DRAFT IN PROGRESS: Contact Grant W. Turner at turnergw@mail.uc.edu if interested in publishing

5G and International Security: How the UK can Lead the Way

By: Russell Huang and Grant W. Turner

Abstract/Summary: The current debates revolving around 5G, Huawei, and how they are resolved, are highly visible indicators of the technology based shifts in the global order which are setting the tone for the 21st century. Currently, it seems that many in the US and the PRC are using Cold War and Thucydides Trap paradigms, with a zero-sum mentality. At least in the case of 5G technology, the UK seems to have taken a more nuanced approach.

This article comes as the UK prepares its new National Cyber Security Strategy, reviewing the 5G and cyber security debates surrounding Huawei in a highly interdisciplinary manner, and directing readers to a rich variety of resources. In addition to its analysis of issues and solutions often absent from the discourse, this article's feature contribution is the argument that the UK can be more than an example of a middle way. Specifically, if the UK scales up and internationalizes its Huawei Cyber Security Evaluation Center, perhaps by creating an International Cyber Security Evaluation Center, it can lead its allies and the world in 5G, 6G, cybersecurity, and international relations, filling a vital leadership vacuum.

*-**Russell Huang** is pursuing a BSc in Security and Crime Science at University College London. He has completed internships with CybSafe and the Centre of Excellence for National Security (CENS), a unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore.*

*-**Grant W. Turner** has a M.A. in Educational Studies with a focus on social change via participatory action research, and a Bachelor of Interdisciplinary Studies focusing largely on topics relating to international relations, both from the University of Cincinnati.*

-Both authors attended the Cambridge Security Initiative's International Security and Intelligence 2019 Summer Program and Conference.

Table of Contents

There are strong arguments to be made that the actor(s) controlling emergent (information) technologies such as artificial intelligence, quantum computing, and 5G technologies, will control the world[1]. 5G is the next generation of wireless communication. It will enable higher speeds of data transfer and the integration of virtually all technology, aka the Internet of Things (IoT) [2].

Huawei[3], a telecommunications company based in the People's Republic of China (PRC), is the global leader in 5G infrastructure[4] and phone production as of January 28, 2020[5]. However, its increasing centrality to global infrastructure[6] and its obligations to the PRC[7] have made it the focus of economic and security concerns[8], particularly for liberal democracies[9]. Simply put, "5G will be … the central nervous system of the 21st-century economy—and if Huawei continues its rise, then Beijing"[10], may control it.

The United States (US) has moved from restricting to banning Huawei, recently filing a

---

[1] Graham Allison, "Is China Beating America to AI Supremacy?," *The National Interest*, December 22, 2019, https://nationalinterest.org/feature/china-beating-america-ai-supremacy-106861; Theresa Hitchens, "US Risks Losing 5G Standard Setting Battle to China, Experts Say," Networks/Cyber. *Breaking Defense*, May 11, 2020, https://breakingdefense.com/2020/05/us-risks-losing-5g-standard-setting-battle-to-china-experts-say/.

[2] Tom Wheeler, "5G in Five (not so) Easy Pieces" Report, The Brookings Institution, July 9, 2019, https://www.brookings.edu/research/5g-in-five-not-so-easy-pieces/; Scott Fulton III, "What is 5G? The Business Guide to Next-Generation Wireless Technology," How 5G Will Transform Business, *ZDNet*, September 19, 2019, https://www.zdnet.com/article/what-is-5g-the-business-guide-to-next-generation-wireless-technology/; Klint Finley, "The WIRED Guide to 5G." WIRED. December 18, 2019. https://www.wired.com/story/wired-guide-5g/.

[3] Karishma Vaswani, "Huawei: The Story of a Controversial Company," *BBC News*, March 6, 2019, https://www.bbc.co.uk/news/resources/idt-sh/Huawei.

[4] Will Townsend, "Who is 'Really' Leading in Mobile 5G, Part 6: Policy, Regulation and Consortia," *Forbes*, October 12, 2019, https://www.forbes.com/sites/moorinsights/2019/10/12 /who-is-really-leading-in-mobile-5g-part-6-policy-regulation-and-consortia/#6f08dffd2755.

[4] Abrar Al-Heeti, "Huawei is the World's Top 5G Phone Vendor, Analyst Says" *CNET*, January 28, 2020, https://www.cnet.com/news/huawei-is-the-worlds-top-5g-phone-vendor-analyst-says/.

[6] Daniel Araya, "Huawei's 5G Dominance in the Post-American World," *Forbes*, April 5, 2019, https://www.forbes.com/sites/danielaraya/2019/04/05/huaweis-5g-dominance-in-the-post-american-world/#47d130c748f7.

[7] Samantha Hoffman and Elsa Kania, "Huawei and the Ambiguity of China's Intelligence and Counter-Espionage Laws," *The Strategist*, September 13, 2018, https://www.aspistrategist.org.au /huawei-and-the-ambiguity-of-chinas-intelligence-and-counter-espionage-laws/.

[8] Andrew Eversden, "China's 5G Tech is a National Security Issue … or is it a Trade One?," *C4ISRNET*, February 28, 2020, https://www.c4isrnet.com/show-reporters/rsa/2020/02/28 /huaweis-a-national-security-issue-or-is-it-a-trade-issue/.

[9] Steven Feldstein, "When it Comes to Digital Authoritarianism, China is a Challenge – But Not the Only Challenge," *War on the Rocks*, February 12, 2020, https://warontherocks.com/2020/02 /when-it-comes-to-digital-authoritarianism-china-is-a-challenge-but-not-the-only-challenge/.

[10] Keith Johnson and Elias Groll, "The Improbable Rise of Huawei: How did a Private Chinese Firm come to Dominate the World's Most Important Emerging Technology?," *Foreign Policy*, April 3, 2019, https://foreignpolicy.com/2019/04/03/the-improbable-rise-of-huawei-5g-global-network-china/.

new slew of criminal charges against it[11]. It's also pressuring others to follow suit, with mixed, if not counterproductive, results[12]. As nations navigate the possible shift[13] from a US led unipolar world[14] to possible bipolar[15], multipolar[16], nonpolar[17], or PRC led[18] worlds, all eyes[19] are on the two superpowers.

The core-periphery nature of great power competition mirrors the core-periphery nature of 5G competition. Thus, debates revolving around 5G, Huawei, and how they are resolved, are highly visible indicators of the technology based shifts in the global order, setting the tone for the 21st century. Many in the US and the PRC are using Cold War and Thucydides Trap paradigms, with zero-sum mentalities[20]. This is unnecessary, counterproductive, and dangerous[21].

---

[11] Sean Keane, "Huawei Ban Timeline," *CNET,* Accessed April 17, 2020 (updated regularly), https://www.cnet.com/news/huawei-ban-full-timeline-us-government-china-trump-security-threat-5g-p40/.

[12] Panettieri, Joe. "Huawei: Banned and Permitted in Which Countries? List and FAQ." ChannelE2E and After Nines Inc. Accessed March 10, 2020. https://www.channele2e.com/business/enterprise/huawei-banned-in-which-countries/; Thomas D. Lairson, David Skidmore, and Wu Xinbo, "Why the US Campaign Against Huawei Backfired," Trans-Pacific View, *The Diplomat*, May 13, 2020, https://thediplomat.com/2020/05/why-the-us-campaign-against-huawei-backfired/.

[13] Peter Harris, "When Will the Unipolar World End?: Hegemony is Premised on Dominance in Asia and Europe," *The National Interest,* May 27, 2019, https://nationalinterest.org/feature/when-will-unipolar-world-end-59202.

[14] Nathan A. Sears, "China, Russia, and the Long 'Unipolar Moment': How Balancing Failures are Actually Extending US Hegemony," *The Diplomat*, April 27, 2016, https://thediplomat.com/2016/04/china-russia-and-the-unipolar-moment/.

[15] Andrew A. Michta, "The Global Realignment: Bipolarity is Back," *The American Interest*, January, 17, 2020, https://www.the-american-interest.com/2020/01/17/bipolarity-is-back/.

[16] Mark Y. Rosenberg, "Experts Get Multipolarity All Wrong," *Foreign Policy,* June 24, 2019, https://foreignpolicy.com/2019/06/24/experts-get-multipolarity-all-wrong/.

[17] Richard N. Haass, "The Age of Nonpolarity: What Will Follow U.S. Dominance," *Foreign Affairs*, May/June, 2008, https://www.foreignaffairs.com/articles/united-states/2008-05-03/age-nonpolarity.

[18] Bradley A. Thayer and John M. Friend, "The World According to China: Understanding the World China Seeks to Create by 2049, When the PRC Turns 100," *The Diplomat*, October 3, 2018, https://thediplomat.com/2018/10/the-world-according-to-china/; Robert D. Kaplan, "America Must Prepare for the Coming Chinese Empire," *The National Interest*, June 17, 2019, https://nationalinterest.org/print/feature/america-must-prepare-coming-chinese-empire-63102.

[19] Laura Silver, Kat Devlin, and Christine Huang, "China's Economic Growth Mostly Welcomed in Emerging Markets, but Neighbors Wary of its Influence," Pew Research Center: Global Attitudes and Trends, The Pew Charitable Trusts, December 5, 2019, https://www.pewresearch.org/global/2019/12/05/chinas-economic-growth-mostly-welcomed-in-emerging-markets-but-neighbors-wary-of-its-influence/; Lindsey Ford, "Refocusing the China Debate: American Allies and the Question of US-China "Decoupling," Blog—Order from Chaos, The Brookings Institution, February 7, 2020, https://www.brookings.edu/blog/order-from-chaos/2020/02/07/refocusing-the-china-debate-american-allies-and-the-question-of-us-china-decoupling/.

[20] Robert D. Kaplan, "Why the U.S.-China Cold War Will Be Different," *The National Interest*, January 19, 2020, https://nationalinterest.org/blog/buzz/why-us-china-cold-war-will-be-different-114986; Catherine Wong, "Thucydides Trap Author Graham Allison says China and US Must Work Together and Not End Up on Path that Leads to War," Diplomacy, *South China Morning Post*, December 20, 2018, https://www.scmp.com/news/china/diplomacy/article/2178905/thucydides-trap-author-says-china-and-us-must-work-together-and; Ben Lowsen, "Does

As Henry Kissinger argues, conflict between the PRC and the West, "is a choice, not a necessity"[22]. Mutual misunderstandings and biases are foundational to their conflicts[23]. These not only undermine cooperation and positive competition, but also peace, deterrence, and de-escalation, particularly in the cyber realm. Further, these factors increase the risk of unintentional conflict[24]. A potential geopolitical and technological repeat of WWI can and must be avoided[25].

Addressing these challenges in part requires that we assess and improve the current state of 5G cyber security politics. Dr. Myriam Dunn-Cavelty and Dr. Andreas Wenger state that cyber security politics is a function of the spheres of science, politics, and technology[26]. Building on an unpublished essay written by Russell Huang in 2019, our qualitative exploration of 5G cyber security politics focuses on the UK's policy approach to Huawei and the PRC, situated within the context of global cyber security politics. Guiding the exploration are two questions:

- Should Huawei be allowed to develop 5G communications within the UK?
- Are there challenges, opportunities, and solutions largely ignored or missing from the 5G and cyber security politics discourse, whether concerned with the UK or the world?

Sino-US Competition Mean a Zero-Sum Game?: It May, but it Doesn't Have to," *The Diplomat*, January 3, 2019, https://thediplomat.com/2019/01/does-sino-us-competition-mean-a-zero-sum-game/.

[21]Dani Rodrik, "Capitalism with US and Chinese Characteristics can Peacefully Coexist – If we Give Up on 'Hyper-Globalism'," Comment—Opinion, *South China Morning Post,* April 12, 2019, https://www.scmp.com /comment/insight-opinion/article/3005674/capitalism-us-and-chinese-characteristics-can-peacefully; Taylor M. Fravel, J. Stapleton Roy, Michael D. Swaine, Susan A. Thornton, and Ezra Vogel, "China is Not an Enemy," Opinions, *The Washington Post*, July 3, 2019, https://www.washingtonpost.com/opinions/making-china-a-us-enemy-is-counterproductive/2019/07/02/647d49d0-9bfa-11e9-b27f-ed2942f73d70_story.html.

[22] Henry A. Kissinger, "The Future of U.S.-Chinese Relations: Conflict Is a Choice, Not a Necessity," *Foreign Affairs*, 91, no. 2 (2012): 44, https://www.jstor.org/stable/23217220.

[23] Josh Kerbel, "Thinking Straight: Cognitive Bias in the US Debate About China," *Studies in Intelligence* 48, no. 3 (2004): 27-35, https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol48no3/pdf/v48i3a03p.pdf; Eric C. Anderson, *China Restored: The Middle Kingdom Looks to 2020 and Beyond*, Santa Barbara, California: Praeger, 2010; Kenneth Lieberthal and Wang Jisi, "Addressing U.S.-China Strategic Distrust," in *John L. Thornton China Center Monograph Series*, no. 4 (Washington D.C.: The Brookings Institution, 2012), https://www.brookings.edu/wp-content/uploads/2016/06/0330_china_lieberthal.pdf.

[24] Eric C. Anderson, *Sinophobia: The Huawei Story*, CreateSpace Independent Publishing Platform, 2013; Clay Wilson and Nicole Drumhiller, "US-China Relations: Cyber Espionage and Cultural Bias," In *National Security and Counterintelligence in the Era of Cyber Espionage*, edited by Eugenie de Silva, 28-47, Hershey, PA, US: Information Science Reference, 2016; Michael Kolton, "Interpreting China's Pursuit of Cyber Sovereignty and Its Views on Cyber Deterrence," *The Cyber Defense Review* 2, no. 1 (2017): 119-54, www.jstor.org/stable/26267405.

[25] Evan Osnos, "The Future of Americas Contest with China," A Reporter at Large, *The New Yorker*, January 6, 2020, https://www.newyorker.com/magazine/2020/01/13/the-future-of-americas-contest-with-china.

[26] Myriam Dunn-Cavelty and Andreas Wenger, "Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science," *Contemporary Security Policy* 41, no. 1 (2020): 5-32, https://doi.org/10.1080/13523260.2019.1678855.

We begin by examining the intersection of cyber security politics, theories of international relations, and the PRC, reviewing Huawei's history, and situating Huawei in the current global political environment. We then evaluate Huawei's 5G relationship with the United Kingdom (UK). This is done by addressing the five principal threats Huawei presents, as we've identified in the literature:

- Huawei's potential to install backdoors for the PRC
- Poor source code
- The risk that Huawei might hold a monopoly over 5G
- The future implications for power when 5G is fully commercialised
- Impacts on UK-US relations, particularly intelligence sharing

After analyzing these threats we explore and propose opportunities, challenges (particularly risks posed by alternative vendors), and solutions that are not commonly or adequately addressed, if at all, in the 5G debate. Two primary conclusions are reached.

The first is that Huang's 2019 essay's conclusion, that for the UK the best course of action is a risk mitigation approach, allowing Huawei to conditionally develop its 5G with oversight, seems to hold. Not working with Huawei is counter-productive. Working with Huawei allows the UK to reap the benefits of Huawei's services while addressing its risks. Further, avoidance of risks does not diminish the threat to the UK or advance its position; proactively confronting risks is the best risk mitigation strategy[27].

Second, having already adopted a proactive culture, in general and with Huawei, the UK's approach to 5G may serve as a blueprint for broader strategies and tactics concerning the world's relationships with Huawei and the PRC. In particular, if the UK scales up its Huawei Thus, as the UK prepares its new National Cyber Security Strategy, with its current one ending in 2021[28], this article argues that the UK is well positioned to take the lead in 5G, 6G[29], cybersecurity, and international relations, particularly in the context of faltering US leadership.

---

[27] "5G Round-Up: A Round-Up of Published NCSC Content Following the UK Government's 5G Announcement," NCSC, January 31, 2020, https://www.ncsc.gov.uk/information/5g-round-up.

[28] "National Cyber Security Strategy 2016-2021," Policy Paper, HM Government, November 1, 2016, https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021; "National Cyber Security Strategy 2016-2021: Progress Report," Policy Paper, Cabinet Office, HM Government, May 31, 2019, https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021-progress-so-far; Conrad Prince and James Sullivan, "The UK Cyber Strategy: Challenges for the Next Phase," Briefing Papers, RUSI, June 27, 2019, https://rusi.org/publication/briefing-papers/uk-cyber-strategy-challenges-next-phase.

[29] Andy Boxall, "What is 6G? It Could Make 5G Look Like 2G, but it's Not Even Close to Reality," Mobile, *Digital Trends*, February 3, 2020, https://www.digitaltrends.com/mobile/what-is-6g/; Iain Morris, "A 6G Arms Race May Define the 2020s," 6G, *Light Reading*, February 4, 2020, https://www.lightreading.com/6g/a-6g-arms-race-may-define-the-2020s/a/d-id/757268.

Part One—Background

Huawei's Rise

Huawei was founded in 1987 by Ren Zhengei, who left his position in 1984 as an engineer and possible intelligence officer in the PRC's People's Liberation Army (PLA)[30], just a few years after the PRC began its market reforms under Deng Xiaoping in 1978[31]. It was in this context that he began his entrepreneurial path, studying the West and attempting small business forays[32]. With the help of a few associates (possibly military and intelligence affiliates) Huawei began in the budding tech hub of Shenzhen by selling, and then developing and producing, phone equipment.

This eventually led to a major P.L.A. contract in the 1990s. By 1995 Huawei's domestic sales were reportedly around $220 million USD. In 1996 it was granted the status of a "national champion"[33], protecting it from foreign competition and significantly boosting its success. In 2000 it began expanding internationally, and by 2005 its international sales surpassed its domestic sales.

Over the next decade Huawei expanded rapidly, particularly in Europe, partnering with or buying into a wide variety of major international telecommunications and technology companies[34]. Its growth attracted attention. Going back to at least 2007, the US's NSA began hacking Huawei, both to spy on officials in the PRC and to have backdoor access to all who bought Huawei's products[35]. By 2011, it was selling products and services in over 140 countries, and by 2012 it had become the, "largest telecommunications equipment maker in the world in terms of revenue"[36]. Since 2016 it has been represented in over 170[37] of the 195-196[38] countries.

---

[30] Norman Pearlstine, David Pierson, Robyn Dixon, David S. Cloud, Alice Su, and Max Hao Lu, "The Man Behind Huawei," *The Los Angeles Times*, April 10, 2019, https://www.latimes.com/projects/la-fi-tn-huawei-5g-trade-war/.

[31] Yu Jie and Joeseph Barnsley, "From Deng to Xi: Economic Reform, the Silk Road, and the Return of the Middle Kingdom," Special Report (023), LSE IDEAS, May, 2017, http://www.lse.ac.uk/ideas/Assets/Documents/reports/LSE-IDEAS-From-Deng-to-Xi.pdf.

[32] Vaswani, "Huawei: The Story".

[33] Thomas A. Hemphill and George O. White III, "China's National Champions: The Evolution of a National Industrial Policy – Or a New Era of Economic Protectionism?," *Thunderbird International Business Review* 55, no. 2 (March/April 2013), DOI: 10.1002/tie.21535.

[34] "Milestones – About Huawei," Accessed February 20, 2020, https://www.huawei.com/en/about-huawei/corporate-information/milestone.

[35] David E. Sanger and Nicole Perlroth, "N.S.A. Breached Chinese Servers Seen as Security Threat," Asia Pacific, *The New York Times*, March 22, 2014, https://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html?partner=rss&emc=rss&_r=1.

[36] Gong, Yeming. *Global Operations Strategy: Fundamentals and Practice*. Berlin: Springer-Verlag, 2013, pp. 62.

[37] "Milestones – About Huawei".

[38] Depending on how you count Taiwan, See: Matt Rosenberg, "The Number of Countries in the World," Geography, *ThoughtCo*, DotDash Publishing Company, February 27, 2020, https://www.thoughtco.com/number-of-countries-in-the-world-1433445.

5G and Huawei

However, due to real and anticipated behaviors, Huawei's rise has raised alarms[39]. The battle for 5G only heightened the stakes[40]. Around 2013, Huawei began investing in 5G technology, co-founding a variety of university, government, and private partnerships throughout Europe[41]. In 2018 Huawei pledged to invest $15-20 billion USD into research and development, focusing on emerging 5G technologies such as autonomous cars, smart cities, and IoT[42]. To date, this has been on track, with over $15 billion USD spent on R&D in 2018[43], outspending Apple, and over $17 billion USD in 2019[44].

By mid-2019, Huawei had at least 50 international contracts to develop 5G[45], and as of February 2020 they have 91 such contracts[46]. By comparison, as of February 2020, the nearest competitors Ericsson and Nokia have 81 and 65 5G contracts respectively[47], though Ericsson claims other metrics put it in the lead[48]. Such contracts are more of a metric used for P.R., and, ironically, Huawei's related dubious claims of an 18-month lead over its competitors serves those wishing to undercut it by portraying it as a major threat, particularly the US[49].

On the one hand, in his 2013 book[50] senior US intelligence analyst, Northeast Asia specialist, and National Intelligence University Professor Dr. Eric C. Anderson[51] analyzes over 1,000 sources concerning Huawei. He concludes that in spite of some warts, "the evidence …

---

[39] Tripti Lahiri and Mary Hui, "Banned: How Huawei Became America's Tech Enemy No. 1," *Quartz*, May 28, 2019, https://qz.com/1627149/huaweis-journey-to-becoming-us-tech-enemy-no-1/.

[40] Zen Soo, Zheping Huang, Sarah Dai, and Li Tao, "SCMP Series: The Battle Over 5G," *South China Morning Post*, February-June, 2019, https://series.scmp.com/5g/.

[41] "Milestones – About Huawei".

[42] Sijia Jiang, "China's Huawei to Raise Annual R&D Budget to at Least $15 Billion," Technology News, *Reuters*, July 26, 2018, https://www.reuters.com/article/us-huawei-r-d/chinas-huawei-to-raise-annual-rd-budget-to-at-least-15-billion-idUSKBN1KG169.

[43] "No Pay, No Gain: Huawei Outspends Apple on R&D for a 5G Edge," New Economy, *Bloomberg News*, April 25, 2019, https://www.bloomberg.com/news/articles/2019-04-25/huawei-s-r-d-spending-balloons-as-u-s-tensions-flare-over-5g.

[44] Yash Mishra, "Huawei Will Invest Over $17 Billion in R&D This Year," News, *Huawei Central*, July 30, 2019, https://www.huaweicentral.com/huawei-will-invest-over-17-billion-in-rd-this-year/.

[45] Rita Liao, "Huawei Says Two-Thirds of 5G Networks Outside China Now Use its Gear," *TechCrunch*, June 25, 2019, https://techcrunch.com/2019/06/25/huawei-wins-5g-contracts/.

[46] Ray Le Maistre, "Huawei's Ding Gets Emotional About 5G, Boasts 91 Deals," 5G, *Light Reading*, February 20, 2020, https://www.lightreading.com/5g/huaweis-ding-gets-emotional-about-5g-boasts-91-deals/d/d-id/757629.

[47] Ibid.

[48] Chris Nuttall, "Ericsson Claims 5G Leadership Over Huawei," Technology Sector, *Financial Times*, February 13, 2020, https://www.ft.com/content/9cdf33f0-4e8e-11ea-95a0-43d18ec715f5.

[49] Iain Morris, "Huawei's '18-Month Lead' in 5G is Telecom's Most Spurious Claim," 5G, *Light Reading*, March 9, 2020, https://www.lightreading.com/5g/huaweis-18-month-lead-in-5g-is-telecoms-most-spurious-claim/a/d-id/758064.

[50] Anderson, *Sinophobia*.

[51] Sadly, Dr. Anderson died in 2018, which we discovered when we tried to follow up on his Huawei analysis.

suggests the US Congress has been engaged in a witch-hunt"[52]. Further, he makes a very compelling case that the US accusations are almost entirely unfounded.

Rather, they reflect a combination of racism, special interests, defense budget justifications, a threatened hegemonic status, and mutual suspicion and misunderstanding between the West and the East. Further, there is a fear of competition that undermines traditional US and Western formulations of how to best protect their interests, which in turn have self-defeating consequences. In May 2019, a senior technology editor for *ZDNet* laid out a similar argument[53].

He notes that while Huawei and the PRC do pose threats, the economic and security interests of Huawei, the PRC, the US, and others generally dissuade hostile actions. Further, he points to the lack of substantiated reports of state-sponsored malware or other threats Huawei is purported to represent. Instead he argues that the international focus should be on greater cybersecurity risks, including those from other states such as North Korea and Iran, criminal actors, and industry/design based risks. In these contexts, even Google has said that banning it from working with Huawei threatens security in the US and elsewhere[54].

On the other hand, going back at least to their 2002 "misappropriation" of Cisco's intellectual property[55], Huawei has a long established pattern of illegal and unethical behaviors. This pattern includes bribery[56], corruption[57], industrial espionage[58], various forms of theft[59], violating sanctions on Iran[60] and North Korea[61], recent RICO charges brought against it in the

---

[52] Anderson, *Sinophobia*, book summary.

[53] Jason Perlow, "Paranoia Will Destroy Us: Why Huawei and Other Chinese Tech is Not Spying on Americans," Tech Broiler, *ZDNet*, May 20, 2019, https://www.zdnet.com/article/paranoia-will-destroy-you-why-chinese-tech-isnt-spying-on-us/.

[54] Dieter Bohn, "Google is Reportedly Arguing that Cutting Huawei Off From Android Threatens US Security," *The Verge*, June 7, 2019, https://www.theverge.com/2019/6/7/18656163/google-huawei-android-security-ban-claims.

[55] Mark Chandler, "Huawei and Cisco's Source Code: Correcting the Record," Executive Platform, *Cisco Blogs*, October 11, 2012, https://blogs.cisco.com/news/huawei-and-ciscos-source-code-correcting-the-record.

[56] Masood Farivar, "Bribery, Corruption Charges Follow Huawei Around the World," East Asia Pacific, *VOA News*, February 11, 2019, https://www.voanews.com/east-asia-pacific/bribery-corruption-charges-follow-huawei-around-world.

[57] Ibid.

[58] Larry Chaffin, "60 Minutes Torpedoes Huawei in Less Than 15 Minutes: Cyber Espionage, Huawei, and the China [*sic*] Government," Putting Realism into Your Network, *Network World*, October 7, 2012, https://www.networkworld.com/article/2223272/60-minutes-torpedoes-huawei-in-less-than-15-minutes.html.

[59] Abrar Al-Heeti, "US Hammers Huawei with 23 Indictments for Alleged Trade Secret Theft, Fraud," *CNET*, January 29, 2019, https://www.cnet.com/news/us-hammers-huawei-with-23-indictments-for-alleged-trade-secret-theft-fraud/; Chuin-Wei Yap, Dan Strumpf, Dustin Volz, Kate O'Keeffe, and Aruna Viswanatha, "Huawei's Yearslong Rise is Littered With Accusations of Theft and Dubious Ethics," Tech, *The Wall Street Journal*, May 25, 2019, https://www.wsj.com/articles/huaweis-yearslong-rise-is-littered-with-accusations-of-theft-and-dubious-ethics-11558756858.

[60] Steve Stecklow, "Exclusive: Newly Obtained Documents Show Huawei Role in Shipping Prohibited U.S. Gear to Iran," Technology News, *Reuters*, March 2, 2020, https://www.reuters.com/article/us-huawei-iran-sanctions-

US[62], and a variety of other legal and security issues[63] (*CNet* also has a detailed and regularly updated timeline of Huawei's international developments and issues, going back to January 2018[64]). Not to mention Huawei's central role in the PRC's internal oppression tactics, especially in Xinjiang[65].

These concerns were heightened in 2014, when the PRC passed its Counter-Espionage Law, and again in 2017 when it passed its National Intelligence Law[66]. The 2017 law in particular has driven many countries to ban or restrict Huawei, particularly from 5G networks, to varying degrees[67]. Its language makes clear why:

> Any organisation and citizen shall, in accordance with the law, support, provide assistance, and cooperate in national intelligence work, and guard the secrecy of any national intelligence work that they are aware of. The state shall protect individuals and organisations that support, cooperate with, and collaborate in national intelligence work[68].

However, as of February 3, 2020 there are apparently no public substantiations of state-sponsored espionage via Huawei[69].

According to the Senior Vice President of CSIS and Director of its Technology Policy Program, Dr. James A. Lewis, a full ban is the best way to be protected from the risks that Huawei and the PRC pose[70]. This is because the nature of 5G makes it difficult, if not

---

exclusive/exclusive-newly-obtained-documents-show-huawei-role-in-shipping-prohibited-u-s-gear-to-iran-idUSKBN20P1VA.

[61] Joseph Kim, "Huawei's Puzzling Wireless Project in North Korea," George W. Bush Presidential Center, September 3, 2019, https://www.bushcenter.org/publications/articles/2019/09/huawei-wireless-north-korea.html.

[62] "Chinese Telecommunications Conglomerate Huawei and Subsidiaries Charges in Racketeering Conspiracy and Conspiracy to Steal Trade Secrets," Justice News, US Department of Justice – Office of Public Affairs, February 13, 2020, https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-subsidiaries-charged-racketeering.

[63] "A Transactional Risk Profile of Huawei." RWR Advisory Group. February 13, 2018. https://www.rwradvisory.com/wp-content/uploads/2019/03/RWR-Huawei-Risk-Report-2-13-18.pdf.

[64] Sean Keane, "Huawei Ban Timeline".

[65] Zak Doffman, "Huawei Accused of 'Theft and Dubious Ethics' - - But That's Not the Worst of it." Innovation, *Forbes*, May 25, 2019, https://www.forbes.com/sites/zakdoffman/2019/05/25/huawei-accused-of-theft-and-dubious-ethics-why-it-should-come-as-no-surprise/#296527373f59.

[66] Hoffman and Kania, "China's Laws".

[67] Panettieri, "Huawei Permitted Banned".

[68] Hoffman and Kania, "China's Laws".

[69] Brad Glosserman, "Huawei and the Realities of the 5G World," Commentary/World, *The Japan Times*, February 3, 2020, https://www.japantimes.co.jp/opinion/2020/02/03/commentary/world-commentary/huawei-realities-5g-world/#.Xptzo-pKjIV.

[70] James Andrew Lewis, "Senate Committee on Commerce, Science and Transportation – 5G Supply Chain Security: Threats and Solutions – Oral Testimony of James A. Lewis," Testimony, CSIS, March 4, 2020, https://csis-prod.s3.amazonaws.com/s3fs-public/congressional_testimony /200304_Oral_Testimony.pdf ?eMPCUCg_p48O8hSNQR7AgV_b3pYHpBeP.

impossible, to keep core, particularly critical core, networks separate from the so-called "edge", where end-user devices interface with core networks[71].

Simeon Gilding, a senior fellow at ASPI and, until December 2019, the head of the Australian Signals Directorate's signals intelligence and offensive cyber missions, was part of the team that determined Australia could not rely on a partial 5G ban due to the core-edge problem, and is highly skeptical of plans to rely on a partial ban[72]. Dr. Lewis seems more open to debate about the efficacy of a core-edge separation, but states that those who feel they can mitigate Huawei's risks can only do so if they follow through with their security plans[73].

Of the Five-Eyes intelligence sharing alliance (which consists of the UK, US, Canada, Australia, and New Zealand), Australia[74] and New Zealand[75] were the first to have fully banned Huawei from their 5G infrastructure, in 2018. The US has encouraged companies not to use Huawei's equipment in their networks since 2012[76]. More recently, it has placed a variety of import and export restrictions on the company, effectively banning Huawei from all US telecommunications networks in May 2019 via an executive order[77]. However Huawei has received consecutive reprieves from the ban, in part due to US rural networks needing time to find alternatives[78]. As of writing this article, Huawei wasn't fully banned until April 1, and even that seems to be subject to change well after that date[79].

Internationally, the US has applied enormous pressure on everyone it can to fully ban

---

[71] Rachel Falk, "Can the 'Core' and 'Edge' of a 5G Network Really be Separated?," Strategist Special Report, *The Strategist*, January 17, 2020, https://www.aspistrategist.org.au/can-the-core-and-edge-of-a-5g-network-really-be-separated/.

[72] Gilding, Simeon. "5G Choices: A pivotal Moment in World Affairs." *The Strategist*, January 29, 2020. https://www.aspistrategist.org.au/5g-choices-a-pivotal-moment-in-world-affairs/.

[73] James Andrew Lewis, "What Did the United Kingdom Just Decide on Huawei and 5G?," Commentary, CSIS, January 28, 2020, https://www.csis.org/analysis/what-did-united-kingdom-just-decide-huawei-and-5g.

[74] Panettieri, "Huawei Permitted Banned", p. 1.

[75] Ibid, p. 2

[76] Jay Greene and Shara Tibken, "Lawmakers to U.S. Companies: Don't Buy Huawei, ZTE," *CNET*, October 8, 2012, https://www.cnet.com/news/lawmakers-to-u-s-companies-dont-buy-huawei-zte/.

[77] Panettieri, "Huawei Permitted Banned", p. 3; Sean Keane, "Huawei Ban Timeline"; Donald J. Trump, "Executive Order on Securing the Information and Communications Technology and Services Supply Chain," Executive Orders – Infrastructure and Technology, The White House, May 15, 2019, https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

[78] Corinne Reichert, "Huawei Gets Another 45-Day Reprieve from Commerce Department," *CNET*, February 14, 2020, https://www.cnet.com/news/huawei-gets-another-45-day-reprieve-from-commerce-department/.

