *supra* note 170, at § 3.

181. Jamie Davies, *Germany Outlines its 5G Security Requirements*, TELECOMS (Mar. 8, 2019, 10:44 AM), https://telecoms.com/496135/germany-outlines-its-5g-security-requirements/.

182. Laurens Cerulus, *Why Germany's Huawei Move Irks More than just Washington*, POLITICO (Oct. 16, 2019, 8:05 PM), https://www.politico.eu/article/germany-defies-us-on-huawei/. The President of the Federal Network Agency, Jochen Homann, argues "exclud[ing Huawei] from the market . . . would delay the roll-out of 5G networks." *Germany Pressures Huawei to mMet Security Requirements*, DW (June 21, 2019), https://www.dw.com/en/germany-pressures-huawei-to-meet-security-requirements/a-49294841.

183. Davies, *supra* note 181.

184. Thomas, *supra* note 176.

185. DW, *supra* note 182.

186. Stolton, *supra* note 172.

187. Dr. Detlev Gabel, *Germany's Draft Bill on IT Security 2.0 – Extended BSI Authorities, Stricter Penalties and New Obligations on Providers*, WHITE & CASE (July 12, 2019), https://www.whitecase.com/publications/article/germanys-draft-bill-it-security-20-extended-bsi-authorities-stricter-penalties. Several German laws are expected to be amended, including: the Act on the German Federal Office for Information Security, the German Telecommunications Act, the German Telemedia Act, and the German Criminal Code. *Id.*

188. *See* Laurens Cerulus, *Deutsche Telekom Ender Pressure After Reports on Huawei Reliance*, POLITICO (July 8, 2020, 10:17 AM), https://www.politico.com/news/2020/07/08/deutsche-telekom-huawei-5g-352317.

supplier.[189] Specifically, the bill introduces a two-stage approval process for permissible operations of certain telecom equipment: first, "a technical check of individual components[,]" and second, "a political assessment of the manufacturer's 'trustworthiness.'"[190]

Germany is heavily dependent on Huawei as it "provides about 45% of Germany's 4G base stations and [remains] a leading supplier to phone companies."[191] This includes Deutsche Telekom, in which the German government "holds a 14.5-percent stake."[192] Deutsche Telekom—a global telecom giant based in Germany—contracted with Huawei in 2019, claiming the company was a "strategic partner."[193] The two companies agreed that Huawei would "shoulder the burdens and costs of U.S. security measures taken."[194] Many within the German Parliament expressed concern over these deals, arguing it problematic if "there is indeed a high degree of dependence of [Deutsche] Telekom on Huawei in expanding the 5G network."[195] Despite Deutsche Telekom's willingness to engage with Huawei, Germany's head of foreign intelligence maintains that Huawei "cannot be trusted and should not play a major role" in 5G networks.[196]

Germany's approach to Huawei is nuanced and divided. While rumors remain that Germany could be headed to adopting legislation to exclude Huawei, it appears that full collaboration with Huawei continues with both government and private sectors.

b. Italy

Italy has adopted ICT SCRM regulation with the force of law that requires network operators to take greater security measures and assigns the government "special powers" to impose conditions on transactions deemed threatening to

189. Guy Chazan & Nic Fildes, *Germany Crackdown set to Exclude Huawei from 5G Rollout*, FIN. TIMES (Sept. 30, 2020), https://www.ft.com/content/35197477-acef-4429-a1d8-71743ee8d8e3.

190. *Id.* "In its current form [the bill] envisages that when doubts arise as to a company's trustworthiness then the government can investigate it, using information provided by the intelligence services." *Id.* (alterations in original).

191. DW, *supra* note 182.

192. Laurens Cerulus, *How U.S. Restrictions Drove Deutsche Telekom and Huawei Closer Together*, POLITICO (July 7, 2020, 6:09 AM), https://www.politico.com/news/2020/07/07/deutsche-telekom-huawei-us-restrictions-350252.

193. *Id.* Despite the purported partnership between Huawei and Deutsche Telekom, before any German bill was finalized, the latter company voluntarily began shifting "away from using Huawei systems in the 'core' – the intelligence part of the network where customer information is processed." Chazan & Fildes, *supra* note 189.