[79] "Department of Commerce Renews Temporary General License for 45 Days," Press Releases – Trade Enforcement, *US Department of Commerce – Office of Public Affairs*, February 13, 2020, https://www.commerce.gov/news/press-releases/2020/02/department-commerce-renews-temporary-general-license-45-days; "Department of Commerce Extends Public Comment Period for Input on Huawei Temporary General License Extensions." Press Releases – Trade Enforcement. US Department of Commerce – Office of Public Affairs. March 25, 2020. https://www.commerce.gov/news/press-releases/2020/03/department-commerce-extends-public-comment-period-input-huawei.

Huawei, at least from their 5G infrastructure, if not more generally from doing business with them[80]. As will shortly be detailed, the UK has not been swayed by this pressure. As a result, Canada finds itself torn between its partners[81].

In spite of the European Union's (EU) reputation for privileging rights and privacy[82] (muted in the face of Huawei's 5G[83]), its complicated relationships with the US, Huawei, and the PRC have resulted in it allowing states to make their own decisions regarding Huawei[84]. Of the European strategic partners of the UK, as of March 12, 2020, only Romania, Poland, and Estonia have signed an agreement with the US to effectively ban Huawei. Their ban decisions are apparently due to their need of US support to counter Russia, as opposed to an overwhelming concern with Huawei[85].

Japan is notable in that while it wishes to become a Five-Eyes partner, it has only banned Huawei from government infrastructure and contracts. However, the result has been that its domestic companies have decided not to use Huawei in their 5G networks[86]. The rest of the allies and strategic partners of the UK and US have thus far opted for their own approaches to mitigating Huawei's risks, focusing primarily on banning Huawei from core networks considered

---

[80] Isobel Asher Hamilton, "The Trump Administration failed to Convince the UK to Ditch Huawei and Its Other Allies Aren't Listening Either," *Business Insider*, March 11, 2020, https://www.businessinsider.com/huawei-how-allies-are-reacting-to-us-calls-to-avoid-the-tech-firm-2019-2.

[81] Kevin Carmichael, "Canada's Waffling on 5G is Just One of the Uncertainties Choking the Life Out of the Economy," Business, *Financial Post*, February 7, 2020, https://business.financialpost.com/news/economy/canadas-waffling-on-5g-is-just-one-of-the-uncertainties-choking-the-life-out-of-the-economy.

[82] Marietje Schaake and Mathias Vermeulen, "Towards a Values-Based European Foreign Policy to Cybersecurity," *Journal of Cyber Policy* 1, no. 1 (2016): 75-84, https://doi.org/10.1080/23738871.2016.1157617.

[83] Carisa Nietsche and Bolton Smith, "Why Europe Won't Combat Huawei's Trojan Tech," National Security, *The National Interest*, October 2, 2019, https://nationalinterest.org/feature/why-europe-wont-combat-huaweis-trojan-tech-85041.

[84] Erik Brattberg and Philipple Le Corre, "Huawei and Europe's 5G Conundrum," *The National Interest*, December 27, 2018, https://nationalinterest.org/feature/huawei-and-europe%E2%80%99s-5g-conundrum-39972; James Andrew Lewis, "5G To Ban or Not to Ban? It's Not Black or White," Commentary, CSIS, April 24, 2019, https://www.csis.org/analysis/5g-ban-or-not-ban-its-not-black-or-white; "EU Deals Another Blow to US, Allowing Members to Decide on Huawei's 5G role," Europe News, CNBC via Reuters, January 29, 2020, https://www.cnbc.com/2020/01/29/eu-deals-blow-to-us-allowing-members-to-decide-on-huaweis-5g-role.html; David E. Sanger and David McCabe, "Huawei is Winning the Argument in Europe, as the U.S. Fumbles to Develop Alternatives," Politics, *The New York Times*, February 17, 2020, https://www.nytimes.com/2020/02/17/us/politics/us-huawei-5g.html; Carisa Nietsche and Martijn Rasser, "Washington's Anti-Huawei Tactics Need a Reboot in Europe," Argument, *Foreign Policy*, April 30, 2020, https://foreignpolicy.com/2020/04/30/huawei-5g-europe-united-states-china/.

[85] Andreea Brinza, "How Russia Helped the United States Fight Huawei in Central and Eastern Europe," *War on the Rocks*, March 12, 2020, https://warontherocks.com/2020/03/how-russia-helped-the-united-states-fight-huawei-in-central-and-eastern-europe/.

[86] Glosserman, "Huawei Realities".

critical to their national security[87].

Amongst the Five Eyes Nations, the UK stands out as the only nation to pioneer a risk management and mitigation approach, leading the way when it comes to partnering with, and oversight of, Huawei. The UK began working with Huawei as a "high-risk vendor" in 2003, taking a mitigation approach from the start[88]. In 2010, due to unusual activity in Huawei's networks being identified by the UK's Government Communications Head Quarters (GCHQ), Huawei and the UK partnered to create the Huawei Cyber Security Evaluation Center (HCSEC)[89]. HCSEC works with GCHQ and the National Cyber Security Centre (NCSC) to assess whether Huawei's products are up to standard and are secure for deployment[90].

As a result, HCSEC has access to Huawei's source code, products, and the capacity to advise it on business matters as part of due diligence to assess if their intentions are purely commercial. This partnership has allowed the UK to focus on harnessing the benefits of working with Huawei while proactively mitigating risks. This early partnership enabled the creation of the 5G Innovation Centre at the University of Surrey in 2015, which quickly became, "the UK's largest academic 5G wireless communications infrastructure research centre"[91].

However, the UK's relationship with Huawei still has its challenges and concerns. First, older critical infrastructure in the UK already contains Huawei components[92]. Then there is the 2019 HCSEC Oversight Board Report[93], which made headlines for its numerous criticisms of Huawei's security. The criticisms revolved around poor-quality of work and a failure to adequately fix issues identified in previous HCSEC reports, though they were attributed to incompetence and negligence, as opposed to malicious intent or PRC interference. Finally, there

---

[87] Hamilton, "Allies Aren't Listening"; Panettieri, "Huawei Permitted Banned".

[88] Ian Levy, "Security, Complexity and Huawei ; Protecting the UK's Telecoms Networks," People, *NCSC Blog*, February 22, 2019, https://www.ncsc.gov.uk/blog-post/blog-post-security-complexity-and-huawei-protecting-uks-telecoms-networks.

[89] Amit Katwala, "Here's How GCHQ Scours Huawei Hardware for Malicious Code," *WIRED UK*, February 22, 2019, https://www.wired.co.uk/article/huawei-gchq-security-evaluation-uk.

[90] HCSEC's yearly reports can be found here: "Search: 'Huawei Cyber Security Evaluation Centre Oversight Board'." Gov.uk. Accessed March 30, 2020. https://www.gov.uk/search/all?keywords=%22Huawei+Cyber+Security+Evaluation+Centre+Oversight+Board%22&order=relevance.

[91] "5G Innovation Centre (5GIC) – University of Surrey," UK Research Partnership Initiative Fund, Accessed March 10, 2020, https://re.ukri.org/funding/our-funds-overview/uk-research-partnership-initiative-fund/case-studies/5g-innovation-centre-5gic-university-of-surrey/.

[92] Juliet Samuel, "Sorry Boris, France Shows There is an Alternative to Huawei After All," News, *The Telegraph*, February 2020, https://www.telegraph.co.uk/news/2020/02/01/sorry-boris-france-shows-alternative-huawei/.

[93] Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board, "Annual Report: 2019," HCSEC, March 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf.

are the years of increasing pressure from the US to ban Huawei outright[94].

When large parts of this article were first drafted in 2019, the UK was holding elections for Prime Minister and there was uncertainty as to whether or not it would ban Huawei, either as a whole or just when it came to 5G. Even up until December 2019 it seemed that PM Boris Johnson would go through with the ban[95]. At the end of January 2020, the Johnson and Parliament decided not to completely ban Huawei and high-risk vendors, voting instead to keep them out of critical core networks and cap their market share at 35%[96]

In March, members of Johnson's own party attempted a full ban, though it was ultimately defeated[97]. Since then it has appeared that the UK's approach allowed the country to move forward with Huawei and high risk vendors confidently, both balancing and benefitting its economy and security[98]. However, the coronavirus pandemic may have an impact on the UK's relations with both the PRC and the US, with implications for 5G and the UK's next National Cyber Security Strategy[99].

Members of Johnson's party view coronavirus as a means of banning Huawei and decoupling Five-Eyes from the PRC[100]. A mid-April poll by the Henry Jackson Society found that 62% of UK adults support Huawei building the UK's 5G, with 12% against, 19% "Neither", and 6% "Don't Know"[101]. The same poll found that 63% support, "adopting a tougher trade, investment and security policy towards China as has been adopted by the US over the past several years", with 12% opposed, 19% "Undecided", and 8% "Don't Know"[102].

---

[94] Garrett M. Graff, "The US is Losing Its Fight Against Huawei," Business, *WIRED*, January 29, 2020, https://www.wired.com/story/uk-huawei-5g-networks-us/.

[95] Gordon Rayner, "Boris Johnson Gives Clearest Indication Yet He Will Ban Huawei After Election," Politics, *The Telegraph*, December 4, 2019, https://www.telegraph.co.uk/politics/2019/12/04/boris-johnson-gives-clearest-indication-yet-will-ban-huawei/.

[96] Paul Sandle and Jack Stubbs, "Defying Trump, UK's Johnson Refuses to Ban Huawei from 5G," Technology News, *Reuters*, January 27, 2020, https://www.reuters.com/article/us-britain-usa-huawei/defying-trump-uks-johnson-refuses-to-ban-huawei-from-5g-idUSKBN1ZR02G.

[97] Norman Smith, "Huawei: Government Wins Vote After Backbench Rebellion," Politics, *BBC News*, March 10, 2020, https://www.bbc.com/news/uk-politics-51806704.

[98] "Johnson: Huawei 5G Decision Will Balance Innovation and Security," AJ Impact/China, *Al Jazeera*, January 27, 2020, https://www.aljazeera.com/ajimpact/johnson-huawei-5g-decision-balance-innovation-security-200127181107270.html; Ian Levy, "The Future of Telecoms in the UK," NCSC Publications, *NCSC Blog*, January 28, 2020, https://www.ncsc.gov.uk/blog-post/the-future-of-telecoms-in-the-uk; Matthew Field, "Why Britain's Spooks 'Think They Know Better' Than the US on Huawei," Technology Intelligence, *The Telegraph*, January 29, 2020, https://www.telegraph.co.uk/technology/2020/01/29/britains-spooks-think-know-better-us-huawei/.

[99] "National Cyber," HM Government; "National Progress," HM Government.

[100] James Rogers, Andrew Foxall, Matthew Henderson, Sam Armstrong, Gisela Stuart, Michael Danby, Andrew Hastie, Peter Mackay, Marco Rubio, and Bob Seely, "Breaking the China Supply Chain: How the 'Five Eyes' Can Decouple from Strategic Dependency," White Paper, Henry Jackson Society, May 2020, https://henryjacksonsociety.org/wp-content/uploads/2020/05/Breaking-the-China-Chain.pdf.

[101] Ibid, p. 14.

[102] Ibid.

In this context, we will now examine the five principle threats Huawei is purported to present to the UK. We then move on to examine some unique 5G and cyber security opportunities the UK has, before exploring challenges and innovative solutions overlooked in the 5G security discourse which the UK and other actors should consider.

Part Two—Five Principal Threats

Backdoors

A backdoor enables remote access to information and is typically invisible to all parties except the one who installed it. Backdoors can be present in either hardware or software; changing a key component, or installing a patch that enables remote access[103]. The risk that Huawei can do this to its 5G apparatus is the most common argument for distrusting Huawei. This distrust does not stem from Huawei itself, but rather the potential threat presented by the PRC and its authoritarian nature[104].

Concerns that the PRC could use Huawei as a resource to further its political agenda against individuals or other states are not just theoretical. Citing US government sources, a February 12, 2020 report by *The Wall Street Journal* states that the 4G networks Huawei helped build around the world has provided Huawei with backdoor capabilities since at least 2009, but does not state that the PRC has utilized them. According to the article, the US shared this information with the UK and Germany at the end of 2019, as they were in the final stages of deciding whether to include Huawei in their development of 5G[105].

This timeline indicates that the UK believes the risks presented by backdoors can be addressed with mitigation strategies[106], as the 2019 draft of this paper concluded. HCSEC has access to the source code and routinely tests equivalence in repeatable builds against what is deployed via patch updates. HCSEC's resources are augmented by GCHQ and the NCSC. Their combined capacities to identify backdoors diminishes the risk of them going undetected, and should assure users that Huawei's products have been vetted and are safe.

Addressing hardware risks is limited by the degree of autonomy PRC factories have over production of components. The question arises, are any viable alternatives for 5G telecommunications providers? PRC based companies provide some components to Nokia and Ericsson, the two potential 5G substitutes for the UK[107]. Then there is the fact that Huawei has a presence in some of Nokia and Ericsson's 4G and 5G networks[108]. However, the hardware threat

---

[103] Aviva Zacks, "What is a Backdoor and How to Protect Against it," Blog, Safety Detectives, September 2, 2018, https://www.safetydetectives.com/blog/what-is-a-backdoor-and-how-to-protect-against-it/.

[104] "5G Security: What is Trust?," Policy, US Department of State, November 2019, https://policystatic.state.gov/uploads/2019/11/5G-What-is-Trust.pdf.

[105] Bojan Pancevski, "U.S. Officials Say Huawei Can Covertly Access Telecom Networks," World, *The Wall Street Journal*, February 12, 2020, https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256.

[106] Levy, "Future Telecoms"; Lewis, "United Kingdom".

[107] Stu Woo and Dustin Volz. "U.S. Considers Requiring 5G Equipment for Domestic Use Be Made Outside China," Tech, *The Wall Street Journal*, June 23, 2019, https://www.wsj.com/articles/u-s-considers-requiring-5g-equipment-for-domestic-use-be-made-outside-china-11561313072.

[108] Z. X., (Editor), "Norway's Telenor Says to Continue Using Huawei Equipment for 5G," *XinHuaNet*, December 14, 2019, http://www.xinhuanet.com/english/2019-12/14/c_138631613.htm.

may not be quite so dire, and there seems to be opportunities to work with stakeholders to mitigate the risks.

Francis Dinha, CEO of the security software company OpenVP, indicates that wireless operators use a variety of hardware vendors, and ultimately it is their duty to secure their networks, as it would be foolish to rely on the vendors for security. According to Dinha, it is already industry standard to add extra layers of security. This is not to say that the PRC and companies based there do not pose a threat. Rather, Dinha believes that private industry partners and other experts have the capacity to address and mitigate the risks that vendors like Huawei pose to 5G, but, at least in the US, he feels they have yet to be appropriately consulted[109].

Acknowledging the PRC's influence, or even control, over companies based there as altogether malicious in intent leaves no economically viable way forward to acquire 5G and reap its benefits. What amounts to threat avoidance is not a viable security approach. The threats posed by the PRC require more than avoidance, deterrence, or other passive, reactive, approaches.

Acknowledging the danger posed by backdoors and other risks diminish them significantly. By remaining vigilant of the threat, agencies and stakeholders can commit to cybersecurity to ensure Huawei behaves benevolently. The HCSEC seems well positioned to do so, domestically, and as will be argued, internationally.

[109] Corinne Reichert and Marguerite Reardon, "Huawei Says US Ban Will 'Significantly Harm' American Jobs, Companies," *CNET*, May 16, 2019, https://www.cnet.com/news/huawei-says-blacklisting-will-significantly-harm-american-companies-jobs/.

Poor Source Code

The HCSEC 2019 report states it can only provide, "limited assurance that all risks to UK national security from Huawei's involvement in the UK's *critical networks* [emphasis added] can be sufficiently mitigated long-term"[110]. Similarly, for Huawei's products in general, HCSEC can, "provide *only limited assurance* [emphasis original] that the long-term security risks can be managed"[111]. Until Huawei's software and cyber security defects are fixed, "*it will be difficult to appropriately risk-manage future products* [emphasis original]"[112].

Of the risks outlined, weak source code is the most tangible security risk to the 5G network. According to the HCSEC 2019 report, there are presently three issues stemming from poor source code[113]:

- Poor source code found in the repeatable builds
- Inconsistency of the builds' equivalence with actual deployed products
- Limited evidence of rectifying poor processes and coding

The UK has since decided to move forward with Huawei as a 5G partner. However, Huawei will not be allowed to provide components and services for networks critical to the UK's security apparatuses. Nonetheless, poor source code remains a general concern.

The risk presented by poor source code stems from the capacity for third parties, such as states, individuals, or organised crime, to penetrate the network and carry out acts of theft, espionage, sabotage, or ransom. The inconsistency of builds' equivalence means that the source code given by Huawei to HCSEC is not identical to what Huawei uses in some or all of its products. This inconsistency limits the degree to which HCSEC can claim Huawei's products are safe.

Outlined in the report is Huawei's "transformation plan" to standardise production and assure security. Specifically, they are to follow procedures that will ensure the proper replication of the source code (meaning what is provided to HCSEC matches the hardware and software deployed), and improve their engineering and security. Although $2 billion USD is to be set aside to execute this, the proposed initial budget does not specify any activities[114].

Enforcing HCSEC's standards is a necessity that the UK must follow through on to mitigate its risks[115]. If it does so, by already having access to Huawei's source code and with the weight of its visible partnership with Huawei, UK will be in a unique position to cement its role

[110] HCSEC, "2019," p. 4.
[111] Ibid.
[112] Ibid.
[113] Ibid, p. 12-29.
[114] Ibid, p. 17.
[115] Ibid; Levy, "Future Telecoms"; Lewis, "United Kingdom".

as a global leader of cybersecurity and take greater control of its threat forecast. There is still reason to question the efficacy of source code review[116]. However, from security and economic perspectives, it would seem more productive to engage Huawei while proactively addressing its risks[117], possibly by making the current risk mitigation effort multilateral.

Security issues inherently become political when they are of the scale presented by Huawei's weak source code. The weak source code is not just concerning when it comes to government intrusion. In many ways what is of greater, mutual, concern is cybercrime, which is a transnational issue[118]. Increased attention and funding, whether by the UK or a multilateral effort, could leverage greater technical expertise and political capital against the risks Huawei poses, whether stemming from government or non-state actors.

More importantly, such actions would make it easier to hold Huawei accountable to security standards not just in the UK, but globally. Avoidance as a mitigation strategy for the UK does not remove the threat presented by Huawei's source code. Cooperation with Huawei, and keeping them in the UK market, is more beneficial for all.

[116] Gilding, "5G Choices".
[117] Levy, "Future Telecoms"; Lewis, "United Kingdom".
[118] "Cyber Crime," United Nations – Office on Drugs and Crime, Accessed March 25, 2020, https://www.unodc.org/unodc/en/cybercrime/index.html.

Potential Monopoly

According to Dr. Lewis, "Huawei wants a monopoly, and the Chinese government supports this because it will give them a global signals intelligence network"[119], akin to the decades long US-Germany Crypto AG operation[120], and the 2007 US hacking of Huawei[121]. While monopolies are not desirable for security or the economy, the looming threat of Huawei's growing monopoly is not simply a threat on its own. Rather, it amplifies the risks previously addressed, and exacerbates issues and risks relating to the PRC's predatory economic practices[122].

By allowing Huawei in via partial bans, European and other nations seek to balance the costs, benefits, and risks Huawei and the PRC present[123]. A Huawei-established global monopoly concentrates power over distribution and production of software and hardware, in general and in 5G. This increases the capacity to install backdoors, whilst poor source code potentially could continue without rectification, making organisations and governments more vulnerable. Further, if Huawei were obligated by the PRC to stop providing services to a client nation as part of the PRC's laws, a monopoly gives Huawei and the PRC incredible leverage over dependent nations.

Presuming coronavirus doesn't decouple the PRC from the West[124], this risk seems to be predominantly a projected one because global economic integration effectively binds Huawei from acting with the liberty of a typical monopolist[125]. For example, Huawei presently runs on the Android operating system (OS), which is owned by Google[126]. While they are developing their own OS, Harmony (aka Hongmeng) in case a US ban halts their Google partnership[127], the

---

[119] Lewis, "5G to Ban or Not".

[120] Greg Miller, "'The Intelligence Coup of the Century': For Decades, the CIA Read the Encrypted Communications of Allies and Adversaries," National Security, *The Washington Post*, February 11, 2020, https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/.

[121] Sanger and Perlroth, "N.S.A. Breached".

[122] Matthew P. Goodman, "Predatory Economics and the China Challenge," *Global Economics Monthly* 6, no. 11 (November 2017): 1-2, https://www.csis.org/analysis/predatory-economics-and-china-challenge.

[123] Brinza, "How Russia".

[124] Ford, "Refocusing Decoupling"; Erica Pandey, "U.S. Bans Could Make Huawei Stronger," Technology, *Axios*, March 5, 2020, https://www.axios.com/huawei-cybersecurity-china-decoupling-5g-11034740-797b-4f00-a17e-7b3265d8bbcd.html; Kurt M. Campbell and Rush Doshi, "The Coronavirus Could Reshape Global Order," *Foreign Affairs*, March 18, 2020, https://www.foreignaffairs.com/articles/china/2020-03-18/coronavirus-could-reshape-global-order.

[125] Morris, "Huawei's '18-Month'"; James Andrew Lewis, "Statement Before the Senate Committee on the Judiciary – '5G: The Impact on National Security, Intellectual Property, and Competition' – A Testimony by: James A. Lewis," Testimony, CSIS, May 14, 2019, https://csis-prod.s3.amazonaws.com/s3fs-public/congressional_testimony/Jim%20Lewis%20Written%20Statement %203-4-20.pdf?j.NdIo307mIklOlZ7sobLj5o088GC53m.

[126] Tom Bedford and Basil Kronfli, "Harmony OS: What You Need to Know About Huawei's New Operating System," News, *TechRadar*, January 17, 2020, https://www.techradar.com/news/harmonyos.

[127] Ibid.

US continues to control the production of semiconductors and key chip components[128]. As Ren Zhengfei, Huawei's CEO, acknowledges, "if one of a thousand key parts is missing, a piece of telecoms equipment will cease to work"[129].

Furthermore, while the PRC's manufacturing capacity to make goods continues to scale[130] (notably making about 90% of the world's PC's and 70% of phones as of 2011[131]), they lack the free market structures that enable the innovation required to pave the way into the 5G future[132]. Even if their capacity for innovation does change, global competitors will certainly remain worthy opponents or even collaborators[133]. In this sense, a successful business strategy for smaller 5G enterprises such as Ericsson and Nokia might be to provide specialist services that Huawei does not. Either way, even if Huawei can potentially establish a monopoly by market share, it cannot behave like a typical monopolist. This is due to its dependence on external suppliers for equipment and services, which in turn limits Huawei's ability to act with impunity.

Now consider the alternative where Huawei is removed from the market in the UK. Aside from the potential retaliation against the UK by the PRC, if Ericsson and Nokia are the remaining 5G competitors, the expenses and opportunity costs will rise. Both suppliers' equipment costs more, primarily due to higher production costs outside of the PRC[134].

Before the Covid-19 pandemic, Ericsson and Nokia were beginning to shift some 5G production outside of the PRC, particularly to India[135]. The political and economic fallout of Covid-19 has caused many countries to reconsider their relationships with the PRC, particularly when it comes to medical and technology supply chains. One result has been an increased interest in trade with India, particularly as far as the UK is concerned[136].

---

[128] Lewis, "Statement Judiciary," p. 7.
[129] James Kynge, Yuan Yang, and Sue-Lin Wong, "Huawei: Still Fighting for Survival Despite Trump Truce," The Big Read – Huawei Technologies, *Financial* Times, July 3, 2019, https://www.ft.com/content/a6db14d8-9993-11e9-9573-ee5cbb98ed36.
[130] Gordon Orr, "What Can We Expect in China in 2020?," Featured Insights – Commentary, McKinsey and Company, December 2019, https://www.mckinsey.com/featured-insights/china/what-can-we-expect-in-china-in-2020.
[131] Matt Schiavenza, "China's Dominance in Manufacturing—in One Chart," China, *The Atlantic*, August 5, 2013,https://www.theatlantic.com/china/archive/2013/08/chinas-dominance-in-manufacturing-in-one-chart/278366/.
[132] Ben Blanchard and Perry Michael, "Lack of Innovation is 'Achilles Heel' for China's Economy, Xi Says," World News, *Reuters*, May 15 2019, https://www.reuters.com/article/us-china-politics-xi/lack-of-innovation-is-achilles-heel-for-chinas-economy-xi-says-idUSKCN1SM08G.
[133] Scott Kennedy, "China's Uneven High-Tech Drive: Implications for the United States," Report, CSIS, February 27, 2020, https://www.csis.org/analysis/chinas-uneven-high-tech-drive-implications-united-states.
[134] Anirban Ghoshal, "Nokia, Ericsson to Soon Export 5G Equipment Made in India," Technology, *TechCircle*, October 26, 2018, https://www.techcircle.in/2018/10/26/nokia-ericsson-to-soon-export-5g-equipment-made-in-india.
[135] Ibid.
[136] George Parker and Daniel Thomas, "UK Looks to Wean Itself Off Chinese Imports," UK Trade, *Financial Times*, June 9, 2020, https://www.ft.com/content/dc22913c-4abd-4258-89fb-e45a4342e2a6.

While diversification is smart for a variety of reasons, it is not so clear that switching production to India will enhance security or prevent higher costs. Long standing tensions between India and the PRC have been rising in recent years, and seem to have taken a turn for the worse with their first lethal clash since 1975 occurring on June 15, 2020[137]. Before, and particularly after Covid-19 and the fatal clash, India was already looking into limiting or banning PRC based companies including Huawei and ZTE[138].

Throughout, escalating economic and political tit for tat has increased costs for both countries[139]. Further, India's protectionist approach is not just impacting its relationship with the PRC. Rather than creating an opportunity for the West and countries like Japan, South Korea, and Australia, India's protectionist policies have been so broadly formulated that they have increased costs for virtually all of their partners[140]. Given India's and the West's trend towards decoupling from the PRC, these costs will likely only increase.

These higher costs may be further compounded by five issues. First, Huawei arguably motivates 5G providers to remain competitive in terms of costs, quality, and innovation[141]. Second, in late 2018 industry experts, and even company insiders, believed that Nokia and Ericsson would struggle with, "replacing Huawei in the core of an operators network", let alone, "across radio sites", though both companies have tried to rebuff these claims with mixed results[142]. Such concerns about abilities, costs, and delays remain in play as of February 2020[143].

Third, Nokia and Ericsson's recent bids with the US[144] and France[145] as an alternative to Huawei, as aggravated by the US-PRC trade war, has caused them to shift even more of their

---

[137] Helen Davidson and Ben Doherty, "Explainer: What is the Deadly India-China Border Dispute About?," World—India, *The Guardian*, June 16, 2020, https://www.theguardian.com/world/2020/jun/17/explainer-what-is-the-deadly-india-china-border-dispute-about.

[138] Akhil Bery and Clarise Brown, "India and China's Digital Divorce," Eurasia Live, Eurasia Group, July 1, 2020, Video, 11m:35s, https://www.eurasiagroup.net/live-post/india-china-digital-divorce.

[139] Ibid.

[140] Ibid.

[141] Iain Morris, "Where Huawei Fears to Tread," 5G, *Light Reading*, December 13, 2018, https://www.lightreading.com/mobile/5g/where-huawei-fears-to-tread/d/d-id/748266; Gordan Corera, "Eric Schmidt: Huawei has Engaged in Unacceptable Practices," Technology, *BBC News*, June 18, 2020, https://www.bbc.com/news/technology-53080113.

[142] Iain Morris, "Huawei Muscle Puts Ericsson, Nokia on 5G Back Foot in Europe – Sources," 5G, *Light Reading*, February 14, 2019, https://www.lightreading.com/mobile/5g/huawei-muscle-puts-ericsson-nokia-on-5g-back-foot-in-europe---sources/d/d-id/749474.

[143] Johannes Ledel and Sam Kingsley, "Can Nokia, Ericsson Compete With Huawei?," China. *Asia Times*, February 3, 2020, https://asiatimes.com/2020/02/can-nokia-ericsson-compete-with-huawei/.

[144] Marguerite Reardon, "Nokia and Ericsson Pitch Themselves as Huawei 5G Alternative," *CNET*, March 4, 2020, https://www.cnet.com/news/nokia-and-ericsson-pitch-themselves-as-huawei-5g-alternative/.

[145] Zak Doffman, "China Just Issued Stark New Threats Over Huawei: This Time Nokia and Ericsson are in Its Sights," Innovation, *Forbes*, February 9, 2020, https://www.forbes.com/sites/zakdoffman/2020/02/09/china-just-issued-stark-new-threats-over-huawei-this-time-nokia-and-ericsson-are-in-its-sights/#57f21d2119d7.

production out of the PRC, likely further raising costs[146]. Fourth, they have been competing for contracts within the PRC which accounts for, "60% of the global 4G infrastructure market"[147], which could be leveraged against Nokia and Ericsson, thus potentially raising costs. Fifth, if the UK, US, Europe, and others oust Huawei in favor of Ericsson and Nokia, it would eliminate around 40 percent of competition[148]. As US hopes for Apple, Samsung, Dell, or Microsoft seem unlikely[149], such a situation creates a comfortable duopoly.

Concentrations of power are security threats in and of themselves, and modern technology makes such concentrations unprecedented[150]. From a cybersecurity standpoint, market concentration itself increases, "the volume of systemic cyber risk"[151]. It also limits the ability to reactively, let alone proactively, address threats[152]. In this context, risk mitigation, "requires better measurement, diversity of systems … attention to market concentration in cyber insurance pricing, and the deliberate choice to avoid ubiquitous interconnection in critical systems"[153].

Such risks are exacerbated for Europe and the UK. Europe only has four Radio Access Network (RAN) hardware suppliers; ZTE, Huawei, Nokia, and Ericsson. The UK only has three RAN suppliers; Huawei, Nokia, and Ericsson[154].

From an economic standpoint, while duopolies do not inherently pose[155] the same degree

---

[146] Iain Morris, "Ericsson, Nokia Prepared for Any US Ban on China-Made Gear," 5G, *Light Reading*, June 24, 2019, https://www.lightreading.com/mobile/5g/ericsson-nokia-prepared-for-any-us-ban-on-china-made-gear/d/d-id/752342.

[147] Iain Morris, "Nokia in Line for 5G Contracts Worth Up to $2.2B With Chinese Telcos," Asia, *Light Reading*, November 11, 2019, https://www.lightreading.com/asia-pacific/nokia-in-line-for-5g-contracts-worth-up-to-$22b-with-chinese-telcos/d/d-id/755523.

[148] Valentin Weber, "Making Sense of Technological Spheres of Influence," Strategic Updates, LSE IDEAS, March 31, 2020, http://www.lse.ac.uk/ideas/publications/updates/technological-spheres-of-influence.

[149] Jeremy Horwitz, "U.S. 5G Security is Imperiled by Trump Administration Infighting and Fantasies," Security – Opinion, *Venture Beat*, February 6, 2020, https://venturebeat.com/2020/02/06/u-s-5g-security-is-imperiled-by-trump-administration-infighting-and-fantasies/.

[150] Adam Garfinkle, "Power Concentrations: The Net Effect," *The American Interest*, April 7, 2020, https://www.the-american-interest.com/2020/04/07/the-net-effect/.

[151] Dan Geer, Eric Jardine, and Eireann Leverett, "On Market Concentration and Cybersecurity Risk," *Journal of Cyber Policy* (published online February 24, 2020), https://doi.org/10.1080/23738871.2020.1728355.

[152] Tom Wheeler and David Simpson, "Why 5G Requires New Approaches to Cybersecurity: Racing to Protect the Most Important Network of the 21st Century," Report, The Brookings Institution, September 3, 2019, https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/.

[153] Ibid.

[154] James Sullivan and Rebecca Lucas, "5G Cyber Security: A Risk Management Approach," The Globalisation of Technology Occasional Paper, RUSI, February 14, 2020, p. 16-17, https://rusi.org/publication/occasional-papers/5g-cyber-security-risk-management-approach.

[155] Erwin A. Blackstone, Larry F. Darby, and Joseph P. Fuhr Jr., "The Case of Duopoly: Industry Structure is not a Sufficient Basis for Imposing Regulation," *Regulation* (Winter 2011-2012): 12-17, https://www.cato.org/sites/cato.org/files/serials/files/regulation/2012/6/v34n4-3.pdf.

of price-setting, anti-competitive, and other problems that monopolies tend to guarantee[156], they do present opportunities for such practices via collusion between the two companies. Collusion is illegal in the US and elsewhere. However, it does not seem to disincentivize industries and companies in from colluding[157]. This is particularly true if they are large or important enough to lobby against attention, lobby to change laws, or just pay fines and move on. Telecommunications and IT industries are already prime examples of such tendencies, crippling innovation and raising costs[158].

Further, duopolies, and their cousins cartels and oligopolies, can bring about "tacit collusion"[159]. Tacit collusion means that the firms and markets may passively (or just not entirely actively) come to behave like colluders and monopolies, harming innovation and consumers. Certain conditions encourage or discourage tacit collusion. While more analysis would be needed, there certainly seems to be a reasonable concern about a Nokia and Ericsson duopoly having unintended negative consequences, including tacit collusion and thus higher prices.

Individually, or as a whole, such factors would limit the speed of introducing 5G networks, their overall quality and coverage, and their subsequent innovation. Relying on such a market dynamic would impose significant fiscal and opportunity costs for those trying to catch up with countries that have already entered the age of fully commercialised 5G made affordable by Huawei. Either way, the UK and West's response to the PRC's protectionism, Huawei's monopoly, and their associated predatory economic practices, shouldn't be to establish their own protectionist monopoly, duopoly, or oligopoly.

Critically, encouraging free-markets and economic integration has historically prevented negative competition and conflicts[160]. For about a century, the UK and US's values of and strategies for liberty, security, and prosperity have been to encourage market competition and increase integration of stakeholders through participation[161]. The eschewal of the PRC in this

---

[156] James A. Schmitz Jr., "The Cost of Monopoly: A New View," Article, Federal Reserve Bank of Minneapolis, July 12, 2016, https://www.minneapolisfed.org/article/2016/the-costs-of-monopoly-a-new-view.

[157] Joseph E. Harrington Jr., *The Theory of Collusion and Competition Policy*, Cambridge, Massachusetts: Massachusetts Institute of Technology, 2017.

[158] Susan P. Crawford, *Captive Audience: The Telecom Industry and Monopoly Power in the New Gilded Age*, New Haven, Connecticut, US: Yale University Press, 2013; Tim Wu, "The Oligopoly Problem," Annals of Technology, *The New Yorker*, April 15, 2013, https://www.newyorker.com/tech/annals-of-technology/the-oligopoly-problem.

[159] Marc Ivaldi, Bruno Jullien, Patrick Rey, Paul Seabright, and Jean Tirole, "The Economics of Tacit Collusion," Final Report for DG Competition, European Commission, March 2013, https://ec.europa.eu/competition/mergers/studies_reports/the_economics_of_tacit_collusion_en.pdf.

[160] Wu Xinbo, "U.S. Security Policy in Asia: Implications for China-U.S. Relations," Report, The Brookings Institution, September 1, 2000, https://www.brookings.edu/research/u-s-security-policy-in-asia-implications-for-china-u-s-relations/; Jong-Wha Lee and Ju Hyun Pyun. "Does Trade Integration Contribute to Peace?," *Review of Development Economics* 20, no. 1 (February 2016): 327-344, https://doi.org/10.1111/rode.12222.

[161] Dani Rodrik, "Globalization's Wrong Turn and How it Hurt America," *Foreign Affairs* 98, no. 4 (July/August 2019): 26-33, https://drodrik.scholar.harvard.edu/files/dani-rodrik/files/globalizations_wrong_turn.pdf.

market and other realms runs contrary to such principles and raises risks[162]. Further, as Dr. Lewis points out, in spite of accusations against the PRC, in recent history the US is the only country to consistently engage in economic warfare, and in a globalized world such actions will backfire[163].

Disenfranchising Huawei thereby encourages both Huawei and the P.R.C to act more independently and even maliciously against those that have barred them from entering new markets[164]. Further, it may weaken the economic, security, and ideological interests of the UK and US[165]. However, this **not** the Cold War, and such comparisons, ideological or otherwise, must be critically assessed[166]. In either case, it is better for the UK and US to incentivize greater and healthier participation in the global system they have created, helping their values sell themselves to the people and officials of the PRC and the world, rather than forfeiting it all.

Enabling Huawei in the UK would increase regional and global competition and innovation in 5G and all it entails. Banning Huawei incentivises negative competition by signaling to policymakers and private enterprises that the UK and the PRC's relationship is adversarial in nature. In turn, the benefits of competition and trade are lost, not only in 5G but in other industries as well.

In the context of 5G, the loss of the UK as a market will not impact the PRC significantly. Whereas the UK will lose access to the competitively priced 5G telecommunications services Huawei provides, as well as other IT benefits both in place and on the horizon. Then there is the fallout that could occur as a result of the PRC's existing, rather pervasive, penetration of UK networks[167], which would be better to mitigate than aggravate.

---

[162] Kolton, "China's Cyber Sovereignty"; Michael D. Swaine, "A Relationship Under Extreme Duress: U.S.-China Relations at a Crossroads," The Carter Center, January 16, 2019, https://www.cartercenter.org/resources/pdfs/peace/china/china-program-2019/swaine.pdf; Robert B. Zoellick, "Can American and China be Stakeholders?," Transcript – U.S.-China Business Council, The Carnegie Endowment for International Peace, December 4, 2019, https://carnegieendowment.org/2019/12/04/can-america-and-china-be-stakeholders-pub-80510.

[163] James Andrew Lewis, "ZTE, the Telecom Wars, and Cyber Spies," Report – CSIS Briefs, CSIS, June 25 2018, https://www.csis.org/analysis/zte-telecom-wars-and-cyber-spies.

[164] Zak Doffman, "China Just Crossed a Dangerous New Line for Huawei: 'There Will be Consequences," Innovation, *Forbes*, December 16, 2019, https://www.forbes.com/sites/zakdoffman/2019/12/16/china-just-crossed-a-dangerous-new-line-for-huawei-there-will-be-consequences/#1d3effb575a3.

[165] Kolton, "China's Cyber Sovereignty"; Zhang Lin, "US-China Trade War is Really a Clash of Civilizations and Ideologies," Economy—Opinion, *South China Morning Post*, October 15, 2018, https://www.scmp.com/economy/china-economy/article/2168492/us-china-trade-war-really-clash-civilisations-and-ideologies; Osnos, "America's Contest China"; Pandey, "Bans Huawei Stronger".

[166] Tarun Chhabra, Rush Doshi, Ryan Hass, and Mira Rapp-Hooper, "Rethinking US-China Competition: Next Generation Perspectives – A Brookings Interview," By Bruce Jones, Edited by Bruce Jones and Will Moreland, Foreign Policy at Brookings, The Brookings Institution, June 2019, https://www.brookings.edu/wp-content/uploads/2019/06/FP_20190625_global_china.pdf; Melvyn P. Leffler, "China isn't the Society Union. Confusing the Two is Dangerous," Ideas, *The Atlantic*, December 2, 2019, https://www.theatlantic.com/ideas/archive/2019/12/cold-war-china-purely-optional/601969/.

[167] Lewis, "United Kingdom".

In either case, the relative risks and deprivation of benefits are much higher for the UK than for the PRC, should Huawei and the PRC be rejected. Given the PRC and Huawei's roles in the present economic order, it seems beneficial to exploit their manufacturing capacity and relative technical expertise in some of the biggest industries of the future (i.e. 5G and 6G). This is particularly true if Huawei is just one of many accepted competitors in the IoT arena.

Arguments for free markets should not go without acknowledging the importance of both well thought out public-private regulations designed to promote competition and innovation[168], and government led research and development funding[169]. Indeed, while the UK and much of the West have generally relied on market forces for cybersecurity, market *failures*, including those just discussed, have posed significant problems[170]. In the case of the UK, market failures including, "ongoing data breaches; inadequate private cybersecurity investments; and a continuous digital skills gap", have resulted in a, "more state-driven public-private partnership"[171]. How this is done matters, particularly for 5G[172].

Balancing free markets and government intervention hinges on neither playing favorites nor allowing significant market distortions and concentrations[173]. When it comes to 5G and cyber security, this balance is all the more crucial[174]. Enforcing antitrust laws against Huawei may be difficult, if not impossible, and the current US approach could, "spell the end of antitrust enforcement as we know it"[175] globally. Further, the US approach can even be leveraged in

---

[168] Crawford, "Captive Audience"; Ivaldi et al., "Tacit Collusion"; Harrington Jr., "Collusion Competition"; Mihail Danov, "Global Competition Law Framework: A Private International Law Solution Needed," *Journal of Private International Law* 12, no. 1 (2016): 77-105, https://doi.org/10.1080/17441048.2016.1150103; Wolfgang Kerber and Heike Schweitzer, "Interoperability in the Digital Economy," *Journal of Intellectual Property, Information Technology and E-Commerce Law* 8, no. 1 (2017): 39-58, https://nbn-resolving.org/urn:nbn:de:0009-29-45317.

[169] Sheila Campbell and Chad Shirley, "Estimating the Long-Term Effects of Federal R&D Spending: CBO's Current Approach and Research Needs," Blog, Congressional Budget Office, June 21, 2018, https://www.cbo.gov/publication/54089.

[170] "Special Issue: Comparative Industrial Policy and Cyber Security." *Journal of Cyber Policy* 3, no. 3 (2018): 287-469. https://www.tandfonline.com/toc/rcyb20/3/3; Wheeler and Simpson, "5G Requires".

[171] Madeline Carr and Leonie Maria Tanczer, "UK Cybersecurity Industrial Policy: An Analysis of Drivers, Market Failures and Interventions," *Journal of Cyber Policy* 3, no. 3 (2018): p. 430, https://doi.org/10.1080/23738871.2018.1550523.

[172] Wheeler and Simpson, "5G Requires".

[173] Ivaldi et al., "Tacit Collusion"; Kerber and Schweitzer, "Interoperability Economy"; Carr and Tanczer, "UK Cybersecurity"; Geer, Jardine, and Leverett, "Market Cybersecurity"; "Why Competition and Consumer Protection Matter," Department of International Trade and Commodities—Competition Law, United Nations Conference on Trade and Development, Accessed April 17, 2020, https://unctad.org/en/Pages/DITC/CompetitionLaw/why-competition-matters.aspx.

[174] "Special Issue", *Journal of Cyber Policy*; Wheeler and Simpson, "5G Requires".

[175] Christian Peeters, "Huawei Ban Creates Challenge for Int'l Antritrust Enforcement," Expert Analysis–Opinion, *Law360*, May 30, 2019, https://www.law360.com/articles/1164251/huawei-ban-creates-challenge-for-int-l-antitrust-enforcement.

Huawei's favor, with consequences for US national security[176].

Other stick based approaches also seem difficult. In spite of its many economic complaints and bans against Huawei, the US has generally opted not to go after it in its trade war, likely because of the risks of doing so, whether political or economic[177]. This is not to suggest discontinuing the pursuit of global antitrust enforcement[178]. However, rather than focusing on punishing Huawei, and thus themselves[179], the UK and others should do more to encourage public and private sector 5G and IoT innovation by funding diverse competition[180].

Compared to the PRC's $75 billion USD in support for Huawei over 20 years[181], and Huawei's $17 billion USD R&D budget, in 2018 the UK reserved a little more than $6.41 billion

[176] Loren Thompson, "Qualcomm Antitrust Case Raises Far-Reaching National Security Concerns," Business, *Forbes*, January 28, 2020, https://www.forbes.com/sites/lorenthompson/2020/01/28/qualcomm-antitrust-case-raises-far-reaching-national-security-concerns/#1d9399f669ea.

[177] Robert Clark, "No One Wants to Talk About Huawei's State Subsidies," News Analysis, *Light Reading*, January 9, 2020, https://www.lightreading.com/asia-pacific/no-one-wants-to-talk-about-huaweis-state-subsidies/d/d-id/756697.

[178] Danov, "Global Competition".

[179] Will Knight, "The Newest US Sanctions on China's Huawei Could Backfire," Business, *WIRED*, March 31, 2020, https://www.wired.com/story/newest-us-sanctions-chinas-huawei-backfire/; Elsa B. Kania and Lindsay Gorman, "The United States Can't Afford to Turn Away Chinese Talent," Argument, *Foreign Policy*, May 13, 2020, https://foreignpolicy.com/2020/05/13/united-states-cant-afford-turn-away-chinese-talent/; Lairson, Skidmore, and Xinbo, "US Backfired".

[180] Carr and Tanczer, "UK Cybersecurity"; Milo Medin, Gilman Louie, Kurt DelBene, Michael McQuade, Richard Murray, and Mark Sirangelo, "The 5G Ecosystem: Risks & Opportunities for DoD," Report, Defense Innovation Board, April 3, 2019, https://media.defense.gov/2019/Apr/04/2002109654/-1/-1/0/DIB_5G_STUDY_04.04.19.PDF; Phil Budden and Fiona Murray, "Defense Innovation Report: Applying MIT's Innovation Ecosystem & Stakeholder Approach to Innovation in Defense on a Country-by-Country Basis," Working Paper, MIT LAB for Innovation Science and Policy, May 2019, https://innovation.mit.edu/assets/Defense-Innovation-Report.pdf; Wheeler, "5G Five"; James Andrew Lewis, Clete Johnson, and Denise E. Zheng. "5G Innovation and Security: Perspectives from Industry and Government Leadership." Christopher Krebs, Kim Hart, Jason Boswell, John Godfrey, Susie Armstrong, Peter Lord, Robert Strayer, Eric Wagner, Kevin Linehan, Chris Boyer, Valerie J. Parker, Geoffrey Starks, and Jennifer Lane. Event. CSIS. July 31, 2019. Audio, 2h:57m:40s. https://www.csis.org/events /5g-innovation-and-security; Elsa B. Kania, "Securing Our 5G Future: The Competitive Challenge and Considerations for U.S. Policy," Reports, Center for a New American Security, November 07, 2019, https:// www.cnas.org/publications /reports/securing-our-5g-future; Kathleen H. Hicks, Joseph Federici, Seamus P. Daniels, Rhys McCormick, and Lindsey R. Sheppard. "Getting to Less? The Innovation Superiority Strategy." Report. CSIS. January 23, 2020. https://www.csis.org /analysis/getting-less-innovation-superiority-strategy; Elsa B. Kania, "Why Doesn't the U.S. Have Its Own Huawei?," The 5G Future—Opinion. *Politico*, February 25, 2020, https://www.politico.com/news/agenda/2020 /02/25/five-g-failures-future-american-innovation-strategy-106378; Daniel Kliman, Ben FitzGerald, Kristine Lee, and Joshua Fitt, "Forging an Alliance Innovation Base," Report—America Competes 2020, CNAS, March 29, 2020, https://www.cnas.org/publications/reports/forging-an-alliance-innovation-base.

[181] Chuin-Wei Yap, "State Support Helped Fuel Huawei's Global Rise," Tech, *The Wall Street Journal*, December 25, 2019, https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736.

USD for 5G investment out of its almost $743 billion USD infrastructure budget[182]. This compares to the 2018 R&D figures for Cisco ($6.37 billion USD), Qualcomm ($5.48 billion USD), Nokia ($5.46 billion USD), and Ericsson ($4.4.8 billion USD), and the potential $1 billion USD the US may allocate for 5G R&D in 2020[183]. For that matter, as of October 2019 the US government's R&D spending is at its lowest levels as a share of GDP since 1955[184].

Regardless of their investment sizes, at least UK and US investments are rightfully focused on aiding academic and business ventures in 5G. However, there remains a danger of putting all of their network investments into just a couple of firms. Ideally they lead by example, increasing support for diverse competition and innovation, rather than propping up their own state sponsored giant(s).

If the West creates their own "national champion(s)", not only would they be capitulating to the PRC's approach, they would be opening themselves up to legal action by the PRC under international competition laws. Yet such market concentrations pose a greater, more costly, risk than all those mentioned so far: that a more innovative, competitive, and secure future is delayed or even missed[185]. Open network architecture is almost certainly that future.

Open network architecture is essentially a software replacement of the current hardware based network approach. According to former US FCC Chairman and member of the Intelligence Advisory Board, Tom Wheeler, while, "the 5G standard itself is open and interoperable" [186], infrastructure companies use their proprietary hardware to lock in consumers. This prevents 5G from reaching its true and intended potential[187].

Open network architecture seeks to, "replace traditional network vendors' proprietary technology with software-driven technology that will run on any off-the-shelf hardware"[188]. This allows for greater innovation, competition, and security in hardware, software, and the IoT. The benefits of open networks are something Huawei greatly fears[189], and the approach is arguably

---

[182] Jamie Davies, "UK Gov Reserves £6.8bn to Realise 5G dream by 2027," News. *Telecoms*, November 27, 2018, https://telecoms.com/493818/uk-gov-reserves-6-8bn-to-realise-5g-dream-by-2027/.
[183] Klint Finley, "Senators Propose $1B to Outpace Huawei in 5G. That's Small Change," Business, *WIRED*, January 14, 2020, https://www.wired.com/story/billion-outpace-huawei-5g-small-change/.
[184] Michael T. Nietzel, "The U.S. Loses Ground to the Rest of the World in R and D Funding," Leadership, *Forbes*, October 22, 2019, https://www.forbes.com/sites/michaeltnietzel/2019/10/22/the-us-loses-ground-to-the-rest-of-the-world-in-r-and-d-funding/#637c3864202d.
[185] Kerber and Schweitzer, "Interoperability Economy".
[186] Tom Wheeler, "Moving from 'Secret Sauce' to Open Standards for 5G," TechTank, The Brookings Institution, February 18, 2020, https://www.brookings.edu/blog/techtank/2020/02/18/moving-from-secret-sauce-to-open-standards-for-5g/.
[187] Ibid.
[188] Ibid.
[189] Ibid.

far more effective than sanctions[190].

Analysts acknowledge the US's one-size fits all approach to Europe's Huawei relationship has failed. Thus they encourage it to take a more nuanced approach while promoting both the development of open networks and their 5G success with Nokia's and Ericsson's technologies[191]. Strangely, in spite of the fact that Ericsson and Nokia have already joined[192] the O-RAN Alliance[193], which is pursuing an open network future, and in spite of bi-partisan support for open networks, the Trump administration disdains open networks[194].

The administration seems unlikely to take a nuanced approach or pursue open networks. Instead, the administration is attempting to force certain radio frequencies open for 5G, against the security concerns of the US Defense Secretary, Air Force, the bipartisan members of the House and Senate Armed Services Committees, private industry, and many others. Experts have pointed out that the disputed frequency band isn't even an effective medium for 5G, yet the administration continues pushing for it. In either case, the solution, again, is open network technology, but there is reason to believe it will be ignored[195].

The O-RAN alliance sent the UK a letter in mid-April 2020 encouraging it to eschew Huawei in favor of open networks, not only for security concerns, but also for maintenance and opportunity costs. However, open networks are not yet a reality and will take time to emerge, so the UK must consider how to best balance its short term and long term interests. This balance could grant the UK with unique economic, security, and political opportunities.

By giving Huawei and the PRC a stake in the global economic order, it further incentivises cooperation with HCSEC and other partners concerned with security and disincentives the installation of backdoors. The alternative, of excluding Huawei from the UK market, does not encourage the UK domestic market to evolve or present any opportunities to take advantage of beyond a sense of security. The partnerships and competition Huawei brings to the UK could spur the immediate development of a greater cybersecurity industry and future IoT-related enterprise – both growth markets with great potential.

Thus, encouraging competition and cooperation with Huawei and the PRC, while

---

[190] "Open standards, not sanctions, are America's Best Weapon Against Huawei," Leaders—5Geopolitics, *The Economist*, April 8, 2020, https://www.economist.com/leaders/2020/04/08/open-standards-not-sanctions-are-americas-best-weapon-against-huawei.

[191] Nietsche and Rasser, "Washington's Reboot".

[192] "America Does Not Want China to Dominate 5G Mobile Networks.: It is Going About it the Wrong Way," Business—5Geopolitics, *The Economist*, April 8, 2020, https://www.economist.com/business/2020/04/08/america-does-not-want-china-to-dominate-5g-mobile-networks.

[193] "O-RAN Alliance Overview." O-RAN Alliance. Accessed April 2, 2020. https://www.o-ran.org/.

[194] Wheeler, "'Secret Sauce'".

[195] Mackenzie Eaglen, "What if the Pentagon Skipped 5G?," Ideas. *Defense One*, May 11, 2020, https://www.defenseone.com/ideas/2020/05/what-if-pentagon-skipped-5g/165277/; Hitchens, "US Risks".

employing a "distrust but verify"[196], mitigation strategy provides opportunities while both disincentivizing and proactively guarding against hostile actions[197]. In turn, Huawei's exclusion from the market does not diminish the risks that they and the PRC present, and arguably amplifies them. Surely, there must be a win-win option, and the UK, so far, seems to be pursuing it effectively. However, there is room for improvement.

[196] Cliff Kupchan and Paul Triolo, "Distrust but Verify: How the U.S. and China Can Work Together on Advanced Technology," Business and Tech—Opinion, *SupChina*, November 26, 2019, https://supchina.com/2019/11/26/distrust-but-verify-the-us-china-advanced-technology/.

[197] Julia Voo and Cindy Gao, "U.S.-China Cyber Competition and Cooperation with Julia Voo," By Joanna Chiu, Podcasts—NuVoices, *SupChina*, April 3, 2020, Audio, 54m:33s. https://supchina.com/podcast/u-s-china-cyber-competition-and-cooperation-with-julia-voo/.

5G Implications for Power

5G is said to be key to the domination of information technology, which in turn is said to be key for dominating the 21st century[198]. 5G networks are key to the Digital Silk Road[199], which will tie the PRC's Belt and Road Initiative together[200]. 5G networks will enable the wide-scale commercialisation of a plethora of new technologies, including quantum computing, artificial intelligence (AI), automated factories, autonomous cars, smart cities, augmented/virtual reality, and healthcare process optimisation. The full impact of these individual technologies on society is unknown. Their economic impacts are predicted to be great. However, their tactical[201] (though perhaps not strategic[202]) implications may be revolutionary[203] (with some caveats[204]).

5G itself has numerous military applications[205]. These applications are often overlooked in public discourse[206]. In addition to espionage, it is part of why 5G security remains a contentious area.

In the UK, other than the ban from critical core networks, and a 35% market share cap on high risk network vendors, Huawei's limits on the development of these technologies have yet to be defined. There are however valid concerns that Huawei's development of 5G networks will

[198] Allison, "AI Supremacy"; Hitchens, "US Risks".
[199] Clayton Cheney, "China's Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism," Blog—Net Politics, Council on Foreign Relations, September 26, 2019, https://www.cfr.org/blog/chinas-digital-silk-road-strategic-technological-competition-and-exporting-political.
[200] Andrew Chatzky and James McBride, "China's Massive Belt and Road Initiative," Backgrounder, Council on Foreign Relations, Accessed March 24, 2020, https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative.
[201] Mark Esper, "Global Security Forum: Emerging Technologies Governance," By Kathleen H. Hicks, Transcript, CSIS, January 24, 2020, https://www.csis.org/analysis/global-security-forum-emerging-technologies-governance.
[202] James Andrew Lewis, "Can Artificial Intelligence Compensate for Strategic Shortcomings?," Commentary, CSIS, January 29, 2020, https://www.csis.org/analysis/can-artificial-intelligence-compensate-strategic-shortcomings.
[203]Michael E. O'Hanlon, "Forecasting Change in Military Technology, 2020-2040," Research—Report, The Brookings Institution, September 2018, https://www.brookings.edu/research/forecasting-change-in-military-technology-2020-2040/.
[204] Laura Schousboe, "The Pitfalls of Writing About Revolutionary Defense Technology," Commentary, *War on the Rocks*, July 15, 2019, https://warontherocks.com/2019/07/the-pitfalls-of-writing-about-revolutionary-defense-technology/.
[205] William Schneider Jr,, "Why 5G is a Big Deal for Militaries Throughout the World," Opinion, *C4ISRNET*, February 5, 2019, https://www.c4isrnet.com/opinion/2019/02/05/why-5g-is-a-big-deal-for-militaries-throughout-the-world/.
[206] Erica D. Borghard and Shawn W. Lonergan. "The Overlooked Military Implications of the 5G Debate," Blog—Net Politics, Council on Foreign Relations, April 25, 2019, https://www.cfr.org/blog/overlooked-military-implications-5g-debate.

concentrate an unprecedented amount of power over these new technologies[207]. Such power could leave the UK and others at the whims of Huawei and, by extension, the PRC. Though hardly discussed, weaponization of IoT devices during conflict, as opposed to surveillance with or without conflict, is what is truly at the heart of the 5G debate[208].

Yet, this risk stems from a fear that has not yet manifested. Huawei's current success in the 5G market does not necessitate future dominance of the IoT market. While Huawei might have a head start, in relatively recent history the West has been more successful at creating new technologies and innovating procedures, due to more liberal values and institutions[209]. The PRC, on the other hand, has largely benefitted from a late-comer's advantage[210].

Now, with their forays into 5G and 6G technology, Huawei and the PRC hope to gain "first-mover status"[211]. First-mover status is not in of itself an inherent advantage[212]. It is indeed a double-edged sword[213]. However, in the case of 5G and 6G, particularly when linked with AI (see also), the stakes become much higher, likely enabling, and even permanently solidifying, the next era of unipolar hegemony[214]. With this understanding, the EU, UK, US, and China are already competing for 6G by 2030[215].

As a 2019 US Defense Innovation Board (DIB) report on 5G discusses, first-mover status has, "commercial, competitive, and security implications"[216], with advantages including setting the standards and specifications of infrastructure and other products. At the same time, the report notes that if first-movers fail to innovate, they fall significantly behind[217]. In the case of 5G and

---

[207] Bob Seely, Peter Varnish Obe, and John Hemmings, "Defending Our Data: Huawei, 5G, and the Five Eyes," Asia Studies Centre. Henry Jackson Society, May 2019, https://henryjacksonsociety.org/wp-content/uploads/2019/05/HJS-Huawei-Report-A1.pdf.

[208] "America Does Not Want China to Dominate 5G", *The Economist*.

[209] Regina M. Abrami, William C. Kirby, and F. Warren McFarlan, "Why China Can't Innovate," Innovation, *Harvard Business Review*, March 2014, https://hbr.org/2014/03/why-china-cant-innovate; Blanchard and Michael, "Innovation is 'Achilles Heel'".

[210] Justin Yifu Lin, "Advantage of Being a Latecomer," Opinion, *China Daily*, August 7, 2013, http://www.china.org.cn/opinion/2013-08/07/content_29646629.htm.

[211] Kennedy, "China's Uneven".

[212] William Boulding and Markus Christen, "First-Mover Disadvantage," Financial Management, *Harvard Business Review*, October 2001, https://hbr.org/2001/10/first-mover-disadvantage.

[213] Ronald Klingebiel and John Joseph, "When First Movers are Rewarded, and When They are Not," Innovation, *Harvard Business Review*, August 11, 2015, https://hbr.org/2015/08/when-first-movers-are-rewarded-and-when-theyre-not?referral=03759&cm_vc=rr_item_page.bottom.

[214] Allison, "AI Supremacy"; Indermit Gill, "Whoever Leads in Artificial Intelligence in 2030 Will Rule the World Until 2100," Blog—Future Development, The Brookings Institution, January 17, 2020, https://www.brookings.edu/blog/future-development/2020/01/17/whoever-leads-in-artificial-intelligence-in-2030-will-rule-the-world-until-2100/.

[215] Martijn Rasser, "Setting the Stage for U.S. Leadership in 6G," Cyber & Technology, *Lawfare*, August 13, 2019, https://www.lawfareblog.com/setting-stage-us-leadership-6g.

[216] Medin et al., "5G Ecosystem", p. 6.

[217] Ibid, p. 6-7.

6G, this puts the West in a dicey, but perhaps advantageous position[218].

Indeed, while stating that a full ban is the most secure approach, Dr. Lewis also acknowledges the UK and Europe's economic interests in collaborating with Huawei and the PRC. While the Five-Eyes partners, Europe, Japan, and South Korea all are more competitive in the 5G realm than discourse often suggests, and the preferred Western 5G companies, Nokia, Ericsson, and Samsung are of better quality than Huawei, each are interdependent[219]. If the Western countries and allies can work together on their economic, security, legal, and civic concerns, they can benefit in the short term by working with Huawei and the PRC, while also taking the lead in the long term. However, Dr. Lewis warns, while the US in particular is primed to be a 5G market leader, its global leadership, in general and when it comes to 5G and cybersecurity, is lacking[220].

As a whole, this seems to strengthen the economic integration case for the UK Tapping into the industrial power that the PRC and Huawei provide enables the West to develop the necessary industry to respond with innovation and specialisation in a way the PRC model does not. This symbiosis may also discourage the PRC from using Huawei maliciously as they are at risk of being deprived of what their economic model has typically failed to produce – ingenuity.

The trickle-down effects that enabling Huawei has on the domestic market permits alternative telecommunication competitors to compete in their respective specialist capacities while Huawei provides the bulk of equipment. This should reduce the concentration of power Huawei has by defining niche roles in the market not provided by Huawei. In turn, Huawei's production capacity can spur growth in these niche industries.

Preventing Huawei's entrance into the UK market reduces the prospect of having a competitive IoT market in future. Having to rely on more expensive telecommunications providers increases start-up costs, reduces available capital for research and development projects and hampers innovation. The UK's free market structure benefits from Huawei's production margins by being responsive to the market conditions. Enabling 5G will bring the necessary surge of creativity that prompts industry to respond to the demand where Huawei fails to deliver. Thus, when weighing the risks, opportunities, costs, and benefits, allowing Huawei to develop 5G in the UK would appear to be a better choice than barring them from the market.

---

[218] Medin et al. "5G Ecosystem"; Budden and Murray, "Defense Innovation"; Morgan Dwyer, "An Alternative to the Defense Department's New, Technology-Focused Organizations," Commentary, CSIS, January 22, 2020, https://www.csis.org/analysis/alternative-defense-departments-new-technology-focused-organizations; Hicks et al., "Getting Less".

[219] Lewis, "Statement 5G"; "Senate 5G".

[220] James Andrew Lewis, "Cyber Solarium and the Sunset of Cybersecurity," Commentary, CSIS, March 13, 2020, https://www.csis.org/analysis/cyber-solarium-and-sunset-cybersecurity.

UK-US Relations

Due in part to 5G policies concerning Huawei, Anglo-American defense and intelligence relationships have become increasingly strained. In May 2019, US President Trump threatened to limit intelligence sharing, should Huawei be allowed to develop 5G in the UK[221]. On January 27, 2020, US Senators introduced legislation to limit intelligence sharing with any country that allows Huawei to develop their 5G networks. Some Senators explicitly threatened the UK-US intelligence relationship[222]. This would seem drastic, and even counterproductive, given the benefits and risks of US foreign intelligence sharing[223], and the US failure to offer an alternative solution.

The policy outcomes of such threats were hard to predict when this essay was first drafted in the summer of 2019, due to the election of UK Prime Minister Johnson. Since then several developments have eliminated some ambiguity. Others have reinforced the relevance of the 2019 draft's arguments for a mitigation strategy and partial ban.

Shockingly, UK officials have declared that they are reconsidering their intelligence and defense partnerships with the US This seems to be a result of Trump's isolationist policies, the threats over Huawei, and particularly the US Soleimani assassination[224]. In a January 12, 2020 interview, UK Defense Secretary Wallace stated that he worries about the US's withdrawal from global leadership. Wallace also stated that the UK is overly reliant on US, "air cover … intelligence, surveillance, and reconnaissance assets" [225], and that the UK must begin diversifying such partnerships.

Likely with such developments in mind, on January 28, 2020, Prime Minister Boris Johnson and his National Security Council decided that they would allow, "high risk vendors", including Huawei, to provide components for UK wireless and 5G infrastructure. Such vendors

---

[221] Telegraph Reporters, "Donald Trump Could 'Limit Sharing of US Intelligence With the UK 'if Britain ' Fails to Ban Huawei," Technology Intelligence, *The Telegraph*, May 31, 2019, https://www.telegraph.co.uk/technology/2019/05/31/donald-trump-could-limit-sharing-us-intelligence-uk-britain/.

[222] Joe Gould, "Key Republicans Seek Ban on Intel Sharing with Countries that Use Huawei," 5G, *C4ISRNET*, January 27, 2020, https://www.c4isrnet.com/congress/2020/01/27/key-republicans-seek-ban-on-intel-sharing-with-countries-that-use-huawei/.

[223] Michael E. DeVine, "United States Foreign Intelligence Relationships: Background, Policy and Legal Authorities, Risks, Benefits," Report, Congressional Research Service, May 15, 2019, https://fas.org/sgp/crs/intel/R45720.pdf.

[224] Adam Bienkov, "The UK is Abandoning Its Alliance with Trump as the United States 'Withdraws from Its Leadership Around the World'," Analysis, *Business Insider*, January 12, 2020, https://www.businessinsider.com/uk-abandoning-trump-iran-us-withdraw-leadership-world-qassem-soleiman2020-1.

[225] Tim Shipman, "Ben Wallace Interview: We Can't Rely on US," News, *The Sunday Times*, January 12, 2020, https://www.thetimes.co.uk/edition/news/ben-wallace-interview-we-cant-rely-on-us-pmwcgv398?wgu=270525_54264_15817040629028_276d8c4cf9&wgexpiry=1589480062&utm_source=planit&utm_medium=affiliate&utm_content=22278.

will be limited to providing components that are, "not seen as posing a threat to the integrity of the system[s]"[226].