194. Cerulus, *supra* note 188.

195. *Id.*

196. Baker & Chalmers, *supra* 166.

national defense and homeland security.[197] To date, however, there has been no action to explicitly exclude Huawei. Rather, Italy's regulatory requirements include vulnerability assessments of companies operating in the communications and technology sectors.[198] Despite this governmental approach, actions of the private industry beckon a shift away from contracting with Huawei for 5G deals.

"Italy is the second largest market for Huawei smartphones,"[199] contributing to robust Italian-Huawei relations.[200] For example, in responding to Italy's economic struggles amidst COVID-19, Huawei's Chief Representative to the European Institutions remarked, "[m]ore than ever, Huawei is committed to its presence in Italy and their digital transformation. 5G [is] key to shaping Italy's economic viability."[201] Correspondingly, in April 2019, Italian Prime Minister Giuseppe Conte assured CEO Zhengfei that Huawei "would not face discrimination in the rollout of Italy's 5G telecoms network."[202]

The Parliamentary Committee for the Security of the Republic, in a public opinion, recommended the government consider preventing specific companies, such as Huawei, from participating in Italy's 5G networks.[203] The Committee stated that excluding particular "companies from the activity of supplying technology for 5G networks" was an appropriate mechanism.[204] By contrast,

197. Baker McKenzie, el al., *The National Cyber Security Perimeter – Italy's Approach to Protecting its Key Communications Infrastructure and Services*, LEXOLOGY (Dec. 20, 2019), https://www.lexology.com/library/detail.aspx?g=169c334b-3e21-40c6-84e2-7105df4cc57c.

198. *See Italy: New Provisions on National Cybersecurity Enter into Force*, LIBR. CONG. L. (Oct. 16, 2019), https://www.loc.gov/law/foreign-news/article/italy-new-provisions-on-national-cybersecurity-enter-into-force/. These new vulnerability factors, designed to guarantee high levels of network security, "include (a) security policies related to organizational structures and risk management, (b) mitigation and management of accidents and their prevention, (c) physical safety and data protection, (d) integrity of networks and information systems, (e) monitoring, testing and control, and (f) training and awareness." *Id.*

199. Giovanna De Maio, *Playing with Fire: Italy, China, and Europe*, BROOKINGS INSTIT. 9 (2020), https://www.brookings.edu/wp-content/uploads/2020/05/FP_20200519_playing_with_fire.pdf.

200. *See* Press Release, *Side by Side with Italy Following Pandemic*, HUAWEI (June 25, 2020), https://www.huawei.eu/press-release/side-side-italy-following-pandemic.

201. *Id.* Huawei's remarks focused heavily on the economic effects Italy faced during the COVID pandemic, and how its 5G technologies could support Italy's economic recovery. *Id.*

202. Mark Bendeich, *Italian PM Assures Huawei it Won't Face Discrimination*, REUTERS (Apr. 26, 2019, 11:39AM), https://www.reuters.com/article/us-italy-huawei-conte/italian-pm-assures-huawei-it-wont-face-discrimination-idUSKCN1S21R7.

203. Pierluigi Paganini, *Negative Opinion of Italy Security Committee Copasir on Huawei, ZTE 5G Solutions*, SEC. AFF. (Dec. 20, 2019), https://securityaffairs.co/wordpress/95424/security/copasir-huawei-ztes.html.

204. *Id.*

the Italian Minister for Industry urges Huawei should "be allowed to play a role in the development of the country's 5G network[s]."[205]

"In November 2019, [Italy] passed law No. 133/2019 (Law 133), which establishe[d] the[] 'National Cyber Security Perimeter' [the "Perimeter"] and amend[ed] the Italian legislation on foreign investments in certain strategic sectors."[206] The goal of Law 133 is ensuring high security for "networks, information systems, and IT services . . . whose failure may harm national security."[207] When establishing the Perimeter, the government must first identify those entities or administrations that are subject to specific security obligations, and second, impose on them duties to notify the Government about any incident affecting such networks.[208] Non-compliance would trigger significant fines and, in some instances, imprisonment.[209] Law 133 also includes a "special powers" amendment, enabling the Government "to impose conditions on . . . certain transactions" in "critical hi-tech infrastructures and 5G technologies" whenever the Government finds the transactions "would result in a threat of serious harm to Italian public interests."[210]

Under the special powers provision, "broadband electronic communication services based on 5G technology" must "notify all 5G-related contracts to the Government, in order for the [government] to assess whether [they must] impose conditions."[211]