In early May 2020, members of the US Congress proposed an amendment to the upcoming defense budget which would prevent the purchase of US F-35 Joint Strike Fighters (JSF) by nations allowing high-risk vendors in their 5G and 6G networks. Nine nations are in the JSF program: the US, the UK, the Netherlands, Italy, Australia, Norway, Denmark, Canada, and Turkey. Additional customers include Israel, South Korea, Belgium, Japan, Poland, and Singapore. Canada has yet to commit to purchasing the F-35 and Turkey was banned over its purchase of the new Russian missile systems[227].

The UK has taken this as a jarring development, particularly given current global instability and US threats, and is seeking to ensure this amendment is not passed. More than anything, it appears to be another instance of a counterproductive diplomatic pressure by the US. Many of the nations it wishes to purchase, and more importantly partake in, the JSF program already have Huawei providing network components generally and for 5G.

Nevertheless, it is unlikely that the "special" US-UK intelligence sharing relationship would end[228]. While it could potentially be impacted by political backlash in the short term, the US's National Security Agency is still reliant on GCHQ's network of overseas listening posts to collect data. Additionally, the US limiting intelligence sharing with the UK would not only require an overhaul of the US-UK partnership, but would also impact the remaining Five Eyes partners, as around 80% of all intelligence is currently shared[229].

Such changes would harm intelligence operations for all stakeholders. Just as not working with Huawei to develop 5G would set back many countries by five to ten years, with the US yet to offer a viable alternative[230]. These facts must be weighed against the risk of Huawei being able to monitor various communications.

The ties that keep the UK and US relationship together are, for now, stronger than

---

[226] Adam Satariano, "Britain Defies Trump Plea to Ban Huawei from 5G Network," Technology, *The New York Times*, January 28, 2020, https://www.nytimes.com/2020/01/28/technology/britain-huawei-5G.html.

[227] Peter Suciu, "Tom Cotton is Trying to Block F-35 Deployment to the UK (Due to Huawei Worries)," Blog—The Buzz, *The National Interest*, May 8, 2020, https://nationalinterest.org/blog/buzz/tom-cotton-trying-block-f-35-deployment-uk-due-huawei-worries-152251; Oriana Pawlyk and Richard Sisk, "Lawmakers Consider Blocking Some F-35 Deployments Over Huawei 5G Network: Reports," News, *Military.com*, May 13 2020, https://www.military.com/daily-news/2020/05/13/lawmakers-consider-blocking-some-f-35-deployments-over-huawei-5g-network-reports.html.

[228] Michael S. Goodman, "The Foundations of Anglo-American Intelligence Sharing," *Studies in Intelligence* 59, no. 2 (Extracts, June 2015): 1-12, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-59-no-2/pdfs/Goodman-Evolution-UK-US-JIC-June-2015.pdf.

[229] David Bond and Jim Pickard, "US Intelligence Threats to Britain 'Not Realistic', Say Spies," Political Espionage, *Financial Times*, May 31, 2019, https://www.ft.com/content/8cdc7aee-83aa-11e9-b592-5fe435b57a3b.

[230] Gould, "Key Republicans".

Huawei's risks threatening to destroy it. By acknowledging Huawei's threat, the impetus is put on intelligence agencies to consider new methods to counter those risks, i.e. limiting the threat of foreign actors in critical networks, which the UK now seems to be in the process of doing[231]. In a complex, globalized, world, multidimensional assessments of partnerships, their risks, costs, benefits, and opportunities to build trust, must be made. Elsewise everyone loses[232]. Regardless of the US position, the UK's oversight of Huawei and similar entities could greatly aid in such threat mitigation, particularly if the oversight becomes an international endeavor.

Exclusion of Huawei from the market does not resolve the inherent issue of distrust of the PRC. In fact, exclusion of Huawei encourages further hostility from the PRC, in a world where it is almost impossible to not work with the PRC. Being anti-Huawei in policy at a national level and pressuring other international partners to adopt similar measures disrupts security, the market, and is detrimental to all sides. This would seem especially true given Huawei's technological position ahead of competitors.

[231] Satariano, "Britain Defies"; "5G Round Up", NCSC.

[232] Richard Oliver, "Partnership and Security: Advancing US/UK Defense Technology Relationship in the Era of Globalization," Event—Summary Transcript, Edited by Peter Bean, Wilson Center, July 12, 2005, https://www.wilsoncenter.org/event/partnership-and-security-advancing-the-usuk-defense-technology-relationship-the-era; Nietsche and Rasser, "Washington's Reboot".

Part Three—Opportunities, Challenges, and Solutions

Opportunities

Internationalising HCSEC

There is potential to reframe the previous and the following problems as opportunities for the UK. Of Huawei's client states, the UK appears to have taken cybersecurity the most seriously with the establishment and dedication of resources to HCSEC. By taking the lead, particularly via a multilateral approach, the UK and the HCSEC can become a rallying institution for the world to hold Huawei to account for better cybersecurity practices multilaterally. Further, the UK is in a unique position to hold the PRC accountable by holding Huawei accountable.

The PRC typically escapes international accountability through practice of its Security Council veto powers and its ability to demand bilateral rather than multilateral negotiations[233]. If the UK internationalises HCSEC and more aggressively expands its existing security agreements, this potential to hold Huawei and the PRC to account could be greatly amplified. With the EU following the UK's recent examples in cybersecurity and cooperation when it comes to Huawei, a mitigation coalition may become a reality[234].

In the context of Brexit, the UK's cybersecurity relationship with the EU will be maintained until December 2020 before being re-examined and possibly extended. Any extensions or re-negotiations will almost certainly include discussions of 5G and 6G policies[235], and the UK's next National Cyber Security Strategy[236]. When the time comes the UK should emphasise, or perhaps even leverage, their unique assets and capabilities relative to Huawei, 5G, and 6G, as embodied by HCSEC.

If the US can be convinced to collaborate with allies and partners instead of dictating, as per its January 2020 House bill[237] and its Congressional Cyberspace Solarium Commission Report, released March 11, 2020[238], all the better. However, Dr. Lewis argues in his review of the report that while its call for the creation and enforcement of cybersecurity norms by leading a

---

[233] Sylvia Hui, "Engaging an Emerging Superpower: Understanding China as a Foreign Policy Actor," Asia Programme Paper, Chatham House, July 2011, https://www.chathamhouse.org/sites/default/files/0711pp_hui.pdf; China Team, "The Costs of International Advocacy: China's Interference in United Nations Human Rights Mechanisms," Report, Human Rights Watch, September 5, 2017, https://www.hrw.org/report/2017/09/05/costs-international-advocacy/chinas-interference-united-nations-human-rights.

[234] "EU Deals," CNBC via Reuters.

[235] Doug Olenick, "Brexit Cybersecurity Implications Hold Steady During Transition Period," Security News, *SC Magazine*, January 31, 2020, https://www.scmagazine.com/home/security-news/brexit-cybersecurity-implications-hold-steady-during-transition-period/.

[236] "National Cyber," HM Government; "National Progress," HM Government.

[237] Emily Birnbaum, "House Passes Bills to Gain Upper Hand in Race to 5G," Policy, *The Hill*, January 08, 2020, https://thehill.com/policy/technology/477429-house-passes-bills-to-gain-upper-hand-in-race-to-5g.

[238] U.S. Cyberspace Solarium Commission, Chaired by Angus King and Mike Gallagher, "Report," US Congress, March 11, 2020, https://www.solarium.gov/report.

coalition of democracies is a strength, it was significantly undermined by several issues. These were report's emphasis on deterrence (which is passive and circumventable), the current partisanship in US politics, and particularly the current leadership in and throughout the executive branch[239].

Dr. Lewis analysis strengthens the arguments for the UK to take the lead. Internationalising the HCSEC could significantly enhance both its and the UK's ability to identify and rectify cybersecurity threats to current, 5G, and 6G infrastructure. Internationalising the HCSEC could also give the UK and its partners greater leverage when it comes to incentivising Huawei, ZTE (another PRC telecom company), and the PRC to pursue better cybersecurity and trade practices. Such a coalition would be mutually beneficial for governments, private entities, and consumers around the world.

Further, such a coalition could be well positioned to be proactive as 6G emerges, perhaps taking a leadership role in the annual 6G Wireless Summit (founded 2019)[240], particularly as the US struggles to set the stage for 5G and 6G leadership[241]. By early 2019 Huawei had already set its sights on dominating 6G in terms of R&D and intellectual property[242]. Between Huawei's difficulties in the West with 5G and its vision for 6G supremacy (which has even resulted in its consideration of forsaking control of 5G in the West)[243], an internationalisation of an entity like the HCSEC could become an invaluable geopolitical tool.

However, the focus of entities like the HCSEC should not simply be on Huawei. It is worth asking, why is Huawei held to such a unique degree of scrutiny? Why is there no Cyber Security Evaluation Centre for ZTE? Sure it is smaller than Huawei, but it allegedly was created for espionage[244], has a history of corruption[245], and it was even important enough for the PRC to ask President Trump to give it special treatment and exemptions[246], which he granted in spite of its broader consequences[247]. ZTE aside, why is there no Cyber Security Evaluation Center for

---

[239] Lewis, "Cyber Solarium".

[240] 6G Wireless Summit. http://www.6gsummit.com/

[241] Rasser, "Setting 6G"; Kania, "Why Doesn't".

[242] Iain Morris, "Huawei Sets Sights on 6G Stardom Amid 5G Strife," 5G, *Light Reading*, February 15, 2019, https://www.lightreading.com/mobile/5g/huawei-sets-sights-on-6g-stardom-amid-5g-strife/d/d-id/749497.

[243] Morris, "6G Arms Race".

[244] Tara Francis Chan, "The Very Purpose of the Chinese Tech Company ZTE is to Spy on Other Countries, a Competitor Alleges in New Court Documents," *Business Insider*, June 1, 2018, https://www.businessinsider.com/zte-created-to-spy-according-to-new-court-documents-2018-6.

[245] "ZTE," News—Topics, Anti-Corruption Digest, Accessed March 3, 2020, https://anticorruptiondigest.com/news-topics/zte/#axzz6Hk3lzgYv.

[246] Henry Farrell, "Bolton Alleges that Trump Helped Out China's Leader on ZTE. What's ZTE?," News— Monkey Cage—Analysis, *The Washington Post*, January 28, 2020, https://www.washingtonpost.com/politics/2020/01/28/bolton-alleges-that-trump-helped-out-chinas-leader-zte-whats-zte/.

[247] Ewan Sutherland, "The Strange Case of US v. ZTE: A Prosecution, a Ban, a Fine and a Presidential Intervention," *Digital Policy, Regulation and Governance* 21, no. 6 (2019): 550-573, https://doi.org/10.1108/DPRG-04-2019-0029.

Western favored tech companies Ericsson, Nokia, Samsung, or Apple?

Make HCSEC ICSEC

As the remainder of this paper demonstrates, Huawei is not the only way for the PRC or other actors to carry out malicious acts. There is a clear need for an international body coordinating 5G, 6G, and cyber security more broadly. While others have called for such an entity, there has been a lack of leadership.

Further, many of the reasons why *all* 5G and IoT companies should be subject to greater scrutiny are missed by focusing on Huawei[248]. In examining these reasons, there is a strong case to be made that UK can and should create an International Cyber Security Evaluation Center (ICSEC), focusing on more than just Huawei. In doing so they could scale up their existing proactive approach and improve it with the help of others.

On the one hand, security concerns are not egalitarian because Western favored tech companies have had a greater culture of integrating security as part of the industrial design process, rather than retroactively including security post-completion of core processes[249]. On the other, both Western and Western preferred companies and governments alike have their own security issues and risks.

These are primarily a result of their supply chains, infrastructure and services (including poor source codes), devices, and, less discussed, corruption and other internal human security liabilities[250]. An examination of supply chain issues, the 5G front runners favored by the West and their allies, and cruxes including the natures of 5G and cybersecurity, demonstrates the need for more than an international coalition just focused on Huawei—the need for ICSEC.

Cyber Security Policy Hub

WEGNER, INTERNATIONAL BUREAU OF CYBER STATISTICS (SEE COMPLEXITY SECTION), NEXT GOV TRANSPARENCY ARTICLE, STEIGER + VALERIANO FOR WAYS TO IMPROVE MODELS OF CYBER CONFLICT

KOLTON TO BETTER COORDINATE THE FORMULATION, COMMUNICATION, AND REINFORCEMENT OF CYBER DOCTRINES

[248] Wheeler and Simpson, "5G requires".
[249] Rich Mogull, "Apple's Security Strategy: Make it Invisible," Business—Security—Opinion, *MacWorld*, June 14, 2013, https://www.macworld.com/article/2041724/apples-security-strategy-make-it-invisible.html.
[250] Medin et al., "5G Ecosystem"; Wheeler and Simpson, "5G Requires".

Challenges

Supply Chains

Jon Boyens is the Deputy Chief of the Computer Security Division and Program Manager for Cyber Supply Chain Risk Management at the US National Institute of Standards and Technology.

In spite of 5G RAN hardware supply chains being relatively secure, more needs to be done to secure 5G RAN supply chains and supply chains more broadly[251]. Though far from a great metric, the UK's 2016-2021 National Cyber Security Strategy only mentions supply chains three times, and its 2019 progress report only mentions them twice[252]. Indeed, as recently as 2020 it appears that UK and US public and private authorities have dragged their feet when it comes to more aggressively addressing supply chain threats[253], though the coronavirus created a focus on supply chain risks[254]. Due to available sources and the US's claims of higher standards, this section focuses on US (defense) supply chain problems, which are arguably similar to the UK's.

To begin with, the US defense industry has a variety of (cyber)security related supply chain problems[255]. These often involve the contractors and the PRC[256], and are aggravated by a wider history of corruption[257]. Willful fraud, motivated by greed, results in a variety of

---

[251] "UK Telecoms Supply Chain Review Report," Notice, Department for Digital, Culture, Media & Sport, HM Government, July 22, 2019, https://www.gov.uk/government/publications/telecoms-supply-chain-review-terms-of-reference; Wheeler and Simpson, "5G Requires"; Sullivan and Lucas, "5G Cyber".

[252] "National Cyber," HM Government; "National Progress," HM Government.

[253] Wheeler and Simpson, "5G Requires"; Trevor Taylor and Rebecca Lucas, "Management of Cyber Security in Defense Supply Chains," *RUSI News Brief*, April 24, 2020, https://www.rusi.org/publication/rusi-newsbrief/management-cyber-security-defence-supply-chains.

[254] Conrad Prince, "The Coronavirus Pandemic and the Cyber Landscape," Commentary, RUSI, April 20, 2020, https://rusi.org/commentary/coronavirus-pandemic-and-cyber-landscape.

[255] Medin et al., "5G Ecosystem"; Ariel (Eli) [*sic*] Levite, "ICT Supply Chain Integrity Principles for Governmental and Corporate Policies," Paper, The Carnegie Endowment for International Peace, October 4, 2019, https://carnegieendowment.org/2019/10/04/ict-supply-chain-integrity-principles-for-governmental-and-corporate-policies-pub-79974; "Supply Chain Risk Management," The National Counterintelligence and Security Center, Office of the Director of National Intelligence, Accessed March 15, 2020, https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-supply-chain-threats.

[256] Steven Aftergood, "Defense Contracting Fraud: A Persistent Problem," Blogs—Secrect News—Dept of Defense, Federation of American Scientists, May 10, 2019, https://fas.org/blogs/secrecy/2019/05/defense-contracting-fraud/; Darrel Williams, "US Logistics Boss Talks Risks to the Supply Chain and Protective Measures," By Jill Aitoro, Interviews, *DefenseNews*, October 28, 2019, https://www.defensenews.com/interviews/2019/10/28/us-logistics-boss-talks-risks-to-the-supply-chain-and-protective-measures/.

[257] Philip M. Nichols, "To Whom Does a Defense Business Owe a Duty When There is an Opportunity to Pay a Bribe?," In *Ethical Dilemmas in the Global Defense Industry*, edited by Claire Finkelstein, Kevin Govern, and Daniel Schoeni, (pages tba), New York: Oxford University Press, 2020 (to be released).

cybersecurity[258] and other threats[259] that jeopardize security, operations, and personnel. There also seems to be a problem with defense industry members selling sensitive assets or being compromised by foreign investment, with little oversight or repercussions[260].

This is all complicated by the PRC being one of the largest customers of defense contractors in key industries, some of which are helping build and export the PRC's authoritarian model[261]. These industries in turn can use their lobbying powers to influence the US government. Of particular concern and influence is the semiconductor industry, which the PRC relies on the US for currently, and which has become increasingly important in the era of 5G, AI, and quantum computing[262].

In February 2020, the Trump administration proposed closing a loophole on the ban that prevents US companies from selling technology components to Huawei. DoD intervened on behalf of industries that were concerned about how the restrictions would directly and indirectly impact their trade with the PRC and those it might influence[263]. With the semiconductor industry particularly concerned about how its diminished sales to Huawei might impact their ability to produce goods for US security, the lobbying temporarily halted the plans[264]. After intense debate the DOD reversed course[265]. As of writing, a final decision hasn't been announced.

As Dr. Lewis writes, there are strong reasons to continue exporting semi-conductors to

---

[258] Jonathan Dienst, Joe Valiquette, and Rich Schapiro, "New York Tech Firm Sold Chinese Equipment to U.S. Military, Feds Say," U.S. News, NBC News, November 7, 2019, https://www.nbcnews.com/news/us-news/feds-raid-new-york-tech-firm-suspected-selling-chinese-equipment-n1078191.

[259] Kyle Rempfer, "DoD Bought Phony Military Gear Made in China, Including Counter-Night Vision Clothing that Didn't Actually Work," News—Your Military, *Military Times*, May 30, 2019, https://www.militarytimes.com/news/your-air-force/2019/05/30/dod-bought-phony-military-gear-made-in-china-including-counter-night-vision-clothing-that-didnt-actually-work/.

[260] Sean Gallagher, "How US Software Ended Up Powering Chinese Assault Helicopters," Policy, *Ars Technica*, July 3, 2012, https://arstechnica.com/tech-policy/2012/07/how-us-software-ended-up-in-chinese-assault-helicopters/; Cory Bennett and Bryan Bender, "How China Acquires 'the Crown Jewels ' of U.S. Technology," Investigation, *Politico*, May 22, 2018, https://www.politico.com/story/2018/05/22/china-us-tech-companies-cfius-572413.

[261] Lindsay Gorman and Matt Schrader, "U.S. Firms Are Helping Build China's Orwellian State," Argument, *Foreign Policy*, March 19, 2019, https://foreignpolicy.com/2019/03/19/962492-orwell-china-socialcredit-surveillance/.

[262] Lewis, "Statement Judiciary".

[263] Sanger and Perlroth, "Huawei Winning".

[264] William Alan Reinsch, "Walk the Line," Commentary, CSIS, February 3, 2020, https://www.csis.org/analysis/walk-line.

[265] Ellen Nakashima, Jeanne Whalen, and David J. Lynch, "Pentagon Drops Opposition to New Rules that would Further Restrict Tech Sales to Huawei," Technology, *The Washington Post*, February 15, 2020, https://www.washingtonpost.com/technology/2020/02/14/pentagon-drops-opposition-new-rules-that-would-further-restrict-tech-sales-huawei/.

the PRC[266]. Specifically, there is no stopping the PRC from achieving its own self-sufficient semiconductor industry, and any drastic restrictions would only hurt the US, US semiconductor companies, and US companies and allies reliant on those companies (particularly Taiwan[267]). Similarly, in the globalized world, traditional export control policies are not effective, and implementing them will only accelerate the development of the PRC's more advanced semiconductor producers.

Dr. Lewis argues that the US need not exclude the PRC, or even Huawei, from semiconductor exports. Rather, the interests of the US would be better served if export controls are carefully employed as part of a larger strategy. Dr. Lewis suggests that the US allow semiconductor manufacturing equipment to be exported to the PRC but only to US and trusted, non-PRC owned, firms.

The US should also work with allies to advance semiconductor research and manufacturing capacities, put pressure on the PRC's market manipulations and intellectual property theft, and increase counterintelligence efforts, focusing not on students but handlers. This is echoed by other security experts concerned with more aggressively containing or countering Huawei's and the PRC's risks, while also avoiding winning the battle just to lose the war by sacrificing the current liberal order, values, and interests[268]. Though we won't detail them here, there are also concrete steps that liberal governmental and non-governmental institutions should take to improve the security and prosperity of their R&D relationships with the PRC[269].

That being said, since the DOD's reversal, in part due to the coronavirus, two other supply chain risks have come into focus. The first is predatory foreign lending, largely by the PRC, targeting a wide variety of tech firms inside and outside the defense industry[270]. The second is that smaller defense contractors are relying on PRC based companies' technology. These companies represent a quarter of the US defense industry and are currently lobbying for the August 2020 technological transition deadline to be moved to February 2021[271].

Examples like these demonstrate a clear need for comprehensive risk mitigation, capable

---

[266] James Andrew Lewis, "Managing Semiconductor Exports to China," Commentary, CSIS, May 5, 2020, https://www.csis.org/analysis/managing-semiconductor-exports-china.
[267] Cheng Ting-Fang and Lauly Li, "Chip Titan TSMC Caught in Crossfire between US and China," Business—Company in Focus, *Nikkei Asian Review*, May 15, 2020, https://asia.nikkei.com/Business/Company-in-focus/Chip-titan-TSMC-caught-in-crossfire-between-US-and-China.
[268] Kania and Gorman, "United Talent"; Lairson, Skidmore, and Xinbo, "US Backfired"
[269] David Zweig and Siqin Kang, "America Challenges China's National Talent Programs," Report, CSIS, May 5, 2020, https://www.csis.org/analysis/america-challenges-chinas-national-talent-programs.
[270] Valerie Insinna, "Pentagon Reports Boost in Predatory Foreign Investment to US Tech Firms Amid Pandemic," *C4ISRNET*, May 6, 2020, https://www.c4isrnet.com/unmanned/2020/05/06/pentagon-reports-boost-in-predatory-foreign-investment-to-us-tech-firms-since-pandemic-start/.
[271] Andrew Eversden, "Proposed Rule Banning Chinese Tech Needs to Consider Small Contractors, Senators Warn," Capital Hill, *Fifth Domain*, May 5, 2020, https://www.fifthdomain.com/congress/capitol-hill/2020/05/05/proposed-rule-banning-chinese-tech-needs-to-consider-small-contractors-senators-warn/.

of addressing internal and external factors. Securing supply chains must go beyond government questionnaires for partners, and other current standards. There needs to be an integrated attempt to gather data on both more traditional internet based cyber threats, including malware, and on the interactions and conversations of malicious actors in places like the dark web, giving a "'total picture' view"[272].

Some nations are slowly trying to make this happen, but maximum efficacy will require an international effort and collaborative leadership. Such leadership is unlikely to come from the US any time soon. Domestically and internationally, the US, "is faltering due to a lack of coherent policy on a wide swathe of foundational issues such as spectrum management for 5G usage, network supply chain security, infrastructure development and data sharing, experts say"[273].

5G Front Runners

On the corporate side, of Western favored 5G front runners, only Apple and Samsung appear to have relatively minimal issues with corruption and security. Apple relies extensively on the PRC for its phone production, and appears to have had minimal corruption issues, likely due to its oversight and intolerance of corruption[274]. However, there has been at least one recent alleged corruption case directly involving Apple employees, which occurred in the PRC. An investigation by Apple appears to have cleared these claims[275].

More significantly, Apple has long claimed their products and firm are virtually un-hackable. Recent events have proven otherwise. In 2018 and Australian teen hacked into their secure computer systems[276]. In 2019 Google found that Apple products have been hackable for years.

All it took was visiting the wrong website, or other black market exploits (even bought or made by governments)[277]. Google also found, and Apple acknowledged, that the PRC hacked

---

[272] Brian Garmey, "How Federal Agencies Can Better Manage Supply-Chain Cyber Risks," Opinion, *Fifth Domain*, July 17, 2019, https://www.fifthdomain.com/opinion/2019/07/17/how-federal-agencies-can-better-manage-supply-chain-cyber-risks/.

[273] Hitchens, "US Risks".

[274] Christian Zibreg, "Corrupt Apple Manager Who Leaked Order Secrets to Asian Suppliers Brought to Justice," Apple, *Geek.com*, August 16, 2010, https://www.geek.com/apple/corrupt-apple-manager-who-leaked-order-secrets-to-asian-suppliers-brought-to-justice-1277412/.

[275] Yoko Kubota and Tripp Mickle, "Apple Investigated Possible Business Misconduct in its Supply Chain: Company Says it Found No Evidence of Bribery or Kickbacks," Tech, *The Wall Street Journal*, November 30, 2018, https://www.wsj.com/articles/apple-investigated-possible-business-misconduct-in-its-supply-chain-1543620611.

[276] Erin Pearson, "Melbourne Teen Hacked into Apple's Secure Computer Network, Court Told," Crime, *The Age*, August 16, 2018, https://www.theage.com.au/national/victoria/melbourne-teen-hacked-into-apple-s-secure-computer-network-court-told-20180816-p4zxwu.html.

[277] John Naughton, "Think Your iPhone is Safe from Hackers?: That's What They Want You to Think," Technology—Opinion, *The Guardian*, September 8, 2019, https://www.theguardian.com/technology/commentisfree

Apple products to surveil and imprison Uighur Muslims, possibly for two years. Both companies declined to mention the PRC for fear of retaliation, as the Uighurs have been used as slave labor for Apple, Google, Dell, Microsoft, and other companies, often via Foxconn[278].

Taiwanese manufacturing giant, Foxconn, is Apple's largest manufacturer, and it manufactures a significant number of Apple's products in its PRC based factories. Foxconn has its own instances of corruption involving Apple products[279]. Both corruption and its dependence on the PRC pose various supply chain based risks. Foxconn has also experienced major data breaches. Two were by the same hacking group (2012 and 2019)[280], and at least one other was by a different group in 2015[281]. These hacks appear to have yielded access to a variety of technical and personnel data, which was and still could be leveraged in a variety of ways.

In October 2019, Samsung ended its mobile phone production in the PRC, moving production to other Southeast Asian countries[282], though this does not make it immune to PRC based risks. South Korea's corruption culture[283], which has impacted Samsung[284], combined with

---

/2019/sep/08/iphone-safe-from-hackers-think-again-ios-android-zero-day-exploit-zerodium-google-threat-analysis; Olivia Solon, "iPhone Spyware Lets Police Log Suspects' Passcodes when Cracking Doesn't Work," Tech—Security, *NBC News*, May 18, 2020, https://www.nbcnews.com/tech/security/iphone-spyware-lets-cops-log-suspects-passcodes-when-cracking-doesn-n1209296.

[278] Patrick Howell O'Neill, "Apple Says China's Uighur Muslims were Targeted in the Recent iPhone Hacking Campaign," Computing, *MIT Technology Review*, September 6, 2019, https://www.technologyreview.com/2019/09/06/133138/apple-says-chinas-uighur-muslims-were-targeted-in-iphone-hacking-campaign/; Jeremy Horwitz, "Apple, Foxconn, and 81 Others are Using Uighur Forced Labor," Mobile. *Venture Beat*, March 2, 2020, https://venturebeat.com/2020/03/02/apple-foxconn-and-81-others-are-accused-of-using-uighur-forced-labor/.

[279] Aries Poon, "In Taiwan, Five Ex-Foxconn Employees are Indicted," Business, *The Wall Street Journal*, May 21, 2014, https://www.wsj.com/articles/five-former-foxconn-employees-indicted-for-accepting-bribes-1400651370?tesla=y; Malcom Owen, "Foxconn Investigating $43M Fraud Ring Involving Faulty iPhone Parts," Articles, Apple Insider, December 18, 2019, https://appleinsider.com/articles/19/12/18/foxconn-investigating-43m-fraud-ring-involving-faulty-iphone-parts.

[280] Juliette Garside, "Apple Supplier Foxconn Hacked in Factory Conditions Protest," Technology—Apple. February 9, 2012, https://www.theguardian.com/technology/2012/feb/09/apple-foxconn-hackers-factory-conditions; Duncan DeAeth, "Taiwan's Foxconn Victim of Webmail System Hack, Employee Data Compromised," Business, *Taiwan News*, April 15, 2019, https://www.taiwannews.com.tw/en/news/3680809.

[281] Kim Zetter, "Attackers Stole Certificate from Foxconn to Hack Kaspersky with Duqu 2.0," *WIRED*, June 15, 2015, https://www.wired.com/2015/06/foxconn-hack-kaspersky-duqu-2/.

[282] Ju-min Park, "Samsung Ends Mobile Phone Production in China," Technology News, *Reuters*, October 2, 2019, https://www.reuters.com/article/us-samsung-elec-china/samsung-ends-mobile-phone-production-in-china-idUSKBN1WH0LR.

[283] Justin Fendos, "South Korea's Corruption Culture," The Koreas, *The Diplomat*, November 17, 2016, https://thediplomat.com/2016/11/south-koreas-corruption-culture/.

[284] Heekyong Yang, "Samsung Sets Up Anti-Corruption Panel as Chief Faces Trials," Technology News, *Reuters*, January 8, 2020, https://www.reuters.com/article/us-samsung-group-compliance/samsung-sets-up-anti-corruption-panel-as-chief-faces-trials-idUSKBN1Z80DR.

South Korea's use of Huawei for its 5G networks[285] and its relations with the PRC[286], certainly make it an appealing target for the PRC to exploit. South Korea's security and intelligence apparatuses do not engender confidence in counterespionage[287]. However, there is seemingly no published English language instance of Samsung having any corruption issues involving the PRC. In either case, neither Samsung nor Apple appears to compete globally in 5G infrastructure, and focus on phone production instead (though Samsung is starting to focus on open network design[288]).

Of greater concern are the 5G infrastructure front runners favored by the West, Nokia and Ericsson. Both are shifting some of their production to other parts of the world due to US bids and concerns, which may mitigate manufacturing based security issues. However, corruption may in fact be more insidious for the two companies and their security.

Ericsson's problems are more direct and serious. In 2019 Ericsson and its subsidiaries were recently found to have a pervasive and international culture of corruption for close to two decades, in countries including the PRC[289]. Its corruption involved high-level executives, and has so far resulted in over $1 billion USD in fines and over 50 employees being dismissed[290].

Nokia's corruption related security risks are more nebulous, and less directly linked to Nokia itself. Nokia is dealing with ongoing legal problems[291], rooted in their 2016, 5G oriented[292], acquisition of French company Alcatel-Lucent. Alcatel (France) and Lucent (US)

---

[285] Richard L. Armitage and Victor Cha, "The 66-Year Alliance Between the U.S. and South Korea is in Deep Trouble," Newsletter, CSIS, November 25, 2019, https://www.csis.org/analysis/66-year-alliance-between-us-and-south-korea-deep-trouble; Clara Gillispie, "South Korea's 5G Ambitions," Academic Paper Series, Korea Economic Institute of America, March 23, 2020, http://keia.org/sites/default/files/publications/kei_aps_gillispie_200316.pdf.

[286] Uri Friedman, "How to Choose Between the U.S. and China? It's Not That Easy," Politics, *The Atlantic*, July 26, 2019, https://www.theatlantic.com/politics/archive/2019/07/south-korea-china-united-states-dilemma/594850/.

[287] "Risks of Intelligence Pathologies in South Korea," Asia, Report 259, International Crisis Group, August 5, 2014, https://www.crisisgroup.org/asia/north-east-asia/korean-peninsula/risks-intelligence-pathologies-south-korea.

[288] "5G Vision," Networks, Samsung, Accessed April 21, 2020, https://www.samsung.com/global/business/networks/insights/5g-vision/.

[289] "Ericsson Fined $1 Billion for Widespread Corruption," News, *Deutsche Welle*, December 7, 2019. https://p.dw.com/p/3UMt3.

[290] Helena Soderpalm and Olof Swahnberg, ""Ericsson Has Dismissed 50 Employees Following U.S. Corruption Probe," Business News, *Reuters*, October 18, 2018, https://www.reuters.com/article/us-ericsson-probe/ericsson-has-dismissed-50-employees-following-u-s-corruption-probe-idUSKCN1MS1R4.

[291] Ray Le Maistre, "Nokia Unearths AlcaLu Compliance Timebomb," Business/Employment, *Light Reading*, March 22, 2019, https://www.lightreading.com/business-employment/nokia-unearths-alcalu-compliance-timebomb/d/d-id/750356.

[292] Morris, Iain. "Nokia's 5G Chip Choice Leaves it Exposed." 5G. *Light Reading*, October 28, 2019. https://www.lightreading.com/5g/nokias-5g-chip-choice-leaves-it-exposed/d/d-id/755184.

merged in 2006, each having their own issues with corruption[293].

Upon merging, Alcatel had over a decade of global corruption practices[294], and Lucent had spent several years bribing PRC officials. Both companies, before and after their merger, had contracts in the PRC. Notably, before and after being acquired by Nokia, Alcatel-Lucent licensed the production of Alcatel and BlackBerry products to PRC based telecommunications company TCL.

In 2018 it became clear that various TCL created apps contained malware. These included pre-loaded apps on a wide variety of TCL products including Alcatel and BlackBerry devices. The malware harvested user data and sent it to the PRC, in addition to other malicious and suspicious behaviors[295].

It is unclear what mitigation steps Nokia has taken regarding Alcatel-Lucent or TCL. However, given the centrality of Alcatel-Lucent's 5G chips to Nokia's network business plan (which has in fact set it back)[296], greater risk assessment seems reasonable. Then there Nokia's two other relationships.

In 2006, Nokia and Siemens began a joint venture to build telecommunications networks and services, which Nokia ultimately bought full control of in 2011[297]. Yet, in 2006 Siemens was also charged with corruption. The Siemens corruption scandal was no small affair. It demonstrated that by the early 1990s a global system of corruption had become the norm within the company and its subsidiaries[298]. Some of this corruption involved the PRC. Worryingly, it would appear that such corrupt practices continued well past 2006, particularly within the PRC,

---

[293] "Lucent Admits to Bribery," News Wire Feed, *Light Reading*, December 21, 2007, https://www.lightreading.com/lucent-admits-to-bribery/d/d-id/650564; "Former Alcatel Exec Sentenced," News Wire Feed, *Light Reading*, September 24, 2008, https://www.lightreading.com/former-alcatel-exec-sentenced/d/d-id/661544.

[294] Naim, Moises. "The Corruption Eruption." *The Brown Journal of World Affairs* 2, no. 2 (Spring/Summer 1995): 245-261. http://bjwa.brown.edu/2-2/the-curruption-eruption/; Richard L. Cassin, "Alcatel-Lucent Settles Bribery Case," *The FCPA Blog*, December 28, 2010, https://fcpablog.com/2010/12/28/alcatel-lucent-settles-bribery-case/.

[295] Catalin Cimpanu, "Malware Found Preinstalled on Some Alcatel Smartphones," *ZDNet*, January 10, 2019, https://www.zdnet.com/article/malware-found-preinstalled-on-some-alcatel-smartphones/; Octavio Mares, "The Most Dangerous & Spying Television Award Goes to TCL," *Information Security Newspaper*, February 4, 2020, https://www.securitynewspaper.com/2020/02/04/the-most-dangerous-spying-television-award-goes-to-tcl/.

[296] Morris, "Nokia's 5G"; Iain Morris, "Nokia Hires 350 R&D Experts to Fix 5G Problems," 5G, *Light Reading*, October 30, 2019, https://www.lightreading.com/5g/nokia-hires-350-randd-experts-to-fix-5g-problems/d/d-id/755257.

[297] Stephen Lawson, "Nokia Closes Acquisition, Renames Nokia Siemens Networks," News—IT Leadership, *ComputerWorld*, August 7, 2013, https://www.computerworld.com/article/2484790/nokia-closes-acquisition--renames-nokia-siemens-networks.html.

[298] Bertrand Venard, "Lessons From the Massive Siemens Corruption Scandal One Decade Later," Economy + Business, *The Conversation*, December 13, 2018, https://theconversation.com/lessons-from-the-massive-siemens-corruption-scandal-one-decade-later-108694.

with reports as recent as 2016[299].

Worth noting here is that Siemens is now working with chip manufacturer Qualcomm to develop 5G networks. In 2016 Qualcomm paid a settlement to avoid charges by the U.S. for corruption in the PRC, including hiring, "relatives of Chinese officials who could influence the selection of its mobile technology products in a competitive market"[300]. In 2018, the EU fined Qualcomm for illegally paying Apple to use their products[301]. Then, in 2019, the US and EU each independently found Qualcomm guilty of violating antitrust laws, leaving experts to doubt punishments will deter Qualcomm from continuing its anticompetitive and corrupt practices[302].

Finally, with regards to Nokia, there is one last event worth mentioning. Apparently a software error resulted in some Nokia phones transmitting data to servers owned by the China Telecommunications Corporation[303]. The phones' hardware and data storage proxies were made by Nokia subsidiary HMD Global Oy, which in turn has its phones manufactured by its partial owner, Foxconn, and contain parts from Qualcomm[304]. HMD and Nokia claim no personal data was shared, but there are reasons to doubt this[305]. Since then, apparently unrelated, Nokia announced its HMD products will store user data in Finland instead of Singapore[306].

In spite of their superior quality of products and security relative to Huawei, both Ericsson's and Nokia's histories should raise alarms. There is almost no knowing if, or more likely how extensively, actors including the PRC, may have compromised their security through any combination of bribes, blackmail, or direct hardware and software manipulation. Their

---

[299] Scilla Alecci, "German Media Reveals How Chinese Bribes for Siemens Products Flowed," Blog, International Consortium of Investigative Journalists, October 1, 2018, https://www.icij.org/blog/2018/10/german-media-reveals-how-chinese-bribes-for-siemens-products-flowed/.

[300] John Ribeiro, "U.S. Slaps Qualcomm With Multi-Million Dollar Fine Over China Corruption Allegations," News—Legal, *PCWorld*, March 2, 2016, https://www.pcworld.com/article/3040157/qualcomm-fined-in-the-us-over-china-corruption-allegations.html.

[301] David Meyer, "Qualcomm Just Got Fined $1.23 Billion for Illegal Payments to Apple," Tech—Antitrust, *Fortune*, January 24, 2018, https://fortune.com/2018/01/24/qualcomm-apple-intel-antitrust-baseband-eu/.

[302] Reed Albergotti, Hamza Shaban, and Taylor Telford, "Qualcomm Violated Antitrust Law, Judge Rules," Technology, *The Washington Post*, May 22, 2019, https://www.washingtonpost.com/technology/2019/05/22/qualcomm-violated-antitrust-law-judge-rules/; Associated Press, "EU Fines Chipmaker Qualcomm for 'Predatory Pricing'," Business News, *U.S. News & World Report*, July 18, 2019, https://www.usnews.com/news/business/articles/2019-07-18/eu-fines-chipmaker-qualcomm-for-predatory-pricing.

[303] Wei Shi, "Nokia-Branded Phones Sent Personal Data from Norway to China," News, *Telecoms.com*, March 22, 2019, https://telecoms.com/496471/nokia-branded-phones-sent-personal-data-from-norway-to-china/.

[304] Ralph Jennings, "Apple Contractor Foxconn Makes Gains With Its Own Brand of Phones in a Tough Market," Asia. *Forbes*, January 31, 2019, https://www.forbes.com/sites/ralphjennings/2019/01/31/apple-contractor-foxconn-makes-gains-with-its-own-brand-of-phones-in-a-tough-market/#1ef048012c48; Shi, "Nokia-Branded"; "Data Collection Technical Details FAQ's," Phones, Nokia, https://www.nokia.com/phones/en_int/data-collection-tech-details.

[305] Shi, "Nokia-Branded".

[306] Wei Shi, "HMD Moves Nokia Phone User Data Storage to Finland," News, *Telecoms.com*, June 19, 2019, https://telecoms.com/498007/hmd-moves-nokia-phone-user-data-storage-to-finland/.

expanding 5G contracts and partnerships in the PRC would seem to increase these risks[307]. The rushed[308], seemingly unexamined, adoption or even nationalization of Nokia and Ericsson[309] seem counterproductive from a security perspective, let alone ideologically or economically[310].

Supply chain risks will always be present and corruption will always be an issue, even with trusted insiders[311]. Indeed, a senior global security and privacy officer for Huawei stated that bribery would be easier and more effective than building or using a backdoor[312]. Though bribery and blackmail are not the most effective tools for controlling an insider in the long run[313], compromising cybersecurity only requires a momentary lapse. Neither of these issues appears to receive appropriate attention, particularly when they involve actors presumed friendly or competent.

However, two other related but more pervasive factors seem to receive less attention when it comes to 5G and network security. The first is that it may already be close to impossible to have secure 5G networks, regardless of the provider. The second is the so-called social layer. An internationalised HCSEC, and particularly creating ICSEC could create and coordinate stronger, more proactive, approaches to such risks.

Governments, Corporations, and Rights

Cryptographer and Harvard Kennedy School fellow, Dr. Schneier, acknowledges the risks and threats Huawei and the PRC pose, but argues that keeping them, "out of Western

---

[307] Bevin Fletcher, "Ericsson, Nokia ink 5G Deals with Chinese Operators – Report," 5G, *Fierce Wireless*, November 8, 2019, https://www.fiercewireless.com/5g/ericsson-nokia-ink-5g-deals-chinese-operators-report.

[308] Nick Statt, "US Pushing Tech and Telecom Industries to Build 5G Alternative to Huawei," Policy, *The Verge*, February 5, 2020, https://www.theverge.com/2020/2/5/21124888/us-5g-huawei-white-house-trump-china-alternative-telecom-standard.

[309] William Barr, "Attorney General William Barr's Keynote Address: China Initiative Conference," Transcript, CSIS, February 6, 2020, https://www.csis.org/analysis/attorney-general-william-barrs-keynote-address-china-initiative-conference.

[310] Josh Horwitz, "The Trump Team's Idea to Counter China with Nationalized 5G is Just What China Would do," *Quartz*, January 29, 2018, https://qz.com/1191154/the-trump-teams-idea-to-counter-china-with-nationalized-5g-is-just-what-china-would-do/; Eric Boehm, "Corporate Socialism? Bill Barr's Suggestion that the U.S. Should Buy Nokia or Ericsson to Counter China is a Terrible Idea," Internet, *Reason*, February 12, 2020, https://reason.com/2020/02/12/corporate-socialism-bill-barr-suggests-the-u-s-should-counter-china-by-buying-nokia-or-ericsson/.

[311] Mike Giglio, "China's Spies Are on the Offensive," Politics, *The Atlantic*, August 26, 2019, https://www.theatlantic.com/politics/archive/2019/08/inside-us-china-espionage-war/595747/.

[312] Eileen Yu, "Huawei: Easier to Bribe Telco Staff than to Build Backdoors," Blog—By the Way, *ZDNet*, October 23, 2019, https://www.zdnet.com/article/huawei-easier-to-bribe-telco-staff-then-build-backdoors/.

[313] Randy Burkett, "An Alternative Framework for Agent Recruitment: From MICE to RASCALS," *Studies in Intelligence* 57, no. 1 (Extracts, March 2013): 7-17, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-57-no.-1-a/vol.-57-no.-1-a-pdfs/Burkett-MICE%20to%20RASCALS.pdf.

infrastructure isn't enough to secure 5G"[314]. This is because the, "insecurities are a result of market forces that prioritize costs over security and of governments, including the United States, that want to preserve the option of surveillance in 5G networks"[315]. Backdoors for governments, like the UK, US, and others have called for or even considered mandating[316], make cyberspace and 5G far less secure[317] (see also). This is not to mention the human rights issues[318] and threats of "authoritarian backsliding"[319] such choices pose, or how they look in the context of arguments against Huawei and the PRC[320].

Further, Dr. Schneier argues, in spite of 5G's security improvements over 4G, there are three key problems. First, because of how its hardware and software are designed and interact, its complexity makes its security standards even harder to implement. Second, extensive and unavoidable backwards compatibility with 4G and other networks will cause, "5G networks to inherit many existing problems"[321], which will take more than a decade to overcome[322]. Third, 5G standards committees made many security features optional, and companies prioritized, "development, performance, cost, and time to market ... over security, which was treated as an afterthought"[323].

Governments have long had the ability to penetrate networks, "without having any control over the hardware, the software, or the companies that produce the devices", and,

---

[314] Bruce Schneier, "China isn't the Only Problem With 5G," Argument, *Foreign Policy*, January 10, 2020, https://foreignpolicy.com/2020/01/10/5g-china-backdoor-security-problems-united-states-surveillance/.
[315] Ibid.
[316] Jacob Kastrenakes, "US, UK, and Other Governments Asks Companies to Build Backdoors into Encrypted Devices," Cybersecurity, *The Verge*, September 3, 2018, https://www.theverge.com/2018/9/3/17815196/five-eyes-encryption-backdoors-us-uk-australia-nz-canada.
[317] Harold Ableson, Ross Anderson, Steven M. Bellovin, Joshn Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael A. Specter, and Daniel J. Weitzner, "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications," *Journal of Cybersecurity* 1, no. 1 (September 2015): 69- 79. https://doi.org/10.1093/cybsec/tyv009; Riana Pfefferkorn, "Security Risks of Government Hacking," The Center for Internet and Society, Stanford Law School, September 2018, https://cyberlaw.stanford.edu/files/publication/files/2018.09.04_Security_Risks_of_Government_Hacking_Whitepaper.pdf; Schneier, "China Problem".
[318] Ryan Goodman, "International Proscriptions on Mass Surveillance (or What's Missing in the Greenwald vs. Wittes Debate," *Just Security*, March 24, 2014, https://www.justsecurity.org/8448/international-proscriptions-mass-surveillance-or-whats-missing-greenwald-vs-wittes-debate/.
[319] Jessica Chen Weiss, "Understanding and Rolling Back Digital Authoritarianism," Commentary, *War on the Rocks*, February 17, 2020, https://warontherocks.com/2020/02/understanding-and-rolling-back-digital-authoritarianism/.
[320] Jennifer Stisa Garnick, "Huawei Hacking is a Security Scandal," *Just Security*, March 24, 2014, https://www.justsecurity.org/8488/huawei-hacking-security-scandal/.
[321] Schneier, "China Problem".
[322] Lily Hay Newman, "5G is More Secure than 4G and 3G—Except When it's Not," Security, *WIRED*, December 15, 2019, https://www.wired.com/story/5g-more-secure-4g-except-when-not/.
[323] Schneier, "China Problem".

"nothing in 5G prevents these activities from continuing, even increasing, in the future"[324]. Outside of the limited benefits of adding secure layers to existing and upcoming networks, Dr. Schneier states, there is little that can be done. As mentioned before, open networks may be one of few such solutions[325].

Yet, these added layers of security are only as good as their design, which have their own issues in need of standards and regulation[326], many of which revolve around existing governmental and corporate standards, processes of regulation, and incentives[327]. Even open network advocate Dr. Wheeler recognizes that keeping Huawei hardware out will not secure 5G, and narrowly focusing on it distracts from real problems and solutions[328]. Further, as is all too often the case, design is only effective when it appropriately accounts for the human factor.

The Social Layer

Human based intelligence remains a vital component of (counter-)espionage, and is only enhanced by technological capabilities[329]. The human factor, in the form of the so-called "social layer" of cyberspace[330], is the one layer of cybersecurity that remains neglected by virtually everyone, even though it is arguably the most vulnerable[331]. The social layer may particularly be an issue when it comes to supply chains, corruption, or the many ways to get past the other two, more widely focused and relied upon, layers of cybersecurity, the "physical layer" and the "logical layer"[332].

The social layer concerns the real world and digital information associated with individuals and organizations (whether personal, academic, commercial, or governmental). It is

---

[324] Ibid.
[325] Wheeler, "'Secret Sauce'".
[326] David Simpson, "FCC White Paper: Cybersecurity Risk Reduction," Report, Public Safety & Homeland Security Bureau—Federal Communications Commission, January 18, 2017, https://www.fcc.gov/document/fcc-white-paper-cybersecurity-risk-reduction; Vinod K. Aggarwal and Andrew W. Reddie, "Comparative Industrial Policy and Cybersecurity: A Framework for Analysis," *Journal of Cyber Policy* 3, no. 3 (2018): 291-305, https://doi.org/10.1080/23738871.2018.1553989; Paul Maxwell and Robert Barnsby, "Insecure at any Bit Rate: Why Ralph Nader is the True OG of the Software Design Industry," *Journal of Cyber Security* 4, no. 3 (2019): 346-361, https://doi.org/10.1080/23738871.2019.1671471; Dunn-Cavelty and Wenger, "Cyber Security Politics".
[327] "Special Issue", *Journal of Cyber* Policy; Wheeler and Simpson, "5G Requires".
[328] Tom Wheeler and Robert D. Williams, "Keeping Huawei Hardware Out of the U.S. Is Not Enough to Secure 5G," Huawei, *Lawfare*, February 20, 2019, https://www.lawfareblog.com/keeping-huawei-hardware-out-us-not-enough-secure-5g; Wheeler and Simpson, "5G Requires".
[329] David V. Gioe, "'The More Things Change': HUMINT in the Cyber Age," In *The Palgrave Handbook of Security, Risk and Intelligence*, edited by Robert Dover, Huw Dylan, and Michael Goodman, 213-227, London: Palgrave Macmillan, 2017.
[330] "The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028," TRADOC Pamphlet 525-7-8, Department of the Army, February 22, 2010, p. 8-9, https://fas.org/irp/doddir/army/pam525-7-8.pdf.
[331] David V. Gioe, Michael S. Goodman, and Alicia Wanless, "Rebalancing Cybersecurity Imperatives: Patching the Social Layer," *Journal of Cyber Policy* 4, no. 1 (2019): 117-137, https://doi.org/10.1080/23738871.2019.1604780.
[332] "US Army's Cyberspace", Department of Army, p. 8-9.

broken into the subcategories of "persona" and "cyber persona"[333]. A persona is the individual with authorized access on a network. A cyber persona, "includes a person's identification or persona on the network (e-mail address, computer IP address, cell phone number, and others)"[334]. Further, "an individual can have multiple cyber personas (for example, different e-mail accounts on different computers) and a single cyber persona can have multiple users (for example, multiple users accessing a single eBay® account)"[335].

In an era of easy information sharing and gathering, it has become quite easy to harvest and leverage a wide variety of data from the social layer. The social layer can be used to compromise the more focused on and secure physical and logical layers, or manipulate targeted individuals and groups, by manipulating or hijacking (cyber) personas. This can be done via broad or targeted propaganda and phishing campaigns.

The social layer is in many ways more difficult to address due to the numerous, more difficult to control, very human variables at play. However, neglecting the social layer is not an option and it should be a key component of any holistic cybersecurity initiative. Indeed, "human minds are effectively critical infrastructure", and, "how deeply vulnerable the social or cognitive layer is in cybersecurity", needs far more attention[336].

POSSIBLY EXPAND FROM GIOE AND NEXT GOV ARTICLE ABOUT TRANSPARENCY + NEED FOR DATA

[333] Ibid.
[334] Ibid.
[335] Ibid.
[336] Gioe et al., "Rebalancing," p. 122.

Innovative Solutions

In addition to open network design[337], there are a variety of innovative cybersecurity solutions that exist or are being developed. Highlighted here are seven approaches that would benefit from greater awareness among policy makers, organizational leaders, technicians, and academics alike. These proactive, thematically related, methods of enhancing (cyber) security can and should be applied to all layers of cybersecurity and aforementioned risks. They also can and should be a part of cyber security politics more broadly.

The first is "zero trust" design[338], "outcome-based" cybersecurity plans[339], red cells[340] (aka red teams[341]), complexity/systems based approaches like anticipatory intelligence[342], increasing the diversity of cyber security policy professionals, and action research[343]. Further developing, integrating, and applying these methods to cybersecurity and security risks more broadly is greatly needed. Again, the UK and a possible ICSEC could help take this on.

A concrete example drives home the importance of the innovative solutions we examine. In 2017, Wikileaks acquired and published 180 GB of US intelligence agencies' classified hacking tools and documents, known as the Vault 7 leaks[344]. The Vault 7 leaks appear to stem from then CIA systems administrator Joshua Schulte. In his criminal trial, it was revealed that, "the virtual machine that held all of the tools apparently used '123ABCdef' as its password"[345]. To make matters worse, "from shared admin passwords to no limitations on removable storage, the agency broke or snubbed virtually every rule in the book"[346]. Such problems appear to be widespread in US intelligence, and three years later, it would appear that little has changed[347].

---

[337] Wheeler, "'Secret Sauce'".
[338] Medin et al., "5G Ecosystem"; Stuart H., "Zero Trust Architecture Design Principles: Alpha Release for the ZTA Principles on GitHub," Blog Post, NCSC, November 20, 2019, https://www.ncsc.gov.uk/blog-post/zero-trust-architecture-design-principles.
[339] John Cosby, "The Most Resilient Organizations Follow Outcome Based Cybersecurity," Opinion, *Fifth Domain*, March 30, 2020, https://www.fifthdomain.com/opinion/2020/03/31/the-most-resilient-organizations-follow-outcome-based-cybersecurity/.
[340] Eric C. Anderson, "Global Agenda 2012 - Red Cell," Global Agenda 2012 Speaker Series—Spies, Lies, & Sneaky Guys: Espionage & Intelligence in the Digital Age, University of Delaware, September 11, 2012, Video, 1h:22m:36s, https://www.youtube.com/watch?v=BAzBtVcNldY&t=1s.
[341] Micah Zenko, *Red Team: How to Succeed by Thinking Like the Enemy*, New York: Basic Books, 2015.
[342] Josh Kerbel, "Coming to Terms With Anticipatory Intelligence," Commentary, *War on the Rocks*, August 13, 2019, https://warontherocks.com/2019/08/coming-to-terms-with-anticipatory-intelligence/.
[343] David Coghlan and Mary Brydon-Miller, (Editors), *The SAGE Encyclopedia of Action Research*, *Vol I & II*, London: SAGE Publications, Ltd., 2014.
[344] Shaun Nichols, "If You're Despairing at Staff Sharing Admin Passwords, Look on the Bright Side. That's CIA-Grad Security," Security, *The Register*, June 16, 2020, https://www.theregister.com/2020/06/16/cia_report_vault_7_leak/.
[345] Ibid.
[346] Ibid.
[347] Ibid.

Zero Trust

The DIB's 2019 report[348] references, and an article on the UK's NCSC website[349] outlines the design principles of, "zero trust" networks. Notably, zero trust was not mentioned in the US Cyber Solarium Report[350]. It is a relatively new and evolving approach to network design that is key in addressing almost all of the risks discussed thus far. A zero trust approach removes inherent trust from the network.

This means that access to a network and its components are highly restricted and compartmentalized, based on a set of design principles and a well planned and executed security policy. Often, if a breach does occur, the intruder can, "move laterally because everything on the network is trusted", but, "in a zero trust architecture, the network is treated as hostile"[351]. Removing, "trust from the network", requires that, "you gain confidence in the authentication, verification and authorization of users and services"[352]. To do this, trust must be built, "into the user's identity (user authentication), their devices (device verification), and the services they access (service authorisation)"[353].

The efficacy of this model requires that, "each connection to a service should be authenticated and the device and connection authorised against a policy, regardless of where the connection request comes from"[354]. In turn, "to enable authorisation decisions, access policies need to be defined, based on who can access which service or data, under which circumstances"[355]. Specifically, "how much confidence you need to trust a connection depends on the value of data being accessed or impact of action being performed"[356].

Similarly, "devices should be inventoried and device verification should be based on defined policies (such as encryption, patch levels, etc)"[357]. This is but a brief outline of zero trust entails. The NCSC source significantly elaborates on the necessity and execution of zero trust, and the DIB report emphasizes the need for, "quantum-resistant key exchange mechanisms"[358], due to the PRC's quantum computer investments. One would hope that collaboration across the proverbial pond is underway.

---

[348] Medin et al, "5G Ecosystem," p. 29.
[349] Stuart H., "Zero Trust".
[350] U.S. Cyber Space Solarium Commission, "Report".
[351] Ibid.
[352] Ibid.
[353] Ibid.
[354] Ibid.
[355] Ibid.
[356] Ibid.
[357] Ibid.
[358] Medin et al., "5G Ecosystem," p. 29.

Outcome-Based Security

Outcome-based cybersecurity is, "more holistic"[359], and proactive philosophy, which builds on the existing approaches to cybersecurity. It requires, "continuously evaluating an organizations' status and the risk environment"[360]. It does so by measuring, "the value and validity of an organization's cyber defenses and enterprise based on active analysis against the organization's total risk profile"[361].

As each organization's status and environment differs, it is the responsibility of each organization to understand, plan for, and reassess their needs constantly. This all is to be done on top of the more basic cybersecurity requirements. Both the more basic and out-come based methods of cybersecurity are included in the DOD's March 18, 2020 release of their Cybersecurity Maturity Model Certification as requirements for those who wish to do business with the DOD[362].

There is a caveat however. While outcome-based security and existing standards are strong approaches, according to former US Undersecretary of Defense Frank Kendall, the certification system in which they are framed is self-defeating on a variety of levels, adding layers of complication to, rather than addressing, core cyber security supply chain issues. In sum, he argues quite effectively that the certification system disincentives integrity, efficiency, and thus efficacy[363]. Policy makers looking for more a model for implementing outcome-based security are advised to take the flaws of the certification system into account.

Red Cells/Teams

Key to any security approach, and explicitly a key part of outcome-based cybersecurity, is the use of red cells[364], perhaps more commonly called red teams[365]. These terms refer to utilizing trusted experts to think and act like potential threats so as to identify and address weaknesses. This method is already employed in various capacities in the UK and US.

However, even more important than their use is actually following through with the recommendations of such teams and the findings of other groups focused on enhancing security,

---

[359] Cosby, "Most Resilient".
[360] Ibid.
[361] Ibid.
[362] "CMMC Model," Cybersecurity Maturity Model Certification, Office of the Undersecretary of Defense for Acquisition & Sustainment, Accessed March 30, 2020, https://www.acq.osd.mil/cmmc/draft.html; Cosby, "Most Resilient".
[363] Frank Kendall, "Cybersecurity Maturity Model Certification: An Idea Whose Time Has Not Come and Never May," Business, *Forbes*, April 29, 2020, https://www.forbes.com/sites/frankkendall/2020/04/29/cyber-security-maturity-model-certificationan-idea-whose-time-has-not-come-and-never-may/#35ea66773bf2.
[364] Anderson, "Red Cells".
[365] Zenko, *Red Team*.

something which both the UK[366] and US[367] have had troubling track records with. This is all the more vital when not utilizing a full ban, as is the case with the UK. Ideally any organization charged with enhancing security for 5G or cyberspace more generally takes full advantage of this method.

Anticipatory Intelligence

Finally, utilizing complexity and systems paradigms like anticipatory intelligence, as outlined in the 2019 US National Intelligence Strategy[368], and applying it to cybersecurity is crucial. Anticipatory intelligence seeks to, "imagine or envision possibilities before they emerge"[369]. National Intelligence University faculty member Dr. Kerbel gives a much needed clarification of the term. He defines it as, "the intelligence process or practice whereby potentially emergent developments stemming from the increasingly complex security environment are foreseen via the cultivation of holistic perspectives"[370].

The Cold War was the formative experience for current security and intelligence paradigms. The bi-polar nature of the Cold War allowed actors to ignore the complex nature of reality and the international environment, and focus on relatively stable, or at least apparent, threats. However, "the spiking global complexity (interconnectivity and interdependence, both virtual and physical) that characterizes the post–Cold War security environment, with its proclivity to generate emergent (nonadditive or nonlinear) phenomena, is essentially new"[371].

In the context of cybersecurity, and security challenges more broadly, this means that systems and complexity sciences must be fully employed. As the senior research director and lead writer for the US Cyberspace Solarium Commission, Dr. Jensen stated after the commission's report was released that it is not enough to simply research risks and failures in complex systems as they apply to cyberspace. There needs to be a focus on compounding

---

[366] Lewis, "United Kingdom".

[367] Mark Pomerleau, "The Pentagon is Handling Cyber Vulnerabilities Inconsistently," DoD, *Fifth Domain*, March 17, 2020, https://www.fifthdomain.com/dod/2020/03/17/the-pentagon-is-handling-cyber-vulnerabilities-inconsistently/; Mariam Baksh, "Stop Hiding Vulnerabilities Found by Red Teams, Joint Staff to Tell Military," Tech, *Defense One*, March 18, 2020, https://www.defenseone.com/threats/2020/03/stop-hiding-vulnerabilities-found-red-teams-joint-staff-tells-military/163868/?oref=d1-related-article; Mariam Baksh, "Pentagon Isn't Following the Cyber Steps it Asks from Suppliers, GAO Says," Tech, *Defense One*, April 15, 2020, https://www.defenseone.com/technology/2020/04/pentagon-lacks-cyber-hygiene-it-will-demand-suppliers-gao-says/164638/?oref=d-nextpost.

[368] "National Intelligence Strategy of the United States of America 2019." Office of the Director of National Intelligence. 2019, p. 7, 9, 32. https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf?utm_source=Press%20Release&utm_medium=Email&utm_campaign=NIS_2019.

[369] Kerbel, "Anticipatory Intelligence".

[370] Ibid.

[371] Ibid.

systemic risks[372]. As Dr. Wheeler and co-author Retired Rear Admiral Simpson state, within 5G this means understanding how the weakest cyber security links in public-private ecosystem put the rest at risk[373].

More importantly, for Dr. Jensen, this means examining how human security challenges like pandemics, economics, political instability, climate change, migration, cyberspace, and more all interact to impact each other or create new phenomenon[374]. He notes that while it touches on the need for examining complex systems, the report is missing critical recommendations. Specifically, the world needs, "new research initiatives that evaluate systemic risk", including something like, "a Bureau of Cyber Statistics"[375]. He mentions the Center for Systemic Peace's[376] Political Instability Task Force as a model[377] for such efforts.

In sum, greater adaptation of transdisciplinary work with systems and complexity paradigms would be invaluable for out-come based cybersecurity, red teams, and anticipatory intelligence, and by extension peace and prosperity. Taken as a whole, there is ample opportunity for the UK, perhaps via HCSEC/ICSEC, to lead its strategic partners and the world in the 5G and cybersecurity realms. Between its proactive approach to cybersecurity thus far, its potential to integrate and coordinate emerging cybersecurity efforts, and its international standing, it seems well suited for taking on the complexities of the 21st century.

Complex Systems Paradigms

As is the case with most academic terms and topics, the definitions of and relationships between complexity and systems science can vary significantly depending on the discipline, field, or author describing them. Some suggest complexity encompasses and transcends systems, some visa-versa, and some believe they are on a more equal footing. Some even just refer to complex systems science. None of these perspectives is right or wrong.

Rather, the varieties of parameters and their implications are arguably a strength, contributing to tailored means and ends as well as the broader discourse and praxis. For those less familiar with complexity and systems sciences, or their (often blurred) distinctions and uses, this appendix reviews some complex systems resources. We begin with general resources, then

---

[372] Benjamin Jensen, "When Systems Fail: What Pandemics and Cyberspace Tell Us About the Future of National Security, Commentary, *War on the* Rocks, April 9, 2020, https://warontherocks.com/2020/04/when-systems-fail-what-pandemics-and-cyberspace-tell-us-about-the-future-of-national-security/.

[373] Wheeler and Simpson, "5G Requires".

[374] Jensen, "When Systems".

[375] Ibid.

[376] "INSCR Data Page," Center for Systemic Peace, Accessed April 9, 2020, http://www.systemicpeace.org/inscrdata.html.

[377] Jack A. Goldstone, Robert H. Bates, David L. Epstein, Ted Robert Gurr, Michael B. Lustik, Monty G. Marshall, Jay Ulfelder, and Mark Woodward, "A Global Model for Forecasting Political Instability," *American Journal of Political Science* 54, no. 1 (2010): 190-208, www.jstor.org/stable/20647979.

move to the intersections of complex systems literature with international relations and security, the PRC, and cyber security. We finish with a nod to the merits of action research.

General Resources

Castellini has created an interactive map of complexity (and systems) sciences over time[378]. This allows for a very accessible meta-perspective, and has a guide at the bottom to help with its interpretation and use. Whereas Castellini uses complexity as an umbrella term, Hieronymi's article makes a similar attempt at visualizing the varying complex systems paradigms while using systems as an umbrella and co-equal term, detailing some debates[379].

The Santa Fe Institute's Complexity Explorer website is regularly updated, offering a wide variety of resources including courses, academic texts, a virtual laboratory, a glossary, organizations focusing on complexity and systems sciences, and much more. The foot note at the end of this sentence leads to their free introduction to complexity course and can be used to navigate elsewhere[380]. Similarly, the website Complexity Explained, offers an excellent variety of educational tools and references[381]. The site and its free twenty page booklet[382] are the result of a worldwide collaboration and survey of complex systems science experts, practitioners, and students.

International Relations and Security

At the intersection of complex systems, international relations, and security, in theory and practice, several resources are worth noting. Janzwood and Piereder curate the works in Oxford Bibliographies' International Relations sub-section, "Complex Systems Approaches to Global Politics"[383]. Lewis, Mackin, and Darken's framework stands out for its analysis of critical infrastructure, and related risk prevention and response measures, as a complex emergent

---

[378] Brian Castellani, "Map of the Complexity Sciences," Art & Science Factory, 2018, https://www.art-sciencefactory.com/complexity-map_feb09.html.

[379] Andreas Hieronymi, "Understanding Systems Science: A Visual and Integrative Approach," *Systems Research and Behavioral Science* 30, no. 5 (2013): 580-595, https://doi.org/10.1002/sres.2215.

[380] Melanie Mitchell and Santiago Guisasola. "Introduction to Complexity," Courses, Complexity Explorer, Santa Fe Institute, Accessed February 23, 2020, https://www.complexityexplorer.org/courses/104-introduction-to-complexity.

[381] Manlio De Dominico and Hiroki Sayama, (Coordinators), Complexity Explained, Accessed, May 1, 2020, https://complexityexplained.github.io/.

[382] Manlio De Domenico, Dirk Brockmann, Chico Camargo, Carlos Gershenson, Daniel Goldsmith, Sabine Jeschonnek, Lorren Kay, Stefano Nichele, Jose R. Nicolas, Thomas Schmickl, Massimo Stella, Josh Brandoff, Angel Jose Martinez Salinas, and Hiroki Sayama. *Complexity Explained.* Creative Commons, 2019. DOI 10.17605/OSF.IO/TQGNW.