In addition to Law 133, in September 2019, the Italian government promulgated Decree Law No. 105 (Decree 105), which contains "urgent provisions on national cybersecurity" with purposes "to guarantee the highest level of security for networks . . . and information technology (IT) services."[212] Decrees are passed by Italian governments in cases of necessity and urgency, which enable the government to adopt "provisional measures having the force of law."[213] Decree 105 states that "regulations must provide for an assessment of vulnerability factors that could compromise the integrity and security of the networks and data of networks with 5G technology."[214]

---

205. Matei Rosca, *Italian Industry Minister Calls for Huawei Access to 5G Network*, POLITICO (Dec. 22, 2019, 3:52 PM), https://www.politico.eu/article/italian-industry-minister-calls-for-huawei-access-to-5g-network/.

206. Baker McKenzie, et al., *supra* note 197.

207. *Id.*

208. *Id.*

209. *Id.*

210. *Id.*

211. *Id.*

212. LIB. CONG. L., *supra* note 198.

213. Marco Gubitosi, et al., *Legal Systems in Italy: Overview*, THOMAS REUTERS PRACTICAL LAW,https://uk.practicallaw.thomsonreuters.com/w-007-7826?transitionType=Default&contextData=(sc.Default)&firstPage=true.

214. LIBR. CONG. L., *supra* note 198.

In the same vein, Law No. 23 (or the "Golden Power Law") was recently expanded to increase screening requirements of various sectors, including communications,[215] in order to offer protections for foreign investments in Italian assets.[216] The Golden Power Law grants the Italian government jurisdiction to review any transaction in the "defense and national security sectors, which may harm or constitute a material threat to the Italian government's essential interests[,]" and in the "communication and high-tech sectors, which may harm or constitute a material threat to the fundamental interests of Italy."[217] Despite its expanded scope, applying this law "is ultimately a matter for political discretion[,]" as Italy does not have "an independent committee to take screening decisions."[218]

In July 2020, Italy's largest telecom provider, Telecom Italia (TIM), excluded Huawei from a tender bidding for 5G equipment for the core network it was building in Italy and Brazil.[219] TIM stated this omission was done "as 'part of [it's] suppliers' diversification policy.'"[220] The invited suppliers included Ericsson, Nokia, and Cisco.[221] Despite its exclusion, the chairman of Huawei's Italian operation claims Huawei is still working with TIM, qualifying their exclusion as merely "a 'commercial' decision, unlike in Britain where he said the Chinese telecoms group's exclusion from 5G services was a 'geopolitical, not a technological decision.'"[222]

---

215. Maio, *supra* note 199 at 10–11.

216. Ferigo Foscari, et al, *COVID-19 – Italy Expands Golden Power Review of Foreign Investments*, WHITE & CASE (Apr. 10, 2020), https://www.whitecase.com/publications/alert/covid-19-italy-expands-golden-power-review-foreign-investments.

217. *Id.* To the extent non-EU persons are involved in transactions, the law grants jurisdiction over "the execution of any agreement relating to the acquisition of assets or services relating to 5G technology infrastructure (or any 5G technology related components)." *Id.*

218. Maio, *supra* note 199 at 11. Based on documentation made publicly available by the Italian government, only twenty-six known procedures have been exercised under the special powers' reviews regarding the subjects of defense, national security, communications, and 5G technologies. Ferigo Foscari, et al., *Foreign Direct Investment Reviews 2020: A Global Perspective – Italy*, WHITE & CASE (Dec. 9, 2020), https://www.jdsupra.com/legalnews/foreign-direct-investment-reviews-2020-44968/. So far these include measures such as approval of safety contingency plans to "monitor strategic assets and operations," monitoring measures such as "independent committees tasked with the duty to monitor" compliance with measures imposed by Italian government, and other technical measures aimed at "preserving the confidentiality of information and the technological know-how of the target." *Id.*

219. Elvira Pollina, *Exclusive: TIM Excludes Huawei from 5G Core Equipment Tender*, REUTERS (July 9, 2020, 10:53 AM), https://www.reuters.com/article/us-huawei-tech-5g-italy-brazil-exclusive/exclusive-tim-excludes-huawei-from-5g-core-equipment-tender-idUSKBN24A2AE.