[383] Scott Janzwood and Jinelle Piereder, "Complex Systems Approaches to Global Politics," International Relations. Oxford Bibliographies, Oxford University Press, February 26, 2020, Accessed April 28, 2020, https://www.oxfordbibliographies.com/view/document/obo-9780199743292/obo-9780199743292-0278.xml?q=cyber#firstMatch.

system[384]. The result is a more nuanced, holistic, and coherent approach to anticipating, preparing for, and responding to incidents. Choucri and Clark's book appears to the only work integrating complex systems, international relations theory, and cyberspace[385].

There are also several additional free publications we are aware of at the intersection of complexity, security, and international relations. Affiliated with the DoD, Alberts and Czerwinski's 1997 book appears to be the earliest compilation of professional and scholar perspectives on the intersection of these topics[386]. Also affiliated with the DoD is Moffatt's more technical and militarily focused[387]. In the context of peace and conflict studies, Hendrick's 2009 working paper[388] and Leoroux-Martin and O'connor's 2017 report[389] offer interdisciplinary overviews of complex systems' meanings and applications.

The PRC

Concerning the PRC and complexity, there are two notable works. Dr. Kerbel's 2004 article is useful, for its descriptions of the US-PRC cognitive biases' based on the human and Cold War desire for simplicity, and how complexity science can help improve analysis and action in this realm[390]. Garlick's analysis of the PRC's rise through the international relations theories of complexity, neorealism, offensive realism, and constructivism compliments Kerbel's work nicely[391].

Cyber Security

In our literature review, there were several notable works concerned with complex systems and cyber security. The earliest publication we identified is Armstrong, Mayo, and Siebenlist's 2009 report on "Complexity Science Challenges in Cybersecurity" for the US

---

[384] Ted G. Lewis, Thomas J. Mackin, and Rudy Darken. "Critical Infrastructure as Complex Emergent Systems." *International Journal of Cyber Warfare and Terrorism* 1, no. 1 (2011): 1-12. DOI: 10.4018/ijcwt.2011010101.

[385] Nazli Choucri and David D. Clark, *International Relations in the Cyber Age: The Co-Evolution Dilemma*, Cambridge, MA, US: MIT Press, 2019.

[386] David S. Alberts and Thomas J. Czerwinski, *Complexity, Global Politics, and National Security*, Washington D.C.: National Defense University Press, 1997, http://www.dodccrp.org/files/Alberts_Complexity_Global.pdf.

[387] James Moffat, *Complexity Theory and Network Centric Warfare*, Information Age Transformation Series, Washington, D.C.: CCRP Publication Series, 2003, http://www.dodccrp.org/files/Moffat_Complexity.pdf.

[388] Diana Hendrick, "Complexity Theory and Conflict Transformation: An Exploration of Potential and Implications," Working Paper 17, Centre for Conflict Resolution—Department of Peace Studies, University of Bradford, June 2009, https://www.beyondintractability.org/bi_affiliated_projects/dsap/publications/complexity-theory-transformation-hendrick.pdf.

[389] Philippe Leroux-Martin and Vivienne O'Connor, "Systems Thinking for Peacebuilding and Rule of Law: Supporting Complex Reforms in Conflict-Affected Environments," Report, Peaceworks, United States Institute of Peace, October 23, 2017, https://www.usip.org/publications/2017/10/systems-thinking-peacebuilding-and-rule-law.

[390] Kerbel, "Thinking Straight".

[391] Jeremy Garlick, "Not So Simple: Complexity Theory and the Rise of China," *China Report* 52, no. 4 (2016): 284-305, https://doi.org/10.1177/0009445516661884.

government[392]. It points to the necessity of applying complexity science to cyber security, particularly to critical cyber infrastructure, indicating that at the time it was a relatively new and unapplied approach to cyber security. In this context they state that complexity science is crucial for the improvement of reactive and proactive forms of mitigation, and explore research directions.

Dr. Tisdale's 2015 cyber security management framework[393], and later study of it[394], are also worthy of consideration. The framework is notable for its integration and application of knowledge management, complexity, systems, and business intelligence to the cyber security needs of organizations. As such the framework seems tailor made for outcome-based security and anticipatory intelligence.

Brantly's 2019 article concerning cyber policy and complexity theory appears to be rather unique[395]. It argues the laws and policies for cyberspace are detrimentally simplistic, using two cryptography case examples are used to demonstrate this. These cases are also used to argue that developing effective cyber policy requires a wider embrace complexity theory.

Diversity

The 5G debate, and cyber security discourses more broadly, have emphasized multi-stakeholderism while also, literally, suffering from a lack of diversity. Dr. Dunn-Cavelty and Dr. Wegner's formulation and analysis of cyber security politics describes the necessity of professional diversity and coordination among actors and stakeholders in the technological, political, and scientific spheres composing it[396]. To some extent they address organizational and national cultures, but they do not discuss diversity in other terms. S

For cyber security to be effective, and by extension for the economic and security interests of companies, nations, and 5G to be optimised, diversity must be fostered at all scales within and by the spheres of cyber security politics. The pursuit of diversity must be subject to continuous critique and improvement[397]. In research and in practice within private and public entities, attention must be paid to gender, race, culture, nationality, sexuality, socio-economic

[392] Robert C. Armstrong, Jackson R. Mayo, and Frank Siebenlist, "Complexity Science Challenges in Cybersecurity," Sandia Report—SAND2009-2007, Sandia National Laboratories, March 2009, https://wiki.cac.washington.edu/download/attachments/7478403/Complexity+Science+Challenges+in+Cybersecurity.pdf.
[393] Susan M. Tisdale, "Cybersecurity: Challenges From a Systems, Complexity, Knowledge Management and Business Intelligence Perspective," *Issues ion Information Systems* 16, no. 3 (2015): 191-198, https://iacis.org/iis/2015/3_iis_2015_191-198.pdf.
[394] Susan M. Tisdale, "Architecting a Cybersecurity Management Framework," *Issues in Information Systems* 17, no. 4 (2016): 227-236, https://iacis.org/iis/2016/4_iis_2016_227-236.pdf.
[395] Aaron F. Brantly, "Conceptualizing Cyber Policy Through Complexity Theory," *Journal of Cyber Policy* 4, no. 2 (2019): 275-289, https://doi.org/10.1080/23738871.2019.1583763.
[396] Dunn-Cavelty and Wenger, "Cyber Security Politics".
[397] Dunn-Cavelty and Wenger, "Cyber Security Politics".

class, education, profession, age, disability, and other variables. For the purposes of this section, diversity can be thought of as:

- Factors that compose or are attributable to individuals.
- Individuals that compose private and public entities.
- The types and natures private and public entities which are more classically deemed stakeholders.

Understanding and representing the perspectives, wants, and needs of diverse communities has a tremendous impact on the scope and efficacy of education, research, development, operations, security, and consumer experience. Without taking diversity into account, threats to cyber security are enhanced and mitigation approaches are severely undermined. Examining the impacts made both by women and AI on cyber security and security issues more broadly, drives this home.

Diversity impacts the quality of research and practice in all three spheres of cyber security politics. This has implications for perceptions and behaviors of all actors involved with cyber security politics, whether human or not. In particular, the increasing reliance on AI to shape and manage security, cyber security, and related policies is concerning, given the biases AI absorbs from humans and those which humans in turn absorb from it.

Data quality, as a function of designer and data biases, impacting reliability, accuracy, ethics, and thus validity of design and functionality of threat prediction detection analysis and mitigation whether concerned with individuals or organizations, not to mention general ethics…

Both individual and aggregate scales of diversity are important. However, as the history of multi-stakeholderism has shown, it can be quite difficult to achieve it may be more easily and quickly beneficial to focus on diversifying the individuals, particularly cyber security experts, within organizations and interest groups, as opposed to the necessary but more difficult coordination of collective entities[398].

Yet, in documents like the US Cyber Solarium Report, multi-stakeholder seems to refer exclusively to private and public organizations, within and between nations[399].

Individual stats for women & other sources (Microsoft etc).

Women offer significant benefits to the cyber security profession, but are not just under-represented, their presence and participation are impeded by layers of bias. Dr. Kshetri is a professor of management who studies, “online crime and security issues facing consumers,

[398] Jeanette Hofmann, “Multi-Stakeholderism in Internet Governance: Putting a Fiction into Practice,” *Journal of Cyber Policy* 1, no. 1 (2016): 29-49, https://doi.org/10.1080/23738871.2016.1158303.

[399] U.S. Cyber Space Solarium Commission, “Report”.

organizations and nations". Dr. Kshetri has, "found that internet security requires strategies beyond technical solutions".

In this context, "women's representation is important because women tend to offer viewpoints and perspectives that are different from men's, and these underrepresented perspectives are critical in addressing cyber risks". Females in cyber security leadership roles, "tend to prioritize important areas that males often overlook". This is partially attributable to their education backgrounds; "forty-four percent of women in information security fields have degrees in business and social sciences, compared to 30 percent of men".

This has implications for the security, operations, and bottom lines of businesses. Women in cyber security, "put a higher priority on internal training and education in security and risk management". They, "are also stronger advocates for online training, which is a flexible, low-cost way of increasing employees' awareness of security issues".

Perhaps more importantly, women cyber security professionals have desirable tendencies in, "selecting partner organizations to develop secure software". Specifically, "women tend to pay more attention to partner organizations' qualifications and personnel, and they assess partners' ability [sic] to meet contractual obligations". Women, "also prefer partners that are willing to perform independent security tests".

In spite of the benefits of having women in cyber security, they remain under represented and face numerous barriers, some of which are easier to remedy quickly than others. In 2013, women composed 11 percent of the global cyber security workforce, with this number rising to 20 percent by 2019. In 2017, it was found that globally women make up only 1 percent of senior management and executive cyber security positions, with women of color facing more significant barriers.

Fortune 500 companies only fare a little better. In 2017, only 13 percent of global chief information officers were women. In 2019 about, "20 percent of Fortune 500 global chief information officers (CIOs)", were women.

In these contexts, the UK has faced some challenges, but also shows promise. Studies between 2004 and 2017 seem to have consistently found that women made up only about 8 percent of the UK's cyber security workforce. More recent efforts by the UK seemed to have paid off, with 18 percent of its cyber security industry being female.

Other countries and regions also lend contrast. In 2017, the US, only 14 percent of those in cyber security were women, compared to 48 percent of the US work force being women. Representation is worse outside of the US. In 2018, females, "accounted for 10 percent of the cybersecurity workforce in the Asia-Pacific region, 9 percent in Africa, 8 percent in Latin America, 7 percent in Europe, and five percent in the Middle East".

Clearly the UK has made meaningful efforts to increase the number of women in cyber security, but more must be done.

The US Cyber Solarium Report highlights the need for collaborations among multiple stakeholders in the public and private realms, domestically and internationally. This is a step in the right direction, but there are a few things worth noting, particularly as the report is merely a set of recommendations. First, it is laudable that the report includes individual diversity as a part of its key recommendation to, "better recruit, develop, and retain cyber talent…for cyber work in the federal government"[400].

It specifically mentions the need for, "identifying opportunities and hiring pathways for members of underrepresented communities including the neurodiverse, women, and people of color"[401]. It also notes that, "today's cybersecurity skills and experiences can be gained with unusual ease outside standard channels of education and training", and, "that the government must more effectively take advantage of those unconventional pathways"[402]. However, though not insignificant, the above quotes are essentially the only references to individual diversity.

Further, the report phrases diversity as merely an effort to increase and retain the workforce numbers. It does not mention diversity as something which has its own unique merits and impacts on the quality of cyber security. Additionally, the call for diversity among individuals is discussed relative to the federal employment pool and not public or international partners (though its call for increased k-career education opportunities for all US citizens may help domestically in the long run).

Most importantly, the current US policies undermine such national, organizational, and individual objectives, and the UK should take note. At the national and organizational levels, the US's zero-sum approach is undermining its cyber, 5G, and great power strategies, driving allies and potential partners away. At the individual level, at least culturally and academically, it is depriving itself of much needed human capital, and ignoring or undermining localized audiences and interests abroad. Countering the authoritarian model the PRC seeks to export, and its desire to build a coalition of illiberal nations, cannot be done by criticizing and punishing the PRC and those it courts[403].

Countering the PRC requires doubling down on liberal values and the comparative advantage they offer. More importantly, it requires, "greater attention on understanding local audiences and discussing issues that matter to them on their own terms…offer[ing] realistic and appealing solutions to the practical problems faced by other nations"[404]. In practice, this means

[400] U.S. Cyber Space Solarium Commission, "Report," p. 43.
[401] Ibid.
[402] Ibid.
[403] Daniel Markey, "Responding to China's New Tools of Global Influence," Commentary, *War on the Rocks*, April 1, 2020, https://warontherocks.com/2020/04/responding-to-chinas-new-tools-of-global-influence/.
[404] Ibid.

investing in human capital at home and abroad by improving the quality of and access to education, healthcare, travel, jobs, the free press, vital infrastructure, human rights, and justice. This can even mean, "building on Chinese projects in ways that serve local needs while demonstrating…goodwill and technical capacity"[405].

The UK can and should avoid sabotaging its own resources at home and abroad, and and blinding itself to opportunities and US undermining multi-stakeholder partnerships…UK has common wealth + EU + 5 Eyes to work with.

Action Research

Action research is an invaluable and flexible paradigm for research and practice in virtually any context. Action research is an umbrella paradigm which can be used by any discipline or profession, and with any other research paradigms, methodology, or method. It excels at enabling effective and sustainable innovation at all scales of research, policy, and technology, via an emphasis on stakeholder integration and emergent, iterative, multi-method research cycles[406].

Action research approaches at base consist of…cycle…values….other…?

Action research approaches can and should be applied to cyber security, anticipatory intelligence, and security issues more broadly. Systemic action research may be particularly useful in such contexts[407]. Historically, action research paradigms have been most heavily utilized in organizational, healthcare, development, peace/conflict, social, political, and educational research and practice contexts. Little work appears to have been explicitly done with it in the cyber security realm and broader security realms, leaving plenty of room for new directions in research and application. In short, action research's very nature makes it uniquely adept at integrating and improving upon the opportunities, challenges, and solutions discussed in this study or otherwise.

[405] Ibid.
[406] Coghlan and Brydon-Miller, *SAGE Action Research*.
[407] Danny Burns, *Systemic Action Research: A Strategy for Whole System Change*, Bristol, UK: Policy Press, 2007.

Conclusion

As Dr. Wheeler and Dr. Williams argue, the fact is, keeping Huawei and PRC hardware out, "does not equate to successfully preventing foreign espionage or sabotage of those networks"[408]. Rather it creates a false sense of security. Even worse, "effective progress towards achieving minimally satisfactory 5G cyber risk outcomes is compromised by a hyper focus on legitimate concerns regarding Huawei"[409].

The West, and the world, "should be conducting a more balanced risk assessment, with a broader focus on vulnerabilities, threat probabilities, and impact drivers of the cyber risk equation"[410]. These steps require oversight to ensure, "that the promise of 5G is not overcome by cyber vulnerabilities, which result from hasty deployments that fail to sufficiently invest in cyber risk mitigation"[411]. Otherwise, "the after-the-fact cost of missing a proactive cybersecurity opportunity will be much greater than the cost of cyber diligence up front"[412].

Then there are the broader strategic, particularly economic and ideological, dimensions to consider. After almost all of our writing was complete, *BBC News* interviewed Eric Schmidt, who was the former CEO and executive chairman of Google and its parent company Alphabet, and is currently the chair of the US DoD's Defense Innovation Board[413]. Schmidt recognizes the threats that Huawei and the PRC pose, stating that one way or another data has gone through Huawei and ended up in the hands of the PRC.

However, Schmidt, "says the west should respond by competing with China and its technologies, rather than disengaging"[414]. In his view, "the real issue with Huawei lies in the challenge to US leadership it represents: a Chinese company operating on a global stage that is building a better product than its competitors"[415]. Of utmost importance is, "'that we have choices…the answer to Huawei…is to compete by having a product and product line that is as good'"[416].

Further, the PRC is rapidly catching up to and even surpassing the West in terms of their innovative abilities and technological capacities. This is in large part because of focused state investment. Schmidt, "denies the Chinese model of state-directed investment in technology is intrinsically more successful than a free-market model"[417]. However, the West must not ignore or undermine key strategies and assets.

---

[408] Wheeler and Williams, "Keeping Huawei".
[409] Ibid.
[410] Ibid.
[411] Ibid.
[412] Ibid.
[413] Corera, "Eric Schmidt".
[414] Ibid.
[415] Ibid.
[416] Ibid.
[417] Ibid.

The US in particular has increasingly been harming itself by cutting research and education funding, blocking immigration, and at various promoting harmful propaganda that demonizes and buries the vital role of the US government in supporting research and innovation. Indeed, "one of the problems in the US and particularly in Silicon Valley, Mr Schmidt believes, is a historical blindness to the role of the government in supporting research"; "'everything you see in Silicon Valley to the first order came from initial federal science grants of one kind or another'"[418].Schmidt, "believes the West needs to make the most of its strengths by: investing more in research funding, ensuring greater collaboration between private sector, the state and academia, [and] remaining open to the best talent from around the world"[419].

More importantly, "Schmidt views the decoupling of the technology sectors in China and the US as 'undesirable', believing it will lead to two distinct systems"[420]. The problem is that, "'once you diverge these global platforms, you don't get them back…we benefit from having a common platform of interchange…and I worry that by building these platforms separate, the countries will understand each other less'"[421]. In Schmidt's opinion, "'China's going to dominate whether we couple or decouple'"[422].

For Schmidt, the question becomes, "'do they operate on global platforms or do they operate on their own platforms'"[423]? As, "'it is in the West's interest that every technology platform has Western values in them…the more segregated the platforms are, the more dangerous it is'"[424]. In this sense, "the rise of nationalism and protectionism around the world is of 'great concern'"[425].

To Schmidt, "'the best strategy is to think of it as a competition not unlike tech companies, where there's brutal competition…[it will be] [*sic*] as rough as it could be – largely unregulated between various players – where we seek to win'"[426]. Thus, "Schmidt is cautious about picking national champions and supporting them"[427]. Similarly, while he acknowledges, "there are weaknesses in the West's own capacity, particularly in not having foundries that manufacture semiconductor chips"[428], he does not believe that recent US moves to band semiconductor sales to and production in and around the PRC is beneficial. Indeed, the ban has only harmed the US while accelerating the PRC's semiconductor independence.

Ultimately, whether discussing 5G, cybersecurity in general, or how to handle the PRC,

[418] Carera, "Eric Schmidt".
[419] Ibid.
[420] Ibid.
[421] Ibid.
[422] Ibid.
[423] Ibid.
[424] Ibid.
[425] Ibid.
[426] Ibid.
[427] Ibid.
[428] Ibid.

virtually all Western countries and allies agree that international cooperation is needed. There seems to be growing rumblings for an international technology alliance after the coronavirus pandemic passes[429]. Yet, what this cooperation looks like, who it involves and how, and who is to take the lead, are all up in the air at the moment. The US and the PRC don't appear ready to lead[430]. In this context, Huawei's threats can be reframed as opportunities, particularly for the UK.

The internationalisation of the HCSEC or the creation of an equivalent body to focus on the creation and execution of proactive and innovative approaches is a necessity. Relying on reactive and passive cyber security measures such as deterrence is ineffective[431]. Even North Korea doesn't seem terribly concerned by it[432].

For that matter, as currently conceptualized in US cyber doctrines, deterrence is arguably counterproductive against the PRC[433]. Similarly, retroactive installation of security measures inherently limits the degree of security possible in system architecture due to constraints in modifying core systems that affect functionality[434]. In short, in the context of conflicts, and particularly great power competition, such passive and reactive approaches are, "untenable – allowing opponents to shape the rules of competition"[435]. Proactivity requires a clear and coordinated understanding of ends ways and means of self and competitor[436].

An international effort by HCSEC and/or greater cybersecurity expertise sharing will significantly enhance network security worldwide. Coordinating efforts to identify the risks Huawei and other vendors present allows better security, mitigation, and contingency plans to be set in place. This would of course be on top of more typical approaches such as carrying out immediate reviews of software updates in source code, damage control, and limiting network

---

[429] Martjijn Rasser, "Technology Alliances Will Help Shape Our Post-Pandemic Future," Opinion, *C$ISRNET*, April 14, 2020, https://www.c4isrnet.com/opinion/2020/04/14/technology-alliances-will-help-shape-our-post-pandemic-future/.

[430] Elizabeth C. Economy, "The Hydra vs. the Headless Horseman: China and the United States," Blog—Asia Unbound, Council on Foreign Relations, April 15, 2020, https://www.cfr.org/blog/hydra-vs-headless-horseman-china-and-united-states.

[431] James Andrew Lewis, "Strategy After Deterrence," Commentary, CSIS, March 11, 2020, https://www.csis.org/analysis/strategy-after-deterrence; Lewis, "Cyber Solarium".

[432] David E. Sanger and Nicole Perlroth, "U.S. Accuses North Korea of Cyberattacks, a Sign that Deterrence is Failing," Asia Pacific, *The New York Times*, April 15, 2020, https://www.nytimes.com/2020/04/15/world/asia/north-korea-cyber.html.

[433] Kolton, "China's Cyber Sovereignty", p. 143.

[434] "Security-by-Design Framework Version: 1.0," Cyber Security Agency of Singapore, Accessed July 20, 2019, https://www.csa.gov.sg/-/media/csa/documents/legislation_supplementary_references/security_by_design_framework.pdf.

[435] Peter Roberts and Sidharth Kaushal, "Competitive Advantage and Rules in Persistent Competitions," Occasional Papers, RUSI, April 29, 2020, https://www.rusi.org/publication/occasional-papers/competitive-advantage-and-rules-persistent-competitions.

[436] Kolton, "China's Cyber Sovereignty"; Roberts and Kaushal, "Competitive Advantage".

penetration.

The internationalisation of HCSEC also presents opportunities for the UK to benefit from Huawei in terms of security integration, increased political capital on the world stage, technological innovation, and economic development. In turn, Huawei's economic integration with the UK and global economy disincentives malicious behaviour. By allowing them into the UK market, Huawei has something to lose.

Antagonism and rejection of Huawei's role in the marketplace on the grounds of security and threats, at least as posited so far, is not a sufficient rationale to guide a full ban decision. Rejection of the world's largest 5G supplier engenders neither friendly competition nor prosperity and peace[437]. Further, Huawei's pervasive global presence makes the elimination of their risks impossible, as, "the director general of MI5, the U.K.'s domestic intelligence service", has argued while, "insisting that Huawei's role and the risks it creates can be managed"[438]. Thus, antagonism and rejection would seem counterproductive to global security and economic interests of the UK and liberal democracies[439].

The opportunities presented by Huawei's entry into the market include cooperation to improve network security globally, economic benefits, and principally, the potential to improve relations, both between liberal democracies and with the PRC. By holding market leaders like Huawei, Ericsson, and Nokia to higher standards, there is potential for a knock-on effect of better cybersecurity across the entire 5G industry and all future industries that base themselves on 5G. The trickle-down benefits of holding market leaders accountable in cybersecurity are positive for future technologies and systems, from economic and security perspectives. It is thus more beneficial to attempt to pursue cooperation and positive competition than to not try at all.

However, while it has generally been assumed that given the prospect of the PRC's integration into the global economy, they would not risk using Huawei to pursue political agendas and behave maliciously, the possibility remains that Huawei could be commanded to install backdoors, if it hasn't already. With questions of US-PRC decoupling agitated by[440] Trump's May 2020 threat to, "cut off the whole relationship"[441], with the PRC, the safeguard of economic integration is increasingly threatened and the risks of malicious behavior are raised. This raises two questions. Namely, what is to be done, and who is to lead?

---

[437] Muhammad Faizal Bin Abdul Rahman and Russell Huang, "The Asia-Pacific's Huawei Conundrum," Flashpoints—Security, *The Diplomat*, March 12, 2020, https://thediplomat.com/2020/03/the-asia-pacifics-huawei-conundrum/.

[438] Glosserman, "Huawei Realities".

[439] Kania and Gorman, "United Talent"; Lairson, Skidmore, and Xinbo, "US Backfired".

[440] Ibid.

[441] Laura Widener, "Trump Says 'We Could Cut Off Whole Relationship' with China; Among Options," *American Military News*, May 14, 2020, https://americanmilitarynews.com/2020/05/trump-says-we-could-cut-off-whole-relationship-with-china-among-options/.

As discussed, Dr. Lewis argues that the most secure option is the US approach of fully banning Huawei, as opposed to just keeping them out of critical networks. However, even he acknowledged that some countries do not believe for various reasons that a full ban is either necessary or in their overall best interest. Again, part of the issue, at least for the UK and presumably others, is that the PRC has already employed a variety of means to successfully infiltrate various networks. More importantly many, including the UK, have concluded that their economic and security interests can both be maximized via a well-executed partial ban, focused on protecting critical infrastructure.

Clearly, there is a split when it comes to what to do. Worse, this split among allies and strategic partners has become adversarial and distracted from numerous options for constructive compromise that can maximize everyone's interests. This rupture among allies is similar to the binary being imposed upon the world order by the US and the PRC. These ruptures are in many ways a function of leadership.

Before President Trump took office, the US took part in the international public-private efforts to forge global 5G standards, oversight, and security, via the 3rd Generation Partnership Project (3GPP). The Obama administration, within the US and with the 3GPP, focused on bringing experts together to, "identify public safety and cybersecurity risk considerations", and, "implement cybersecurity risk reduction as part of the development and deployment cycle"[442] However, as Dr. Schneier alludes to, profit, politics, and ease were prioritized over security[443].

Lobbyists and Republican Federal Communications Commission Members blocked these efforts. In 2016 the cyber security initiatives were scrapped by the Trump administration, which then left the 3GPP[444]. Over the years that followed, domestically and internationally, US cybersecurity and 5G policies lacked a coherent strategy, with the Trump administration wavering between ignoring, disrupting, and dismantling cyber security efforts. The "responsibility" was left to Congress, which has traditionally abdicated this role to lobbyists[445].

The Cyberspace Solarium Commission[446] is arguably the first strong Congressional effort[447]. Yet, as discussed, it has concerning weaknesses[448]. Additionally, its recommendations

---

[442] Wheeler and Simpson, "5G Requires".
[443] Wheeler and Simpson, "5G Requires"; Schneier, "China Problem".
[444] Wheeler and Simpson, "5G Requires".
[445] Ishan Mehta, "Under Trump, the Fight Against Cybercrime has Waned," Security—Opinion, *WIRED*, June 20, 2019, https://www.wired.com/story/under-trump-the-fight-against-cybercrime-has-waned/; Susan Landau, "A Security Failure in the White House," Cyber & Technology, *Lawfare*, November 1, 2019, https://www.lawfareblog.com/security-failure-white-house; Breanne Deppisch, "DHS was Finally Getting Serious About Cybersecurity. Then Came Trump," Magazine Feature, *Politico*, December 18, 2019, https://www.politico.com/news/magazine/2019/12/18/america-cybersecurity-homeland-security-trump-nielsen-070149
[446] U.S. Cyber Space Solarium Commission, "Report".
[447] Mehta, "Under Trump".

will almost certainly be slowly and selectively legislated and enforced[449].

Alarmingly, Congress had to compel the Trump administration to act on 5G security[450]. The US's Secure 5G and Beyond Act, signed into law on March 23, 2020[451], obligates the executive branch to develop a national and international strategy for, "issues faced by 5G and future generations of wireless networks", within 180 days[452]. In addition to strengthening industry partnerships[453], it also requires that the executive branch, "assist mutual defense treaty allies, strategic partners, and other countries in maximizing the security of 5G systems and infrastructure"[454].

Soon after, in late March, the White House released a broadly outlined strategy[455]. It principally references "The Prague Proposals"[456], a document resulting from the May 2019 Prague 5G Security Conference, particularly when it comes to international standards and partnerships. The conference included all Five-Eyes partners, EU members, Japan, South Korea, Israel, and a few other, primarily NATO, members. The PRC was not included, and though neither it nor Huawei were mentioned, the document's goals are in part aimed at mitigating their risks[457].

The Prague Proposals emphasize cooperation on all fronts between the participating nations. The US and the White House's strategy also outlines the need for such cooperation, yet it emphasises US leadership. In the context of what has transpired between the release of the Prague Proposals and the White House's release of their strategy, it's worth questioning whether

---

[448] Lewis, "Cyber Solarium".

[449] Andrew Eversden, "Cyber Policy Suggestions for Pentagon Could be Implemented This Year," Capital Hill, *Fifth Domain*, April 22, 2020, https://www.fifthdomain.com/congress/capitol-hill/2020/04/22/cyber-policy-suggestions-for-pentagon-could-be-implemented-this-year/.

[450] Wheeler and Simpson, "5G Requires".

[451] John Cornyn, "S.893 – Secure 5G and Beyond Act of 2020," 116th Congress Public Law 129, U.S. Government Publishing Office, March 23, 2020, https://www.congress.gov/bill/116th-congress/senate-bill/893/text?overview=closed.

[452] Andrew Eversden, "Trump Administration Must Produce 5G Security Strategy Under New Law," Critical Infrastructure, *Fifth Domain*, March 24, 2020, https://www.fifthdomain.com/civilian/2020/03/24/trump-administration-must-produce-5g-security-strategy-under-new-law/.

[453] Andrew Eversden, "Ways Government, Industry Can Overcome a Perpetual Challenge," Industry, *Fifth Domain*, March 16, 2020, https://www.fifthdomain.com/home/2020/03/16/ways-government-industry-can-overcome-a-perpetual-challenge/.

[454] Cornyn, "S.893".

[455] Donald J. Trump, "National Strategy to Secure 5G of the United States of America," The White House. March 2020, https://www.whitehouse.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf.

[456] "The Prague Proposals," Government of the Czech Republic, March 5, 2019, https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/.

[457] Michael Kahn and Jan Lopatka, "Western Allies Agree 5G Security Guidelines, Warn of Outside Influence," Technology News, *Reuters*, May 3, 2019, https://www.reuters.com/article/us-telecoms-5g-security/western-allies-agree-5g-security-guidelines-warn-of-outside-influence-idUSKCN1S91D2.

the US is looking to lead cooperation, or just to employ coercive, counterproductive, methods.

The battle for 5G in many ways comes down to who influences its technological and legal standards[458]. Between its withdrawal from the 3GPP, and its policies aimed at Huawei beginning in May 2019, the US has effectively removed itself from standards setting and the battle it seeks to lead and win[459]. As of May 11, 2020, participation and cohesive strategy are lacking[460].

Between the coronavirus[461], current leadership, and the state of international relations, for Europe and others it seems risky to depend on the US for the generation and execution of such an international strategy[462]. Further, in addition to what has been discussed, some dimensions of the US approach to cyber strategy itself are off putting to its allies, and may in fact offer a variety of opportunities for adversaries to exploit[463]. A similar dynamic is playing out among non-allied countries struggling to balance their US and PRC interests (i.e. members of the Association of Southeast Asian Nations)[464]. Indeed, though Dr. Lewis may disagree to some extent, to Dr. Schneier it seems that the US has generally missed its opportunities for proactive global leadership when it comes to 5G and cybersecurity in the short and long run.

At least for the moment, the means and ends of liberal democracies' economic and security interests, let alone those of other nations, clearly aren't quite the same. With effective

---

[458] Nicol Turner Lee, "Navigating the U.S.-China 5G Competition," Report, Global China, The Brookings Institution, April 2020, https://www.brookings.edu/research/navigating-the-us-china-5g-competition/; Aaron Klein, Nicol Turner Lee, Carrick Flynn, Frank A. Rose, and Sheena Chestnut Greitens, "Panel Conversation: Global Technology Infrastructure," Moderated by Chris Meserole, Webinar: Global China—Assessing China's Technological Reach in the World, The Brookings Institution, May 8, 2020, Transcript and Video, https://www.brookings.edu/events/webinar-global-china-assessing-chinas-technological-reach-in-the-world/.

[459] Lindsay Gorman, "The U.S. Needs to Get in the Standards Game—With Like-Minded Democracies," Cybersecurity and Deterrence, *Lawfare*, April 2, 2020, https://www.lawfareblog.com/us-needs-get-standards-game-minded-democracies.

[460] Hitchens, "US Risks".

[461] Campbell and Doshi, "Coronavirus Order"; George N. Tzogopoulos, "Coronavirus, Security, and the Cyber-Order," Perspectives Papers, Begin-Sadat Center for Strategic Studies, April 21, 2020, https://besacenter.org/perspectives-papers/coronavirus-security-and-the-cyber-order/; John Seaman, (Editor), "Covid-19 and Europe China Relations: A Country-Level Analysis," Special Report, European Think-Tank Network on China, French Institute of International Relations, April 29, 2020, https://merics.org/en/report/covid-19-and-europe-china-relations.

[462] Julianne Smith and Garima Mohan, "In a Crisis, a Fumbling America Confirms Europe's Worst Fears," Commentary, *War on the Rocks*, April 23, 2020, https://warontherocks.com/2020/04/in-a-crisis-a-fumbling-america-confirms-europes-worst-fears/.