220. *Id.*

221. *Id.*

222. Reuters, *Huawei Says It's Working With Telecom Italia Despite 5G Exclusion: Paper*, U.S. NEWS (July 20, 2020), https://www.usnews.com/news/technology/articles/2020-07-20/huawei-italy-executive-says-tim-decision-not-political-newspaper.

Overall, although Italy has not officially excluded Huawei, Italy's actions have shifted toward heightened security standards for 5G technological equipment contracts that equip the government with powers capable of imposing conditions on transactions deemed threatening to Italy's security. These standards have reached the point of affecting private industries, as the leading provider TIM has seemingly reacted by excluding Huawei from 5G deals, even though government policy does not officially exclude Huawei equipment from networks.

III. CATEGORIZING THE FIVE NATIONS INTO THREE GROUPS BASED ON SHARED CHARACTERISTICS

Although each nation's supply chain risk mitigation policies are distinct, each nation fits into one of three approaches, categorically including: legislation excluding Huawei, legislation not excluding Huawei, and an absence of legislation addressing supply chain security. Grouping nations based on these categorical approaches helps shed light on the effects international and domestic factors have on the development of ICT SCRM policies.

A. Group One – ICT SCRM Legislation, Completely Exclude Huawei

Countries in Group One, comprised of the US and the UK, have adopted a policy that prohibits Huawei equipment in developing 5G networks. This group exhibits three primary characteristics. First, there is a whole of government approach toward developing policy and law to mitigate ICT supply chain risks. Second, adopted—or imminently expected to be adopted—policy with the force of law targets Huawei explicitly and restricts the use of its equipment in 5G infrastructures. Finally, against tense political overlays, Group One nations adopt firm and stringent international policies toward China.

Policy approaches that are adopted by a "whole of government" strategy facilitate relatively quick passing of legislation and regulation.[223] For example, both the US and UK's whole of government approaches have led to, respectively, promulgation and expected promulgation of legislation and regulation prohibiting or restricting Huawei. Through several government agencies' efforts, the US achieved significant prohibitions on Huawei equipment and continues to undergo policy refinements. One example of this achievement is demonstrated by the regulatory agency, FCC.[224] The FCC is currently implementing a policy that calls for the complete removal and replacement of Huawei equipment purchased with USF subsidies, which tend to involve smaller providers in more rural areas.[225] Similarly, the U.K.'s planned legislative efforts

223. Phillips, et al., *supra* note 99 (discussing the U.S. "whole of government" approach to creating Huawei policy).

224. *See* discussion *infra* Section II.A.1.b.

225. SECOND REPORT AND ORDER, *supra* note 85, at 1, 10–11.

empower its regulatory agency to place conditions on providers regarding which entities are allowed in 5G contracts.[226]

The US, through its executive branch, is treating Huawei as "an unusual and extraordinary threat to . . . national security."[227] Pursuant to an executive order, executive branch agencies, under their delegated authorities, are pursuing policies to secure ICT supply chains.[228] In addition to these executive and regulatory actions, the U.S. Congress enacted legislation explicitly excluding executive agencies from contracting with Huawei for any purpose.[229] Thus, through congressional as well as regulatory and executive action, the government has comprehensively restricted Huawei's presence.

In a similar vein, the U.K.'s Prime Minister, Boris Johnson, stated his intent to remove Huawei equipment from U.K. systems by 2027.[230] These plans echo the US's removal and replacement policies. Additionally, they demonstrate the UK's collaborative whole of government approach to securing ICT supply chains, given that both the head of government plans for Huawei's exclusion and legislative efforts to exclude Huawei are complementary.[231]

US and UK laws, either expected or currently in force, demonstrate zero tolerance for Huawei equipment. These policy efforts also shed light on the influence government action can have on private providers, even absent direct regulation on private providers. For example, although the UK presently has no enforceable law regulating Huawei equipment, a U.K. mobile operator nevertheless voluntarily decided not to contract with Huawei for its 5G technology.[232] Thus, even absent enacted law, the UK has arguably reached the point where private providers are wary of contracting with Huawei. Considering the passage of the US's NDAA FY21, US providers will also likely exercise similar caution, especially given the advent of Open RAN technology and the possibility of federally funded grants to support this choice of technology.[233] In turn, this development will likely result in the private industry's voluntary exclusion of Huawei in the US.

The impact of delicate political situations involving Chinese relations with both the US and UK have arguably impacted ICT SCRM policies. In the US, the former Trump Administration adopted a series of tough trade policies on China and Chinese companies in several sectors, including

226. DEP'T FOR DIGIT., CULTURE, MEDIA & SPORT, *supra* note 100, at 6–7.
227. Exec. Order No. 13873, *supra* note 56, at 22689.
228. *Id.* at 22690; discussion *infra* II.A.1.
229. *See* discussion *infra* II.A.1.a.
230. Seidel, *supra* note 106.
231. *See id.*
232. Devanesan, *supra* note 128.
233. *See* NDAA FY21, *supra* note 91, at § 9202(a)(1)(C)(ii).

telecommunications.[234] Similarly, there is evidence that the U.K.'s shift toward stricter Huawei policy was prompted by the political changes brought by US actions regarding Huawei.[235] On top of this, though it is difficult to prove a direct linkage, the UK's policy shift toward restricting Huawei aligns temporally with the escalating tensions between China and the UK regarding political and economic freedom in Hong Kong.[236]

In summary, Group One's policies are effectuated through a whole of government approach because various members and sectors of the governments agree on the broad policy approach to restricting Huawei's presence. The political overlay of each nation has led to the adoption of stringent policies mitigating Chinese-related threats. As a result, ICT supply chain legislation—either promulgated or expected—would exclude Huawei equipment from 5G infrastructures.

B. Group Two—ICT SCRM Legislation, No Official Exclusion on Huawei

Countries in Group Two, comprised of Italy and Germany, have no official policy excluding Huawei. The countries exhibit three primary characteristics. First, unlike the whole of government approach in Group One, the positions advanced by government agencies and officials are inconsistent regarding the appropriate role for Huawei.[237] Second, ICT SCRM methodologies are composed of vetting processes to certify trustworthiness and operability in networks.[238] Finally, unlike Group One where the overlay of political climates encourages them to adopt tougher policies, Group Two nations' political overlays discourage the nations from being overly tough towards China.[239] Thus, they have not yet, nor do they appear likely to in the future, pursue policy explicitly excluding Huawei.

Discordant approaches regarding the proper role for Huawei are exhibited by contrasting statements issued by the former German head of government, Merkel, and the German head of foreign intelligence. Merkel's statements emphasize that, although Germany has no intention of excluding Huawei from their networks, they instead aim to find alternative ways to assure adequate supply chain security.[240] Contrastingly, the head of intelligence emphasizes that

234. *See* Hass & Denmark, *supra* note 60 (discussing the "war on trade" with China); *see* Macias, *supra* note 61 (discussing how former President Trump urged nations to hold China accountable for the Coronavirus pandemic).

235. Gold, *supra* note 108 (explaining that United Kingdom's Digital and Culture Minister, Oliver Dowden, stated the new U.S. sanctions imposed on Huawei "significantly changed" the landscape, such that the "UK [could] no longer be confident" that Huawei equipment could supply its 5G equipment.)

236. *See* Yip, *supra* note 111.

237. *See infra* Sections II.A.4.a–b.

238. *See infra* Sections II.A.4.a–b.

239. *See infra* Sections II.A.4.a–b.

240. Donahue, *supra* note 173.

Huawei definitively "cannot be trusted" nor "should [it] play a major role" in Germany's networks.[241]

This tension between the leaders within the German government parallels that within Italy. On the one hand, both the Italian Prime Minister and Italian Minister for Industry are on record as not supporting the singling out of Huawei, [242] and that instead, Huawei should "be allowed to play a role in" Italian 5G networks.[243] On the other hand, the Parliamentary Committee for the Security of the Republic is on record saying the opposite, specifically that certain companies, such as Huawei, should be excluded from "supplying technology for 5G networks."[244]

Without more congruity of viewpoints among government actors regarding the extent to which 5G deployment is linked to national security policy and the level of threat posed by Huawei, it seems unlikely that ICT SCRM policies in Germany and Italy will develop to the point of singling out and excluding any particular entity. This prediction is reflected through legislation and regulations adopted by both Italy and Germany that take incremental, bureaucratic approaches.