[463] Max Smeets, "Cyber Command's Strategy Risks Friction With Allies," Cybersecurity and Deterrence, *Lawfare*, May 28, 2019, https://www.lawfareblog.com/cyber-commands-strategy-risks-friction-allies; Mark Pomerleau, "Two Years in, How Has a New Strategy Changed Cyber Operations?," CyberCon, *Fifth Domain*, November 11, 2019, https://www.fifthdomain.com/dod/2019/11/11/two-years-in-how-has-a-new-strategy-changed-cyber-operations/.

[464] Seungha Lee, "Southeast Asian Struggle: Caught up in the U.S.-China 5G Rivalry," *The SAIS China Studies Review*, May 1, 2020, https://saiscsr.org/2020/05/01/southeast-asian-struggle-caught-up-in-the-u-s-china-5g-rivalry/.

US leadership looking unlikely for 5G[465] and 6G[466], and Europe in a unique position between the PRC and the US[467], it would seem that the UK has an opportunity to lead. If the UK continues its proactive work on 5G, the threats Huawei and the PRC present time can be mitigated and even turned into opportunities.

HCSEC and other UK efforts can serve as a model to be scaled up, perhaps leading to an ICSEC. The UK has the means and opportunity to lead innovative international (cyber) security efforts. It may in fact be better positioned than the US to create and lead cyber security politics[468] via an, "alliance innovation base"[469], and an "international cybersecurity capacity building community", of, "'cyber knowledge brokers'"[470], while avoiding the potential pitfalls of doing so[471]. By taking the lead, the UK can maximize the security and economic outcomes for themselves and their partners, while also creating a much stronger mechanism for dealing with Huawei and the PRC in a constructive manner[472].

[465] Kania, "Why Doesn't".
[466] Rasser, "Setting 6G".
[467] Amy Zhou, "Huawei or the Highway," World, *Harvard Political Review*, March 5, 2020, https://harvardpolitics.com/world/huawei-or-the-highway/.
[468] Dunn-Cavelty and Wenger, "Cyber Security Politics".
[469] Kliman et al., "Forging Alliance".
[470] Patryk Pawlak and Panagiota-Nayia Barmpaliou, "Politics of Cybersecurity Capacity Building : Conundrum and Opportunity," *Journal of Cyber Policy* 2, no. 1 (2017): 123, https://doi.org/10.1080/23738871.2017.1294610.
[471] Zine Homburger, "The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace," *Global Society*, 33, no. 2 (2019): 224-242, https://doi.org/10.1080/13600826.2019.1569502.
[472] Thomas Renard, "EU Cyber Partnerships: Assessing the EU Strategic Partnerships with Third Countries in the Cyber Domain." *European Politics and Society* 19, no. 3 (2018). https://doi.org/10.1080/23745118.2018.1430720; "Special Issue", *Journal of Cyber Policy*; Fabrice Pothier and David Fernandez, "China-EU: Living Up to the Ten Actions?," Ramussen Global, May 2020, https://rasmussenglobal.com/wp-content/uploads/2020/05/EU-China-_audit_Rasmussen_Global.pdf; Seaman, (Editor), "Covid Europe-China".

Bibliography

"5G Innovation Centre (5GIC) – University of Surrey." UK Research Partnership Initiative Fund. Accessed March 10, 2020. https://re.ukri.org/funding/our-funds-overview/uk-research-partnership-initiative-fund/case-studies/5g-innovation-centre-5gic-university-of-surrey/.

"5G Security: What is Trust?." Policy. US Department of State. November 2019. https://policystatic.state.gov/uploads/2019/11/5G-What-is-Trust.pdf.

"5G Round-Up: A Round-Up of Published NCSC Content Following the UK Government's 5G Announcement." NCSC. January 31, 2020. https://www.ncsc.gov.uk/information/5g-round-up.

"5G Vision." Networks. Samsung. Accessed April 21, 2020. https://www.samsung.com/global/business/networks/insights/5g-vision/.

6G Wireless Summit. http://www.6gsummit.com/

"A Transactional Risk Profile of Huawei." RWR Advisory Group. February 13, 2018. https://www.rwradvisory.com/wp-content/uploads/2019/03/RWR-Huawei-Risk-Report-2-13-18.pdf.

Ableson, Harold, Ross Anderson, Steven M. Bellovin, Joshn Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael A. Specter, and Daniel J. Weitzner. "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications." *Journal of Cybersecurity* 1, no. 1 (September 2015): 69- 79. https://doi.org/10.1093/cybsec/tyv009.

Abrami, Regina M., William C. Kirby, and F. Warren McFarlan. "Why China Can't Innovate." Innovation. *Harvard Business Review*, March 2014. https://hbr.org/2014/03/why-china-cant-innovate.

Aftergood, Steven. "Defense Contracting Fraud: A Persistent Problem." Blogs—Secrect News—Dept of Defense. Federation of American Scientists. May 10, 2019. https://fas.org/blogs/secrecy/2019/05/defense-contracting-fraud/.

Aggarwal, Vinod K. and Andrew W. Reddie. "Comparative Industrial Policy and Cybersecurity: A Framework for Analysis." *Journal of Cyber Policy* 3, no. 3 (2018): 291-305. https://doi.org/10.1080/23738871.2018.1553989.

Albergotti, Reed, Hamza Shaban, and Taylor Telford. "Qualcomm Violated Antitrust Law, Judge Rules." Technology. *The Washington Post*, May 22, 2019. https://www.washingtonpost.com/technology/2019/05/22/qualcomm-violated-antitrust-law-judge-rules/

Alberts, David S. and Thomas J. Czerwinski. *Complexity, Global Politics, and National Security*. Washington D.C.: National Defense University Press, 1997. http://www.dodccrp.org/files/Alberts_Complexity_Global.pdf.

Alecci, Scilla. "German Media Reveals How Chinese Bribes for Siemens Products Flowed." Blog. International Consortium of Investigative Journalists. October 1, 2018. https://www.icij.org/blog/2018/10/german-media-reveals-how-chinese-bribes-for-siemens-products-flowed/.

Al-Heeti, Abrar. "Huawei is the World's Top 5G Phone Vendor, Analyst Says." *CNET*, January 28, 2020. https://www.cnet.com/news/huawei-is-the-worlds-top-5g-phone-vendor-analyst-says/.

Al-Heeti, Abrar. "US Hammers Huawei with 23 Indictments for Alleged Trade Secret Theft, Fraud." *CNET*, January 29, 2019. https://www.cnet.com/news/us-hammers-huawei-with-23-indictments-for-alleged-trade-secret-theft-fraud/.

Allison, Graham. "Is China Beating America to AI Supremacy?." *The National Interest*, December 22, 2019. https://nationalinterest.org/feature/china-beating-america-ai-supremacy-106861.

"America Does Not Want China to Dominate 5G Mobile Networks.: It is Going About it the Wrong Way." Business—5Geopolitics. *The Economist*, April 8, 2020. https://www.economist.com/business/2020/04/08/america-does-not-want-china-to-dominate-5g-mobile-networks.

Anderson, Eric C. *China Restored: The Middle Kingdom Looks to 2020 and Beyond*. Santa Barbara, California: Praeger, 2010.

Anderson, Eric C. "Global Agenda 2012 - Red Cell." Global Agenda 2012 Speaker Series—Spies, Lies, & Sneaky Guys: Espionage & Intelligence in the Digital Age. University of Delaware. September 11, 2012. Video, 1h:22m:36s. https://www.youtube.com/watch?v=BAzBtVcNldY&t=1s.

Anderson, Eric C. *Sinophobia: The Huawei Story*. CreateSpace Independent Publishing Platform, 2013.

Araya, Daniel. "Huawei's 5G Dominance in the Post-American World." *Forbes*, April 5, 2019. https://www.forbes.com/sites/danielaraya/2019/04/05/huaweis-5g-dominance-in-the-post-american-world/#47d130c748f7.

Armitage, Richard L. and Victor Cha. "The 66-Year Alliance Between the U.S. and South Korea is in Deep Trouble." Newsletter. CSIS. November 25, 2019. https://www.csis.org/analysis/66-year-alliance-between-us-and-south-korea-deep-trouble.

Armstrong, Robert C., Jackson R. Mayo, and Frank Siebenlist. "Complexity Science Challenges in Cybersecurity." Sandia Report—SAND2009-2007. Sandia National Laboratories. March 2009. https://wiki.cac.washington.edu/download/attachments/7478403/Complexity+Science+Challenges+in+Cybersecurity.pdf.

Associated Press. "EU Fines Chipmaker Qualcomm for 'Predatory Pricing'." Business News. *U.S. News & World Report*, July 18, 2019. https://www.usnews.com/news/business/articles/2019-07-18/eu-fines-chipmaker-qualcomm-for-predatory-pricing.

Baksh, Mariam. "Stop Hiding Vulnerabilities Found by Red Teams, Joint Staff to Tell Military." Tech. *Defense One*, March 18, 2020. https://www.defenseone.com/threats/2020/03/stop-hiding-vulnerabilities-found-red-teams-joint-staff-tells-military/163868/?oref=d1-related-article.

Baksh, Mariam. "Pentagon Isn't Following the Cyber Steps it Asks from Suppliers, GAO Says." Tech. *Defense One*, April 15, 2020. https://www.defenseone.com/technology/2020/04/pentagon-lacks-cyber-hygiene-it-will-demand-suppliers-gao-says/164638/?oref=d-nextpost.

Barr, William. "Attorney General William Barr's Keynote Address: China Initiative Conference." Transcript. CSIS. February 6, 2020. https://www.csis.org/analysis/attorney-general-william-barrs-keynote-address-china-initiative-conference.

Bedford, Tom and Basil Kronfli. "Harmony OS: What You Need to Know About Huawei's New Operating System." News. *TechRadar*, January 17, 2020. https://www.techradar.com/news/harmonyos.

Bennett, Cory and Bryan Bender. "How China Acquires 'the Crown Jewels ' of U.S. Technology." Investigation. *Politico*, May 22, 2018. https://www.politico.com/story/2018/05/22/china-us-tech-companies-cfius-572413.

Bery, Akhil and Clarise Brown. "India and China's Digital Divorce." Eurasia Live. Eurasia Group. July 1, 2020. Video. 11m:35s. https://www.eurasiagroup.net/live-post/india-china-digital-divorce.

Bienkov, Adam. "The UK is Abandoning Its Alliance with Trump as the United States 'Withdraws from Its Leadership Around the World'." Analysis. *Business Insider*, January 12, 2020. https://www.businessinsider.com/uk-abandoning-trump-iran-us-withdraw-leadership-world-qassem-soleiman2020-1.

Bin Abdul Rahman, Muhammad Faizal and Russell Huang. "The Asia-Pacific's Huawei Conundrum." Flashpoints—Security. *The Diplomat*, March 12, 2020. https://thediplomat.com/2020/03/the-asia-pacifics-huawei-conundrum/.

Birnbaum, Emily. "House Passes Bills to Gain Upper Hand in Race to 5G." Policy. *The Hill*, January 08, 2020. https://thehill.com/policy/technology/477429-house-passes-bills-to-gain-upper-hand-in-race-to-5g.

Blackstone, Erwin A., Larry F. Darby, and Joseph P. Fuhr Jr. "The Case of Duopoly: Industry Structure is not a Sufficient Basis for Imposing Regulation." *Regulation* (Winter 2011-2012): 12-17. https://www.cato.org/sites/cato.org/files/serials/files/regulation/2012/6/v34n4-3.pdf.

Blanchard, Ben and Perry Michael. "Lack of Innovation is 'Achilles Heel' for China's Economy, Xi Says." World News. *Reuters*, May 15 2019. https://www.reuters.com/article/us-china-politics-xi/lack-of-innovation-is-achilles-heel-for-chinas-economy-xi-says-idUSKCN1SM08G.

Boehm, Eric. "Corporate Socialism? Bill Barr's Suggestion that the U.S. Should Buy Nokia or Ericsson to Counter China is a Terrible Idea." Internet. *Reason*, February 12, 2020. https://reason.com/2020/02/12/corporate-socialism-bill-barr-suggests-the-u-s-should-counter-china-by-buying-nokia-or-ericsson/.

Bohn, Dieter. "Google is Reportedly Arguing that Cutting Huawei Off From Android Threatens US Security." *The Verge*, June 7, 2019. https://www.theverge.com/2019/6/7/18656163/google-huawei-android-security-ban-claims.

Bond, David and Jim Pickard. "US Intelligence Threats to Britain 'Not Realistic', Say Spies." Political Espionage. *Financial Times*, May 31, 2019. https://www.ft.com/content/8cdc7aee-83aa-11e9-b592-5fe435b57a3b.

Borghard, Erica D. and Shawn W. Lonergan. "The Overlooked Military Implications of the 5G Debate." Blog—Net Politics. Council on Foreign Relations. April 25, 2019. https://www.cfr.org/blog/overlooked-military-implications-5g-debate.

Boulding, William and Markus Christen. "First-Mover Disadvantage." Financial Management. *Harvard Business Review*, October 2001. https://hbr.org/2001/10/first-mover-disadvantage.

Boxall, Andy. "What is 6G? It Could Make 5G Look Like 2G, but it's Not Even Close to Reality." Mobile. *Digital Trends*, February 3, 2020. https://www.digitaltrends.com/mobile/what-is-6g/.

Brantly, Aaron F. "Conceptualizing Cyber Policy Through Complexity Theory." *Journal of Cyber Policy* 4, no. 2 (2019): 275-289. https://doi.org/10.1080/23738871.2019.1583763.

Brattberg, Erik and Philipple Le Corre. "Huawei and Europe's 5G Conundrum." *The National Interest*, December 27, 2018. https://nationalinterest.org/feature/huawei-and-europe%E2%80%99s-5g-conundrum-39972.

Brinza, Andreea. "How Russia Helped the United States Fight Huawei in Central and Eastern Europe." *War on the Rocks*, March 12, 2020. https://warontherocks.com/2020/03/how-russia-helped-the-united-states-fight-huawei-in-central-and-eastern-europe/.

Budden, Phil and Fiona Murray. "Defense Innovation Report: Applying MIT's Innovation Ecosystem & Stakeholder Approach to Innovation in Defense on a Country-by-Country Basis." Working Paper. MIT LAB for Innovation Science and Policy. May 2019. https://innovation.mit.edu/assets/Defense-Innovation-Report.pdf.

Burkett, Randy. "An Alternative Framework for Agent Recruitment: From MICE to RASCALS." *Studies in Intelligence* 57, no. 1 (Extracts, March 2013): 7-17. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-57-no.-1-a/vol.-57-no.-1-a-pdfs/Burkett-MICE%20to%20RASCALS.pdf.

Burns, Danny. *Systemic Action Research: A Strategy for Whole System Change*. Bristol, UK: Policy Press, 2007.

Campbell, Kurt M. and Rush Doshi. "The Coronavirus Could Reshape Global Order." *Foreign Affairs*, March 18, 2020. https://www.foreignaffairs.com/articles/china/2020-03-18/coronavirus-could-reshape-global-order.

Campbell, Sheila and Chad Shirley. "Estimating the Long-Term Effects of Federal R&D Spending: CBO's Current Approach and Research Needs." Blog. Congressional Budget Office. June 21, 2018. https://www.cbo.gov/publication/54089.

Carmichael, Kevin. "Canada's Waffling on 5G is Just One of the Uncertainties Choking the Life Out of the Economy." Business. *Financial Post*, February 7, 2020. https://business.financialpost.com/news/economy/canadas-waffling-on-5g-is-just-one-of-the-uncertainties-choking-the-life-out-of-the-economy.

Carr, Madeline and Leonie Maria Tanczer. "UK Cybersecurity Industrial Policy: An Analysis of Drivers, Market Failures and Interventions." *Journal of Cyber Policy* 3, no. 3 (2018): 430-444. https://doi.org/10.1080/23738871.2018.1550523.

Cassin, Richard L. "Alcatel-Lucent Settles Bribery Case." *The FCPA Blog*, December 28, 2010. https://fcpablog.com/2010/12/28/alcatel-lucent-settles-bribery-case/.

Castellani, Brian. "Map of the Complexity Sciences." Art & Science Factory. 2018. https://www.art-sciencefactory.com/complexity-map_feb09.html.

Chaffin, Larry. "60 Minutes Torpedoes Huawei in Less Than 15 Minutes: Cyber Espionage, Huawei, and the China [*sic*] Government." Putting Realism into Your Network. *Network World*, October 7, 2012. https://www.networkworld.com/article/2223272/60-minutes-torpedoes-huawei-in-less-than-15-minutes.html.

Chan, Tara Francis. "The Very Purpose of the Chinese Tech Company ZTE is to Spy on Other Countries, a Competitor Alleges in New Court Documents." *Business Insider*, June 1, 2018. https://www.businessinsider.com/zte-created-to-spy-according-to-new-court-documents-2018-6.

Chandler, Mark. "Huawei and Cisco's Source Code: Correcting the Record." Executive Platform. *Cisco Blogs*, October 11, 2012. https://blogs.cisco.com/news/huawei-and-ciscos-source-code-correcting-the-record.

Chatzky, Andrew and James McBride. "China's Massive Belt and Road Initiative." Backgrounder. Council on Foreign Relations. Accessed March 24, 2020. https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative.

Cheney, Clayton. "China's Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism." Blog—Net Politics. Council on Foreign Relations. September 26, 2019. https://www.cfr.org/blog/chinas-digital-silk-road-strategic-technological-competition-and-exporting-political.

Chhabra, Tarun, Rush Doshi, Ryan Hass, and Mira Rapp-Hooper. "Rethinking US-China Competition: Next Generation Perspectives – A Brookings Interview." By Bruce Jones. Edited by Bruce Jones and Will Moreland. Foreign Policy at Brookings. The Brookings Institution, June 2019. https://www.brookings.edu/wp-content/uploads/2019/06/FP_20190625_global_china.pdf.

China Team. "The Costs of International Advocacy: China's Interference in United Nations Human Rights Mechanisms." Report. Human Rights Watch. September 5, 2017. https://www.hrw.org/report/2017/09/05/costs-international-advocacy/chinas-interference-united-nations-human-rights.

"Chinese Telecommunications Conglomerate Huawei and Subsidiaries Charges in Racketeering Conspiracy and Conspiracy to Steal Trade Secrets." Justice News. US Department of Justice – Office of Public Affairs. February 13, 2020. https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-subsidiaries-charged-racketeering.

Choucri, Nazli and David D. Clark. *International Relations in the Cyber Age: The Co-Evolution Dilemma*. Cambridge, MA, US: MIT Press, 2019.

Cimpanu, Catalin. "Malware Found Preinstalled on Some Alcatel Smartphones." *ZDNet*, January 10, 2019. https://www.zdnet.com/article/malware-found-preinstalled-on-some-alcatel-smartphones/.

Clark, Robert. "No One Wants to Talk About Huawei's State Subsidies." News Analysis. *Light Reading*, January 9, 2020. https://www.lightreading.com/asia-pacific/no-one-wants-to-talk-about-huaweis-state-subsidies/d/d-id/756697.

"CMMC Model." Cybersecurity Maturity Model Certification. Office of the Undersecretary of Defense for Acquisition & Sustainment. Accessed March 30, 2020. https://www.acq.osd.mil/cmmc/draft.html

Coghlan, David and Mary Brydon-Miller. (Editors). *The SAGE Encyclopedia of Action Research, Vol I & II*. London: SAGE Publications, Ltd., 2014.

Corera, Gordan. "Eric Schmidt: Huawei has Engaged in Unacceptable Practices." Technology. *BBC News*, June 18, 2020. https://www.bbc.com/news/technology-53080113.

Cornyn, John. "S.893 – Secure 5G and Beyond Act of 2020." 116th Congress Public Law 129. U.S. Government Publishing Office. March 23, 2020. https://www.congress.gov/bill/116th-congress/senate-bill/893/text?overview=closed.

Cosby, John. "The Most Resilient Organizations Follow Outcome Based Cybersecurity." Opinion. *Fifth Domain*, March 30, 2020. https://www.fifthdomain.com/opinion/2020/03/31/the-most-resilient-organizations-follow-outcome-based-cybersecurity/.

Crawford, Susan P. *Captive Audience: The Telecom Industry and Monopoly Power in the New Gilded Age*. New Haven, Connecticut, US: Yale University Press, 2013.

"Cumulative Index for *International Security*, through Vol. 44, No. 4 (Spring 2020). Quarterly Journal—International Security. Harvard University's Belfer Center for Science and International Affairs. The MIT Press. Accessed April 25, 2020. https://www.belfercenter.org/journal-international-security/overview#!cumulative-index.

"Cyber Crime." United Nations – Office on Drugs and Crime. Accessed March 25, 2020. https://www.unodc.org/unodc/en/cybercrime/index.html.

Danov, Mihail. "Global Competition Law Framework: A Private International Law Solution Needed." *Journal of Private International Law* 12, no. 1 (2016): 77-105. https://doi.org/10.1080/17441048.2016.1150103.

"Data Collection Technical Details FAQ's." Phones. Nokia. https://www.nokia.com/phones/en_int/data-collection-tech-details.

Davidson, Helen and Ben Doherty. "Explainer: What is the Deadly India-China Border Dispute About?." World—India. *The Guardian*, June 16, 2020. https://www.theguardian.com/world/2020/jun/17/explainer-what-is-the-deadly-india-china-border-dispute-about.

Davies, Jamie. "UK Gov Reserves £6.8bn to Realise 5G dream by 2027." News. *Telecoms*, November 27, 2018. https://telecoms.com/493818/uk-gov-reserves-6-8bn-to-realise-5g-dream-by-2027/.

De Domenico, M., Dirk Brockmann, Chico Camargo, Carlos Gershenson, Daniel Goldsmith, Sabine Jeschonnek, Lorren Kay, Stefano Nichele, Jose R. Nicolas, Thomas Schmickl, Massimo Stella, Josh Brandoff, Angel Jose Martinez Salinas, and Hiroki Sayama. *Complexity Explained.* Creative Commons, 2019. DOI 10.17605/OSF.IO/TQGNW.

De Domenico, Manlio and Hiroki Sayama. (Coordinators). Complexity Explained. Accessed, May 1, 2020. https://complexityexplained.github.io/.

DeAeth, Duncan. "Taiwan's Foxconn Victim of Webmail System Hack, Employee Data Compromised." Business. *Taiwan News*, April 15, 2019. https://www.taiwannews.com.tw/en/news/3680809.

"Department of Commerce Renews Temporary General License for 45 Days." Press Releases – Trade Enforcement. *US Department of Commerce – Office of Public Affairs*. February 13, 2020. https://www.commerce.gov/news/press-releases/2020/02/department-commerce-renews-temporary-general-license-45-days.

"Department of Commerce Extends Public Comment Period for Input on Huawei Temporary General License Extensions." Press Releases – Trade Enforcement. US Department of Commerce – Office of Public Affairs. March 25, 2020. https://www.commerce.gov/news/press-releases/2020/03/department-commerce-extends-public-comment-period-input-huawei.

Deppisch, Breanne. "DHS was Finally Getting Serious About Cybersecurity. Then Came Trump." Magazine Feature. *Politico*, December 18, 2019. https://www.politico.com/news/magazine/2019/12/18/america-cybersecurity-homeland-security-trump-nielsen-070149

DeVine, Michael E. "United States Foreign Intelligence Relationships: Background, Policy and Legal Authorities, Risks, Benefits." Report. Congressional Research Service. May 15, 2019. https://fas.org/sgp/crs/intel/R45720.pdf.

Dienst, Jonathan, Joe Valiquette, and Rich Schapiro. "New York Tech Firm Sold Chinese Equipment to U.S. Military, Feds Say." U.S. News. NBC News. November 7, 2019. https://www.nbcnews.com/news/us-news/feds-raid-new-york-tech-firm-suspected-selling-chinese-equipment-n1078191.

Doffman, Zak. "Huawei Accused of 'Theft and Dubious Ethics' - - But That's Not the Worst of it." Innovation. *Forbes*, May 25, 2019. https://www.forbes.com/sites/zakdoffman/2019/05/25/huawei-accused-of-theft-and-dubious-ethics-why-it-should-come-as-no-surprise/#296527373f59.

Doffman, Zak. "China Just Crossed a Dangerous New Line for Huawei: 'There Will be Consequences." Innovation. *Forbes*, December 16, 2019. https://www.forbes.com/sites/zakdoffman/2019/12/16/china-just-crossed-a-dangerous-new-line-for-huawei-there-will-be-consequences/#1d3effb575a3.

Doffman, Zak. "China Just Issued Stark New Threats Over Huawei: This Time Nokia and Ericsson are in Its Sights." Innovation. *Forbes*, February 9, 2020. https://www.forbes.com/sites/zakdoffman/2020/02/09/china-just-issued-stark-new-threats-over-huawei-this-time-nokia-and-ericsson-are-in-its-sights/#57f21d2119d7.

Dunn-Cavelty, Myriam and Andreas Wenger. "Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science." *Contemporary Security Policy* 41, no. 1 (2020): 5-32. https://doi.org/10.1080/13523260.2019.1678855.

Dwyer, Morgan. "An Alternative to the Defense Department's New, Technology-Focused Organizations." Commentary. CSIS. January 22, 2020. https://www.csis.org/analysis/alternative-defense-departments-new-technology-focused-organizations.

Economy, Elizabeth C. "The Hydra vs. the Headless Horseman: China and the United States." Blog—Asia Unbound. Council on Foreign Relations. April 15, 2020. https://www.cfr.org/blog/hydra-vs-headless-horseman-china-and-united-states.

Eaglen, Mackenzie. "What if the Pentagon Skipped 5G?." Ideas. *Defense One*, May 11, 2020. https://www.defenseone.com/ideas/2020/05/what-if-pentagon-skipped-5g/165277/.

"Ericsson Fined $1 Billion for Widespread Corruption." News. *Deutsche Welle*, December 7, 2019. https://p.dw.com/p/3UMt3.

Esper, Mark. "Global Security Forum: Emerging Technologies Governance." By Kathleen H. Hicks. Transcript. CSIS. January 24, 2020. https://www.csis.org/analysis/global-security-forum-emerging-technologies-governance.

"EU Deals Another Blow to US, Allowing Members to Decide on Huawei's 5G role." Europe News. CNBC via Reuters. January 29, 2020. https://www.cnbc.com/2020/01/29/eu-deals-blow-to-us-allowing-members-to-decide-on-huaweis-5g-role.html.

Eversden, Andrew. "China's 5G Tech is a National Security Issue … or is it a Trade One?." *C4ISRNET*, February 28, 2020. https://www.c4isrnet.com/show-reporters/rsa/2020/02/28/huaweis-a-national-security-issue-or-is-it-a-trade-issue/.

Eversden, Andrew. "Ways Government, Industry Can Overcome a Perpetual Challenge." Industry. *Fifth Domain*, March 16, 2020. https://www.fifthdomain.com/home/2020/03/16/ways-government-industry-can-overcome-a-perpetual-challenge/.

Eversden, Andrew. "Trump Administration Must Produce 5G Security Strategy Under New Law." Critical Infrastructure. *Fifth Domain*, March 24, 2020. https://www.fifthdomain.com/civilian/2020/03/24/trump-administration-must-produce-5g-security-strategy-under-new-law/.

Eversden, Andrew. "Cyber Policy Suggestions for Pentagon Could be Implemented This Year." Capital Hill. *Fifth Domain*, April 22, 2020. https://www.fifthdomain.com/congress/capitol-hill/2020/04/22/cyber-policy-suggestions-for-pentagon-could-be-implemented-this-year/.

Eversden, Andrew. "Proposed Rule Banning Chinese Tech Needs to Consider Small Contractors, Senators Warn." Capital Hill. *Fifth Domain*, May 5, 2020. https://www.fifthdomain.com/congress/capitol-hill/2020/05/05/proposed-rule-banning-chinese-tech-needs-to-consider-small-contractors-senators-warn/.

Falk, Rachael. "Can the 'Core' and 'Edge' of a 5G Network Really be Separated?." Strategist Special Report. *The Strategist*, January 17, 2020. https://www.aspistrategist.org.au/can-the-core-and-edge-of-a-5g-network-really-be-separated/.

Farivar, Masood. "Bribery, Corruption Charges Follow Huawei Around the World." East Asia Pacific. *VOA News*, February 11, 2019. https://www.voanews.com/east-asia-pacific/bribery-corruption-charges-follow-huawei-around-world.

Farrell, Henry. "Bolton Alleges that Trump Helped Out China's Leader on ZTE. What's ZTE?." News— Monkey Cage—Analysis. *The Washington Post*, January 28, 2020. https://www.washingtonpost.com/politics/2020/01/28/bolton-alleges-that-trump-helped-out-chinas-leader-zte-whats-zte/.

Feldstein, Steven. "When it Comes to Digital Authoritarianism, China is a Challenge – But Not the Only Challenge." *War on the Rocks*, February 12, 2020. https://warontherocks.com/2020/02/when-it-comes-to-digital-authoritarianism-china-is-a-challenge-but-not-the-only-challenge/.

Fendos, Justin. "South Korea's Corruption Culture." The Koreas. *The Diplomat*, November 17, 2016. https://thediplomat.com/2016/11/south-koreas-corruption-culture/.

Field, Matthew. "Why Britain's Spooks 'Think They Know Better' Than the US on Huawei." Technology Intelligence. *The Telegraph*, January 29, 2020. https://www.telegraph.co.uk/technology/2020/01/29/britains-spooks-think-know-better-us-huawei/.

Finley, Klint. "The WIRED Guide to 5G." WIRED. December 18, 2019. https://www.wired.com/story/wired-guide-5g/.

Finley, Klint. "Senators Propose $1B to Outpace Huawei in 5G. That's Small Change." Business. *WIRED*, January 14, 2020. https://www.wired.com/story/billion-outpace-huawei-5g-small-change/.

Fletcher, Bevin. "Ericsson, Nokia ink 5G Deals with Chinese Operators – Report." 5G. *Fierce Wireless*, November 8, 2019. https://www.fiercewireless.com/5g/ericsson-nokia-ink-5g-deals-chinese-operators-report.

Ford, Lindsey. "Refocusing the China Debate: American Allies and the Question of US-China "Decoupling." Blog—Order from Chaos. The Brookings Institution. February 7, 2020. https://www.brookings.edu/blog/order-from-chaos/2020/02/07/refocusing-the-china-debate-american-allies-and-the-question-of-us-china-decoupling/.

"Former Alcatel Exec Sentenced." News Wire Feed. *Light Reading*, September 24, 2008. https://www.lightreading.com/former-alcatel-exec-sentenced/d/d-id/661544.

Fravel, M. Taylor, J. Stapleton Roy, Michael D. Swaine, Susan A. Thornton, and Ezra Vogel. "China is Not an Enemy." Opinions. *The Washington Post*, July 3, 2019. https://www.washingtonpost.com/opinions/making-china-a-us-enemy-is-counterproductive/2019/07/02/647d49d0-9bfa-11e9-b27f-ed2942f73d70_story.html.

Friedman, Uri. "How to Choose Between the U.S. and China? It's Not That Easy." Politics. *The Atlantic*, July 26, 2019. https://www.theatlantic.com/politics/archive/2019/07/south-korea-china-united-states-dilemma/594850/.

Fulton III, Scott. "What is 5G? The Business Guide to Next-Generation Wireless Technology." How 5G Will Transform Business. *ZDNet*, September 19, 2019. https://www.zdnet.com/article/what-is-5g-the-business-guide-to-next-generation-wireless-technology/.

Gallagher, Sean. "How US Software Ended Up Powering Chinese Assault Helicopters." Policy. *Ars Technica*, July 3, 2012. https://arstechnica.com/tech-policy/2012/07/how-us-software-ended-up-in-chinese-assault-helicopters/.

Garfinkle, Adam. "Power Concentrations: The Net Effect." *The American Interest*, April 7, 2020. https://www.the-american-interest.com/2020/04/07/the-net-effect/.

Garlick, Jeremy. "Not So Simple: Complexity Theory and the Rise of China." *China Report* 52, no. 4 (2016): 284-305. https://doi.org/10.1177/0009445516661884.

Garmey, Brian. "How Federal Agencies Can Better Manage Supply-Chain Cyber Risks." Opinion. *Fifth Domain*, July 17, 2019. https://www.fifthdomain.com/opinion/2019/07/17/how-federal-agencies-can-better-manage-supply-chain-cyber-risks/.

Garnick, Jennifer Stisa. "Huawei Hacking is a Security Scandal." *Just Security*, March 24, 2014. https://www.justsecurity.org/8488/huawei-hacking-security-scandal/.

Garside, Juliette. "Apple Supplier Foxconn Hacked in Factory Conditions Protest." Technology—Apple. February 9, 2012. https://www.theguardian.com/technology/2012/feb/09/apple-foxconn-hackers-factory-conditions.

Geer, Dan, Eric Jardine, and Eireann Leverett. "On Market Concentration and Cybersecurity Risk." *Journal of Cyber Policy* (published online February 24, 2020). https://doi.org/10.1080/23738871.2020.1728355.

Ghoshal, Anirban. "Nokia, Ericsson to Soon Export 5G Equipment Made in India." Technology. *TechCircle*, October 26, 2018. https://www.techcircle.in/2018/10/26/nokia-ericsson-to-soon-export-5g-equipment-made-in-india.

Giglio, Mike. "China's Spies Are on the Offensive." Politics. *The Atlantic*, August 26, 2019. https://www.theatlantic.com/politics/archive/2019/08/inside-us-china-espionage-war/595747/.