Germany has moved toward adopting IT-SiG 2.0, which would create a regulatory framework in German law designed to ensure 5G network security.[245] This bill's proposal to require both a technical check and a political assessment[246] contrasts with the approach taken by the Federal Network Agency's catalogue, which requires providers to obtain a supply source's self-declaration of trustworthiness.[247] Even though neither of these approaches excludes, or even restricts, Huawei, the contrast between these views demonstrates the increasing tensions within the government regarding the lack of a unified approach, blocking the path for a cohesive national strategy. In fact, the two approaches would likely yield opposite results. On the one hand, under the proposal envisaged by IT-SiG 2.0, Huawei would likely be de facto banned, assuming it were to fail either technical or political assessment. On the other hand, under the catalogue, Huawei would likely be permitted in intrastate networks, assuming it were to simply declare itself trustworthy. Because different approaches could produce vastly different results for the future of Huawei, it seems problematic that there is a lack of unity among the critical proposals.

Similarly, differing views and tension exist within the Italian government. Italian laws have addressed government vetting of 5G-related contracts,[248] new

241. Baker & Chalmers, *supra* note 166.
242. Bendeich, *supra* note 202.
243. Rosca, *supra* note 205.
244. Paganini, *supra* note 203.
245. Gabel, *supra* note 187.
246. *Id.*
247. Catalogue, *supra* note 170.
248. *See* Baker McKenzie, *supra* note 197.

vulnerability factor assessments for supply sources,[249] and governmental review of national security-related transactions.[250] These legal efforts demonstrate the government's expansion of ICT SCRM policy framework, but they also demonstrate the lack of a unified approach. This finding is demonstrated through assigning vague powers and vulnerability factor assessments in policy, rather than including any controversial language or naming specific entities, as the Parliamentary Committee for the Security of the Republic would seemingly prefer.[251]

Arguably, both Italy and Germany are giving greater credence to economic factors in dealing with Huawei than the US or UK. Huawei's smartphone market in Italy[252] and commitment to supporting Italy's 5G deployment have generated Italian dependence on Huawei products.[253] This resulting reluctance to take a harsher stance in its relationship with China reflects in its approach toward Huawei. Similarly, Germany is already heavily dependent on Huawei products in its 4G network[254] and on China for much of its foreign trade.[255] Thus, any effort to adopt regulation or law targeting Huawei poses a significant economic challenge, more significant than in the US or UK.

C. Group Three—No Official Action on ICT SCRM, No Official Stance

Group Three is comprised of Canada, which has not developed an ICT supply chain policy.

Despite criticism for not affirmatively choosing a policy direction on Huawei,[256] Canada has remained silent regarding whether it will develop or integrate ICT SCRM policies.[257] Unlike Group Two's internal political tensions, Group Three is beset with external pressure from two superpowers to adopt policy regulating Huawei's role in 5G technologies. China has threatened Canada that if Canada adopts any version of a ban on Huawei, Canada will face "repercussions."[258] Canada likely views such threats as significant, given that China retaliated against Canada when Canada acted against China's best interests.[259] Meanwhile, the US's threats to revoke business deals with Canada

249. *See* LIBR. CONG. L., *supra* note 198.

250. *See* Foscari, et. al, *supra* note 216.

251. *See id.* (demonstrating the vague powers and factor assessments).

252. *See* Maio, *supra* note 199, at 9.

253. *See* HUAWEI, *supra* note 200.

254. Cerulus, *supra* note 182 (explaining that Huawei equipment comprises 45% of Germany's 4G base stations).

255. *See* Leisegang, *supra* note 168.

256. *See* Wicary, *supra* note 152.

257. *See* Fife, et al., *supra* note 131.

258. Zhou, *supra* note 133.

259. *See* Ljunggren, *supra* note 151 (explaining that after Canada arrested a Huawei executive on its soil, Canada retaliated against the nation by arresting two Canadians in China, and halting Canada's agricultural imports to China).

if it does not agree to exclude Huawei from its networks are also significant. Of all five countries examined, Canada's posture appears to be influenced by external political threats rather than internal national security or economic concerns.[260]

Faced with this dilemma, Canada is unwilling to take action to signal a direction. Absent a supervening event—such as the discovery of a major security breach attributed to Huawei and/or the Chinese government directly—Canada seems unlikely to move forward anytime soon on ICT SCRM.

D. Implications for the Future – Is There Another Way?

Although governments have adopted different ICT SCRM policies, generally, and different approaches to Huawei, specifically, private industry has begun to voluntarily shift away from Huawei. Arguably, this shift is motivated by (1) a sense that restrictions on Huawei are imminent, and (2) presently enforceable restrictions on Huawei equipment, which at least in the case of the US, are augmented by the appropriation of funds to remove Huawei equipment and develop instead, Open RAN technology. For example, a provider based in a Group One country, Vodafone, officially announced its decision to find alternatives to Huawei equipment, turning instead to Open RAN technology.[261] Similarly, a provider under Group Two, Telecom Italia, excluded Huawei from participating in its 5G tender deals.[262] Group Three's most dominant providers, Bell, Telus, and Rogers Communications, likewise announced a partnership with Ericsson and/or Nokia for their 5G networks.[263] Across all three groups, private industry is increasingly finding that it is in their interest to find ways to deploy 5G without—or at least greatly reduced—influence from Huawei.

Action by the private industry may be needed to result in effective and efficient exclusions of Huawei from 5G networks. Although some governments have decided to exclude Huawei in 5G networks, the results may not be seen until as late as 2027,[264] with some partial expenses estimated at $1.6 billion.[265] The financial cost and logistical speed with which the government can implement restrictions on Huawei are, respectively, enormous and slow.

If international providers place heavier emphasis on developing and adopting Open RAN measures, then private industry action offers not only a quicker avenue to excluding Huawei than legislation is capable but also a necessary avenue. This result is because many government actions are incapable of

260. Fife, et al., *supra* note 131.

261. Devanesan, *supra* note 128; *see also* discussion *infra* Section II.A.1 (discussing how similarly, U.S. providers AT&T and Verizon, pursuant to pressure imposed by various members of Congress, withdrew from previous agreements to contract with Huawei for 5G smartphones).

262. Pollina, *supra* note 219.

263. Warburton & Malara, *supra* note 161.

264. Seidel, *supra* note 106.

265. James, *supra* note 86.

completely regulating private industries' purchases, and even where they do, such regulations are bogged down by arduous and lengthy processes.

CONCLUSION

As network providers move forward with acquiring cost-effective and high-quality 5G equipment, the attractiveness of Huawei equipment has pushed countries to address issues involving ICT SCRM. Several nations have adopted distinct approaches to mitigating ICT supply chain threats. Five of these nations are selected from the Fourteen Eyes allied nations and are discussed in detail regarding their respective methodologies. The US, UK, Canada, Italy, and Germany all have distinct policies, but the policies nevertheless illustrate three general ICT SCRM approaches regarding Huawei. Nations have (1) promulgated law excluding Huawei, (2) promulgated law improving security measures but not explicitly excluding Huawei, or (3) undertaken no efforts to promulgate ICT SCRM policy.

Domestic policies are influenced by a variety of factors. These aspects include whether the entirety of the government agrees on the proper role for Huawei and whether political climates encourage nations to develop tough stances on China. These factors have influenced the five nations, in varying ways, and have resulted in the three general approaches toward ICT SCRM policy. The US and UK have promulgated, or are expected to promulgate, bans on Huawei with the force of law. Italy and Germany have promulgated generalized security standards with the force of law that does not explicitly ban Huawei. Finally, Canada has not adopted any ICT SCRM measures, nor has implied plans to do so, indicating the desired role for Huawei in its 5G networks.

Regardless of which general approach governments fall within, the private sector within each of the examined groups has begun to assume an increasingly significant role for the future of reducing supply chain risk. Across the nations, private providers have begun shifting away from Huawei equipment in new 5G deals, opting instead for alternative vendors or technologies. This shift in the private industry suggests that private action may have more of an immediate influence on Huawei's future than any governmental action.

As ICT security threats continue to evolve, nations must frequently reassess the proper prioritization of national security concerns against the quick deployment of 5G technology. Presently, Huawei poses the most significant threat to ICT SCRM, and companies and nations have thus focused on defining its appropriate role. Yet, as new threats develop, nations will continue to find themselves considering whether other Chinese entities offer trustworthy equipment given that "there is nearly zero daylight [existing] between the communist government of China and its 'companies.'"[266] Whether it be governments or private industries leading the way, various international efforts are beginning to pave the path for an alternative to Huawei.

---

266. STATEMENT OF COMMISSIONER MICHAEL O'RIELLY, *supra* note 1.