Gilding, Simeon. "5G Choices: A pivotal Moment in World Affairs." *The Strategist*, January 29, 2020. https://www.aspistrategist.org.au/5g-choices-a-pivotal-moment-in-world-affairs/.

Gill, Indermit. "Whoever Leads in Artificial Intelligence in 2030 Will Rule the World Until 2100." Blog—Future Development. The Brookings Institution. January 17, 2020. https://www.brookings.edu/blog/future-development/2020/01/17/whoever-leads-in-artificial-intelligence-in-2030-will-rule-the-world-until-2100/.

Gillispie, Clara. "South Korea's 5G Ambitions." Academic Paper Series. Korea Economic Institute of America. March 23, 2020. http://keia.org/sites/default/files/publications/kei_aps_gillispie_200316.pdf.

Gioe, David V. "'The More Things Change': HUMINT in the Cyber Age." In *The Palgrave Handbook of Security, Risk and Intelligence*, edited by Robert Dover, Huw Dylan, and Michael Goodman, 213-227. London: Palgrave Macmillan, 2017.

Gioe, David V., Michael S. Goodman, and Alicia Wanless. "Rebalancing Cybersecurity Imperatives: Patching the Social Layer." *Journal of Cyber Policy* 4, no. 1 (2019): 117-137. https://doi.org/10.1080/23738871.2019.1604780.

Glosserman, Brad. “Huawei and the Realities of the 5G World.” Commentary/World. *The Japan Times*, February 3, 2020. https://www.japantimes.co.jp/opinion/2020/02/03/commentary/world-commentary/huawei-realities-5g-world/#.Xptzo-pKjIV.

Goldstone, Jack A., Robert H. Bates, David L. Epstein, Ted Robert Gurr, Michael B. Lustik, Monty G. Marshall, Jay Ulfelder, and Mark Woodward. "A Global Model for Forecasting Political Instability." *American Journal of Political Science* 54, no. 1 (2010): 190-208. www.jstor.org/stable/20647979.

Gong, Yeming. *Global Operations Strategy: Fundamentals and Practice*. Berlin: Springer-Verlag, 2013.

Goodman, Matthew P. “Predatory Economics and the China Challenge.” *Global Economics Monthly* 6, no. 11 (November 2017): 1-2. https://www.csis.org/analysis/predatory-economics-and-china-challenge.

Goodman, Michael S. “The Foundations of Anglo-American Intelligence Sharing.” *Studies in Intelligence* 59, no. 2 (Extracts, June 2015): 1-12. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-59-no-2/pdfs/Goodman-Evolution-UK-US-JIC-June-2015.pdf.

Goodman, Ryan. “International Proscriptions on Mass Surveillance (or What’s Missing in the Greenwald vs. Wittes Debate.” *Just Security*, March 24, 2014. https://www.justsecurity.org/8448/international-proscriptions-mass-surveillance-or-whats-missing-greenwald-vs-wittes-debate/.

Gorman, Lindsay and Matt Schrader. “U.S. Firms Are Helping Build China’s Orwellian State.” Argument. *Foreign Policy*, March 19, 2019. https://foreignpolicy.com/2019/03/19/962492-orwell-china-socialcredit-surveillance/.

Gorman, Lindsay. “The U.S. Needs to Get in the Standards Game—With Like-Minded Democracies.” Cybersecurity and Deterrence. *Lawfare*, April 2, 2020. https://www.lawfareblog.com/us-needs-get-standards-game-minded-democracies.

Gould, Joe. “Key Republicans Seek Ban on Intel Sharing with Countries that Use Huawei.” 5G. *C4ISRNET*, January 27, 2020. https://www.c4isrnet.com/congress/2020/01/27/key-republicans-seek-ban-on-intel-sharing-with-countries-that-use-huawei/.

Graff, Garrett M. "The US is Losing Its Fight Against Huawei." Business. *WIRED*, January 29, 2020. https://www.wired.com/story/uk-huawei-5g-networks-us/.

Greene, Jay and Shara Tibken. "Lawmakers to U.S. Companies: Don't Buy Huawei, ZTE." *CNET*, October 8, 2012.

Haass, Richard N. "The Age of Nonpolarity: What Will Follow U.S. Dominance." *Foreign Affairs*, May/June, 2008. https://www.foreignaffairs.com/articles/united-states/2008-05-03/age-nonpolarity.

Hamilton, Isobel Asher. "The Trump Administration failed to Convince the UK to Ditch Huawei and Its Other Allies Aren't Listening Either." *Business Insider*, March 11, 2020. https://www.businessinsider.com/huawei-how-allies-are-reacting-to-us-calls-to-avoid-the-tech-firm-2019-2.

Harrington Jr., Joseph E. *The Theory of Collusion and Competition Policy*. Cambridge, Massachusetts: Massachusetts Institute of Technology, 2017.

Harris, Peter. "When Will the Unipolar World End?: Hegemony is Premised on Dominance in Asia and Europe." *The National Interest*, May 27, 2019. https://nationalinterest.org/feature/when-will-unipolar-world-end-59202.

H., Stuart. "Zero Trust Architecture Design Principles: Alpha Release for the ZTA Principles on GitHub." Blog Post. NCSC. November 20, 2019. https://www.ncsc.gov.uk/blog-post/zero-trust-architecture-design-principles.

Hemphill, Thomas A. and George O. White III. "China's National Champions: The Evolution of a National Industrial Policy – Or a New Era of Economic Protectionism?." *Thunderbird International Business Review* 55, no. 2 (March/April 2013). DOI: 10.1002/tie.21535.

Hendrick, Diane. "Complexity Theory and Conflict Transformation: An Exploration of Potential and Implications." Working Paper 17. Centre for Conflict Resolution—Department of Peace Studies. University of Bradford. June 2009. https://www.beyondintractability.org/bi_affiliated_projects/dsap/publications/complexity-theory-transformation-hendrick.pdf.

Hicks, Kathleen H., Joseph Federici, Seamus P. Daniels, Rhys McCormick, and Lindsey R. Sheppard. "Getting to Less? The Innovation Superiority Strategy." Report. CSIS. January 23, 2020. https://www.csis.org/analysis/getting-less-innovation-superiority-strategy.

Hieronymi, Andreas. "Understanding Systems Science: A Visual and Integrative Approach." *Systems Research and Behavioral Science* 30, no. 5 (2013): 580-595. https://doi.org/10.1002/sres.2215.

Hitchens, Theresa. "US Risks Losing 5G Standard Setting Battle to China, Experts Say." Networks/Cyber. *Breaking Defense*, May 11, 2020. https://breakingdefense.com/2020/05/us-risks-losing-5g-standard-setting-battle-to-china-experts-say/.

Hoffman, Samantha and Elsa Kania. "Huawei and the Ambiguity of China's Intelligence and Counter-Espionage Laws." *The Strategist*, September 13, 2018. https://www.aspistrategist.org.au/huawei-and-the-ambiguity-of-chinas-intelligence-and-counter-espionage-laws/.

Hofmann, Jeanette. "Multi-Stakeholderism in Internet Governance: Putting a Fiction into Practice." *Journal of Cyber Policy* 1, no. 1 (2016): 29-49. https://doi.org/10.1080/23738871.2016.1158303.

Homburger, Zine. "The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace." *Global Society*, 33, no. 2 (2019): 224-242. https://doi.org/10.1080/13600826.2019.1569502.

Horwitz, Jeremy. "U.S. 5G Security is Imperiled by Trump Administration Infighting and Fantasies." Security – Opinion. *Venture Beat*, February 6, 2020. https://venturebeat.com/2020/02/06/u-s-5g-security-is-imperiled-by-trump-administration-infighting-and-fantasies/.

Horwitz, Jeremy. "Apple, Foxconn, and 81 Others are Using Uighur Forced Labor." Mobile. *Venture Beat*, March 2, 2020. https://venturebeat.com/2020/03/02/apple-foxconn-and-81-others-are-accused-of-using-uighur-forced-labor/.

Horwitz, Josh. "The Trump Team's Idea to Counter China with Nationalized 5G is Just What China Would do." *Quartz*, January 29, 2018. https://qz.com/1191154/the-trump-teams-idea-to-counter-china-with-nationalized-5g-is-just-what-china-would-do/.

Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board. "Annual Report: 2019." HCSEC. March 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf.

Hui, Sylvia. "Engaging an Emerging Superpower: Understanding China as a Foreign Policy Actor." Asia Programme Paper. Chatham House. July 2011. https://www.chathamhouse.org/sites/default/files/0711pp_hui.pdf.

"INSCR Data Page." Center for Systemic Peace. Accessed April 9, 2020. http://www.systemicpeace.org/inscrdata.html.

Insinna, Valerie. "Pentagon Reports Boost in Predatory Foreign Investment to US Tech Firms Amid Pandemic." *C4ISRNET*, May 6, 2020. https://www.c4isrnet.com/unmanned/2020/05/06/pentagon-reports-boost-in-predatory-foreign-investment-to-us-tech-firms-since-pandemic-start/.

"International Organization." Journals. Cambridge University Press. Accessed April 19, 2020. https://www.cambridge.org/core/journals/international-organization.

Ivaldi, Marc, Bruno Jullien, Patrick Rey, Paul Seabright, and Jean Tirole. "The Economics of Tacit Collusion." Final Report for DG Competition. European Commission, March 2013. https://ec.europa.eu/competition/mergers/studies_reports/the_economics_of_tacit_collusion_en.pdf.

Janzwood, Scott and Jinelle Piereder. "Complex Systems Approaches to Global Politics." International Relations. Oxford Bibliographies. Oxford University Press. February 26, 2020. Accessed April 28, 2020. https://www.oxfordbibliographies.com/view/document/obo-9780199743292/obo-9780199743292-0278.xml?q=cyber#firstMatch.

Jennings, Ralph. "Apple Contractor Foxconn Makes Gains With Its Own Brand of Phones in a Tough Market." Asia. *Forbes*, January 31, 2019. https://www.forbes.com/sites/ralphjennings/2019/01/31/apple-contractor-foxconn-makes-gains-with-its-own-brand-of-phones-in-a-tough-market/#1ef048012c48.

Jensen, Benjamin. "When Systems Fail: What Pandemics and Cyberspace Tell Us About the Future of National Security. Commentary. *War on the* Rocks, April 9, 2020. https://warontherocks.com/2020/04/when-systems-fail-what-pandemics-and-cyberspace-tell-us-about-the-future-of-national-security/.

Jiang, Sijia. "China's Huawei to Raise Annual R&D Budget to at Least $15 Billion." Technology News. *Reuters*, July 26, 2018. https://www.reuters.com/article/us-huawei-r-d/chinas-huawei-to-raise-annual-rd-budget-to-at-least-15-billion-idUSKBN1KG169.

Jie, Yu and Joeseph Barnsley. "From Deng to Xi: Economic Reform, the Silk Road, and the Return of the Middle Kingdom." Special Report (023). LSE IDEAS. May, 2017. http://www.lse.ac.uk/ideas/Assets/Documents/reports/LSE-IDEAS-From-Deng-to-Xi.pdf.

"Johnson: Huawei 5G Decision Will Balance Innovation and Security." AJ Impact / China. *Al Jazeera*, January 27, 2020. https://www.aljazeera.com/ajimpact/johnson-huawei-5g-decision-balance-innovation-security-200127181107270.html.

Johnson, Keith and Elias Groll. "The Improbable Rise of Huawei: How did a Private Chinese Firm come to Dominate the World's Most Important Emerging Technology?." *Foreign Policy*, April 3, 2019. https://foreignpolicy.com/2019/04/03/the-improbable-rise-of-huawei-5g-global-network-china/.

Kahn, Michael and Jan Lopatka. "Western Allies Agree 5G Security Guidelines, Warn of Outside Influence." Technology News. *Reuters*, May 3, 2019. https://www.reuters.com/article/us-telecoms-5g-security/western-allies-agree-5g-security-guidelines-warn-of-outside-influence-idUSKCN1S91D2.

Kania, Elsa B. "Securing Our 5G Future: The Competitive Challenge and Considerations for U.S. Policy." Reports. Center for a New American Security. November 07, 2019. https://www.cnas.org/publications/reports/securing-our-5g-future.

Kania, Elsa B. "Why Doesn't the U.S. Have Its Own Huawei?." The 5G Future—Opinion. *Politico*, February 25, 2020. https://www.politico.com/news/agenda/2020/02/25/five-g-failures-future-american-innovation-strategy-106378.

Kania, Elsa B., and Lindsay Gorman. "The United States Can't Afford to Turn Away Chinese Talent." Argument. *Foreign Policy*, May 13, 2020. https://foreignpolicy.com/2020/05/13/united-states-cant-afford-turn-away-chinese-talent/.

Kaplan, Robert D. "America Must Prepare for the Coming Chinese Empire." *The National Interest*, June 17, 2019. https://nationalinterest.org/print/feature/america-must-prepare-coming-chinese-empire-63102.

Kaplan, Robert D. "Why the U.S.-China Cold War Will Be Different." *The National Interest*, January 19, 2020. https://nationalinterest.org/blog/buzz/why-us-china-cold-war-will-be-different-114986.

Kastrenakes, Jacob. "US, UK, and Other Governments Asks Companies to Build Backdoors into Encrypted Devices." Cybersecurity. *The Verge*, September 3, 2018. https://www.theverge.com/2018/9/3/17815196/five-eyes-encryption-backdoors-us-uk-australia-nz-canada.

Katwala, Amit. "Here's How GCHQ Scours Huawei Hardware for Malicious Code." *WIRED UK*, February 22, 2019. https://www.wired.co.uk/article/huawei-gchq-security-evaluation-uk.

Keane, Sean. "Huawei Ban: Full Timeline as it Warns Against Disrupting its Role in Britain's 5G Rollout." *CNET*, April 17, 2020. Accessed April 17, 2020 (updated regularly). https://www.cnet.com/news/huawei-ban-full-timeline-us-government-china-trump-security-threat-5g-p40/.

Kendall, Frank. "Cybersecurity Maturity Model Certification: An Idea Whose Time Has Not Come and Never May." Business. *Forbes*, April 29, 2020. https://www.forbes.com/sites/frankkendall/2020/04/29/cyber-security-maturity-model-certificationan-idea-whose-time-has-not-come-and-never-may/#35ea66773bf2.

Kennedy, Scott. "China's Uneven High-Tech Drive: Implications for the United States." Report. CSIS. February 27, 2020. https://www.csis.org/analysis/chinas-uneven-high-tech-drive-implications-united-states.

Kerbel, Josh. "Thinking Straight: Cognitive Bias in the US Debate About China." *Studies in Intelligence* 48, no. 3 (2004): 27-35. https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol48no3/pdf/v48i3a03p.pdf.

Kerbel, Josh. "Coming to Terms With Anticipatory Intelligence." Commentary. *War on the Rocks*, August 13, 2019. https://warontherocks.com/2019/08/coming-to-terms-with-anticipatory-intelligence/.

Kerber, Wolfgang and Heike Schweitzer. "Interoperability in the Digital Economy." *Journal of Intellectual Property, Information Technology and E-Commerce Law* 8, no. 1 (2017): 39-58.

Kim, Joseph. "Huawei's Puzzling Wireless Project in North Korea." George W. Bush Presidential Center, September 3, 2019. https://www.bushcenter.org/publications/articles/2019/09/huawei-wireless-north-korea.html.

Kissinger, Henry A. "The Future of U.S.-Chinese Relations: Conflict Is a Choice, Not a Necessity." *Foreign Affairs*, 91, no. 2 (2012): 44-55. https://www.jstor.org/stable/23217220.

Klein, Aaron, Nicol Turner Lee, Carrick Flynn, Frank A. Rose, and Sheena Chestnut Greitens. "Panel Conversation: Global Technology Infrastructure." Moderated by Chris Meserole. Webinar: Global China—Assessing China's Technological Reach in the World. The Brookings Institution. May 8, 2020. Transcript and Video. https://www.brookings.edu/events/webinar-global-china-assessing-chinas-technological-reach-in-the-world/.

Kliman, Daniel, Ben FitzGerald, Kristine Lee, and Joshua Fitt. "Forging an Alliance Innovation Base." Report—America Competes 2020. CNAS. March 29, 2020. https://www.cnas.org/publications/reports/forging-an-alliance-innovation-base.

Klingebiel, Ronald and John Joseph. "When First Movers are Rewarded, and When They are Not." Innovation. *Harvard Business Review*, August 11, 2015. https://hbr.org/2015/08/when-first-movers-are-rewarded-and-when-theyre-not?referral=03759&cm_vc=rr_item_page.bottom.

Knight, Will. "The Newest US Sanctions on China's Huawei Could Backfire." Business. *WIRED*, March 31, 2020. https://www.wired.com/story/newest-us-sanctions-chinas-huawei-backfire/.

Kolton, Michael. "Interpreting China's Pursuit of Cyber Sovereignty and Its Views on Cyber Deterrence." *The Cyber Defense Review* 2, no. 1 (2017): 119-54. www.jstor.org/stable/26267405.

Kubota, Yoko and Tripp Mickle. "Apple Investigated Possible Business Misconduct in its Supply Chain: Company Says it Found No Evidence of Bribery or Kickbacks." Tech. *The Wall Street Journal*, November 30, 2018. https://www.wsj.com/articles/apple-investigated-possible-business-misconduct-in-its-supply-chain-1543620611.

Kupchan, Cliff and Paul Triolo. "Distrust but Verify: How the U.S. and China Can Work Together on Advanced Technology." Business and Tech—Opinion. *SupChina*, November 26, 2019. https://supchina.com/2019/11/26/distrust-but-verify-the-us-china-advanced-technology/.

Kynge, James, Yuan Yang, and Sue-Lin Wong. "Huawei: Still Fighting for Survival Despite Trump Truce." The Big Read – Huawei Technologies. *Financial* Times, July 3, 2019. https://www.ft.com/content/a6db14d8-9993-11e9-9573-ee5cbb98ed36.

Lahiri, Tripti and Mary Hui. "Banned: How Huawei Became America's Tech Enemy No. 1." *Quartz*, May 28, 2019. https://qz.com/1627149/huaweis-journey-to-becoming-us-tech-enemy-no-1/.

Lairson, Thomas D., David Skidmore, and Wu Xinbo. "Why the US Campaign Against Huawei Backfired." Trans-Pacific View. *The Diplomat*, May 13, 2020, https://thediplomat.com/2020/05/why-the-us-campaign-against-huawei-backfired/.

Landau, Susan. "A Security Failure in the White House." Cyber & Technology. *Lawfare*, November 1, 2019. https://www.lawfareblog.com/security-failure-white-house.

Lawson, Stephen. "Nokia Closes Acquisition, Renames Nokia Siemens Networks." News—IT Leadership. *ComputerWorld*, August 7, 2013. https://www.computerworld.com/article/2484790/nokia-closes-acquisition--renames-nokia-siemens-networks.html.

Le Maistre, Ray. "Nokia Unearths AlcaLu Compliance Timebomb." Business/Employment. *Light Reading*, March 22, 2019. https://www.lightreading.com/business-employment/nokia-unearths-alcalu-compliance-timebomb/d/d-id/750356.

Le Maistre, Ray. "Huawei's Ding Gets Emotional About 5G, Boasts 91 Deals." 5G. *Light Reading*, February 20, 2020. https://www.lightreading.com/5g/huaweis-ding-gets-emotional-about-5g-boasts-91-deals/d/d-id/757629.

Ledel, Johannes and Sam Kingsley. "Can Nokia, Ericsson Compete With Huawei?." China. *Asia Times*, February 3, 2020. https://asiatimes.com/2020/02/can-nokia-ericsson-compete-with-huawei/.

Lee, Jong-Wha and Ju Hyun Pyun. "Does Trade Integration Contribute to Peace?." *Review of Development Economics* 20, no. 1 (February 2016): 327-344. https://doi.org/10.1111/rode.12222.

Lee, Seungha. "Southeast Asian Struggle: Caught up in the U.S.-China 5G Rivalry." *The SAIS China Studies Review*, May 1, 2020. https://saiscsr.org/2020/05/01/southeast-asian-struggle-caught-up-in-the-u-s-china-5g-rivalry/.

Leroux-Martin, Philippe and Vivienne O'Connor. "Systems Thinking for Peacebuilding and Rule of Law: Supporting Complex Reforms in Conflict-Affected Environments." Report. Peaceworks. United States Institute of Peace. October 23, 2017. https://www.usip.org/publications/2017/10/systems-thinking-peacebuilding-and-rule-law.

Levite, Ariel (Eli) [*sic*]. "ICT Supply Chain Integrity Principles for Governmental and Corporate Policies." Paper. The Carnegie Endowment for International Peace. October 4, 2019. https://carnegieendowment.org/2019/10/04/ict-supply-chain-integrity-principles-for-governmental-and-corporate-policies-pub-79974.

Levy, Ian. "Security, Complexity and Huawei ; Protecting the UK's Telecoms Networks." People. *NCSC Blog*, February 22, 2019. https://www.ncsc.gov.uk/blog-post/blog-post-security-complexity-and-huawei-protecting-uks-telecoms-networks.

Levy, Ian. "The Future of Telecoms in the UK." NCSC Publications. *NCSC Blog*, January 28, 2020. https://www.ncsc.gov.uk/blog-post/the-future-of-telecoms-in-the-uk.

Lewis, Ted G., Thomas J. Mackin, and Rudy Darken. "Critical Infrastructure as Complex Emergent Systems." *International Journal of Cyber Warfare and Terrorism* 1, no. 1 (2011): 1-12. DOI: 10.4018/ijcwt.2011010101.

Lewis, James Andrew. "ZTE, the Telecom Wars, and Cyber Spies." Report – CSIS Briefs. CSIS, June 25 2018. https://www.csis.org/analysis/zte-telecom-wars-and-cyber-spies.

Lewis, James Andrew. "5G To Ban or Not to Ban? It's Not Black or White." Commentary. CSIS. April 24, 2019. https://www.csis.org/analysis/5g-ban-or-not-ban-its-not-black-or-white.

Lewis, James Andrew. "Statement Before the Senate Committee on the Judiciary – '5G: The Impact on National Security, Intellectual Property, and Competition' – A Testimony by: James A. Lewis." Testimony. CSIS. May 14, 2019. https://csis-prod.s3.amazonaws.com/s3fs-public/congressional_testimony/Jim%20Lewis%20Written%20Statement%203-4-20.pdf?j.NdIo307mIklOlZ7sobLj5o088GC53m.

Lewis, James Andrew, Clete Johnson, and Denise E. Zheng. "5G Innovation and Security: Perspectives from Industry and Government Leadership." Christopher Krebs, Kim Hart, Jason Boswell, John Godfrey, Susie Armstrong, Peter Lord, Robert Strayer, Eric Wagner, Kevin Linehan, Chris Boyer, Valerie J. Parker, Geoffrey Starks, and Jennifer Lane. Event. CSIS. July 31, 2019. Audio, 2h:57m:40s. https://www.csis.org/events/5g-innovation-and-security.

Lewis, James Andrew. "What Did the United Kingdom Just Decide on Huawei and 5G?." Commentary. CSIS. January 28, 2020. https://www.csis.org/analysis/what-did-united-kingdom-just-decide-huawei-and-5g.

Lewis, James Andrew. "Can Artificial Intelligence Compensate for Strategic Shortcomings?." Commentary. CSIS. January 29, 2020. https://www.csis.org/analysis/can-artificial-intelligence-compensate-strategic-shortcomings.

Lewis, James Andrew. "Senate Committee on Commerce, Science and Transportation – 5G Supply Chain Security: Threats and Solutions – Oral Testimony of James A. Lewis." Testimony. CSIS. March 4, 2020. https://csis-prod.s3.amazonaws.com/s3fs-public/congressional_testimony/200304_Oral_Testimony.pdf?eMPCUCg_p48O8hSNQR7AgV_b3pYHpBeP.

Lewis, James Andrew. "Strategy After Deterrence." Commentary. CSIS. March 11, 2020. https://www.csis.org/analysis/strategy-after-deterrence.

Lewis, James Andrew. "Cyber Solarium and the Sunset of Cybersecurity." Commentary. CSIS. March 13, 2020. https://www.csis.org/analysis/cyber-solarium-and-sunset-cybersecurity.

Lewis, James Andrew. "Managing Semiconductor Exports to China." Commentary. CSIS, May 5, 2020. https://www.csis.org/analysis/managing-semiconductor-exports-china.

Leffler, Melvyn P. "China isn't the Society Union. Confusing the Two is Dangerous." Ideas. *The Atlantic*, December 2, 2019. https://www.theatlantic.com/ideas/archive/2019/12/cold-war-china-purely-optional/601969/.

Liao, Rita. "Huawei Says Two-Thirds of 5G Networks Outside China Now Use its Gear." *TechCrunch*, June 25, 2019. https://techcrunch.com/2019/06/25/huawei-wins-5g-contracts/.

Lieberthal, Kenneth, and Wang Jisi. "Addressing U.S.-China Strategic Distrust." In *John L. Thornton China Center Monograph Series*, no. 4. Washington D.C.: The Brookings Institution, 2012. https://www.brookings.edu/wp-content/uploads/2016/06/0330_china_lieberthal.pdf.

Lin, Justin Yifu. "Advantage of Being a Latecomer." Opinion. *China Daily*, August 7, 2013. http://www.china.org.cn/opinion/2013-08/07/content_29646629.htm.

Lin, Zhang. "US-China Trade War is Really a Clash of Civilizations and Ideologies." Economy—Opinion. *South China Morning Post*, October 15, 2018. https://www.scmp.com/economy/china-economy/article/2168492/us-china-trade-war-really-clash-civilisations-and-ideologies.

Lowsen, Ben. "Does Sino-US Competition Mean a Zero-Sum Game?: It May, but it Doesn't Have to." *The Diplomat*, January 3, 2019. https://thediplomat.com/2019/01/does-sino-us-competition-mean-a-zero-sum-game/.

"Lucent Admits to Bribery." News Wire Feed. *Light Reading*, December 21, 2007. https://www.lightreading.com/lucent-admits-to-bribery/d/d-id/650564.

Mares, Octavio. "The Most Dangerous & Spying Television Award Goes to TCL." *Information Security Newspaper*, February 4, 2020. https://www.securitynewspaper.com/2020/02/04/the-most-dangerous-spying-television-award-goes-to-tcl/.

Markey, Daniel. "Responding to China's New Tools of Global Influence." Commentary. *War on the Rocks*, April 1, 2020. https://warontherocks.com/2020/04/responding-to-chinas-new-tools-of-global-influence/.

Maxwell, Paul and Robert Barnsby. "Insecure at any Bit Rate: Why Ralph Nader is the True OG of the Software Design Industry." *Journal of Cyber Security* 4, no. 3 (2019): 346-361. https://doi.org/10.1080/23738871.2019.1671471.

Medin, Milo, Gilman Louie, Kurt DelBene, Michael McQuade, Richard Murray, and Mark Sirangelo. "The 5G Ecosystem: Risks & Opportunities for DoD." Report. Defense Innovation Board. April 3, 2019. https://media.defense.gov/2019/Apr/04/2002109654/-1/-1/0/DIB_5G_STUDY_04.04.19.PDF.

Mehta, Ishan. "Under Trump, the Fight Against Cybercrime has Waned." Security—Opinion. *WIRED*, June 20, 2019. https://www.wired.com/story/under-trump-the-fight-against-cybercrime-has-waned/.

Meyer, David. "Qualcomm Just Got Fined $1.23 Billion for Illegal Payments to Apple." Tech—Antitrust. *Fortune*, January 24, 2018. https://fortune.com/2018/01/24/qualcomm-apple-intel-antitrust-baseband-eu/.

Michta, Andrew A. "The Global Realignment: Bipolarity is Back." *The American Interest*, January, 17, 2020. https://www.the-american-interest.com/2020/01/17/bipolarity-is-back/.

"Milestones – About Huawei." Accessed February 20, 2020. https://www.huawei.com/en/about-huawei/corporate-information/milestone.

Miller, Greg. "'The Intelligence Coup of the Century': For Decades, the CIA Read the Encrypted Communications of Allies and Adversaries." National Security. *The Washington Post*, February 11, 2020. https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/.

Mishra, Yash. "Huawei Will Invest Over $17 Billion in R&D This Year." News. *Huawei Central*, July 30, 2019. https://www.huaweicentral.com/huawei-will-invest-over-17-billion-in-rd-this-year/.

Mitchell, Melanie and Santiago Guisasola. "Introduction to Complexity." Courses. Complexity Explorer. Santa Fe Institute. Accessed February 23, 2020. https://www.complexityexplorer.org/courses/104-introduction-to-complexity

Moffat, James. *Complexity Theory and Network Centric Warfare*. Information Age Transformation Series. Washington, D.C.: CCRP Publication Series, 2003. http://www.dodccrp.org/files/Moffat_Complexity.pdf.

Mogull, Rich. "Apple's Security Strategy: Make it Invisible." Business—Security—Opinion. *MacWorld*, June 14, 2013. https://www.macworld.com/article/2041724/apples-security-strategy-make-it-invisible.html.

Morris, Iain. "Where Huawei Fears to Tread." 5G. *Light Reading*, December 13, 2018. https://www.lightreading.com/mobile/5g/where-huawei-fears-to-tread/d/d-id/748266.

Morris, Iain. "Huawei Muscle Puts Ericsson, Nokia on 5G Back Foot in Europe – Sources." 5G. *Light Reading*, February 14, 2019. https://www.lightreading.com/mobile/5g/huawei-muscle-puts-ericsson-nokia-on-5g-back-foot-in-europe---sources/d/d-id/749474.

Morris, Iain. "Huawei Sets Sights on 6G Stardom Amid 5G Strife." 5G. *Light Reading*, February 15, 2019. https://www.lightreading.com/mobile/5g/huawei-sets-sights-on-6g-stardom-amid-5g-strife/d/d-id/749497.

Morris, Iain. "Ericsson, Nokia Prepared for Any US Ban on China-Made Gear." 5G. *Light Reading*, June 24, 2019. https://www.lightreading.com/mobile/5g/ericsson-nokia-prepared-for-any-us-ban-on-china-made-gear/d/d-id/752342.

Morris, Iain. "Nokia's 5G Chip Choice Leaves it Exposed." 5G. *Light Reading*, October 28, 2019. https://www.lightreading.com/5g/nokias-5g-chip-choice-leaves-it-exposed/d/d-id/755184.

Morris, Iain. "Nokia Hires 350 R&D Experts to Fix 5G Problems." 5G. *Light Reading*, October 30, 2019. https://www.lightreading.com/5g/nokia-hires-350-randd-experts-to-fix-5g-problems/d/d-id/755257.

Morris, Iain. "Nokia in Line for 5G Contracts Worth Up to $2.2B With Chinese Telcos." Asia. *Light Reading*, November 11, 2019. https://www.lightreading.com/asia-pacific/nokia-in-line-for-5g-contracts-worth-up-to-$22b-with-chinese-telcos/d/d-id/755523.

Morris, Iain. "A 6G Arms Race May Define the 2020s." 6G. *Light Reading*, February 4, 2020. https://www.lightreading.com/6g/a-6g-arms-race-may-define-the-2020s/a/d-id/757268.

Morris, Iain. "Huawei's '18-Month Lead' in 5G is Telecom's Most Spurious Claim." 5G. *Light Reading*, March 9, 2020. https://www.lightreading.com/5g/huaweis-18-month-lead-in-5g-is-telecoms-most-spurious-claim/a/d-id/758064.

Nakashima, Ellen, Jeanne Whalen, and David J. Lynch. "Pentagon Drops Opposition to New Rules that would Further Restrict Tech Sales to Huawei." Technology. *The Washington Post*, February 15, 2020. https://www.washingtonpost.com/technology/2020/02/14/pentagon-drops-opposition-new-rules-that-would-further-restrict-tech-sales-huawei/.

Naim, Moises. "The Corruption Eruption." *The Brown Journal of World Affairs* 2, no. 2 (Spring/Summer 1995): 245-261. http://bjwa.brown.edu/2-2/the-curruption-eruption/.

"National Cyber Security Strategy 2016-2021." Policy Paper. HM Government. November 1, 2016. https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.

"National Cyber Security Strategy 2016-2021: Progress Report." Policy Paper. Cabinet Office. HM Government. May 31, 2019. https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021-progress-so-far.

"National Intelligence Strategy of the United States of America 2019." Office of the Director of National Intelligence. 2019. https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf?utm_source=Press%20Release&utm_medium=Email&utm_campaign=NIS_2019.

Naughton, John. "Think Your iPhone is Safe from Hackers?: That's What They Want You to Think." Technology—Opinion. *The Guardian*, September 8, 2019. https://www.theguardian.com/technology/commentisfree/2019/sep/08/iphone-safe-from-hackers-think-again-ios-android-zero-day-exploit-zerodium-google-threat-analysis.

Newman, Lily Hay. "5G is More Secure than 4G and 3G—Except When it's Not." Security. *WIRED*, December 15, 2019. https://www.wired.com/story/5g-more-secure-4g-except-when-not/.

Nichols, Shaun. "If You're Despairing at Staff Sharing Admin Passwords, Look on the Bright Side. That's CIA-Grad Security." Security. *The Register*, June 16, 2020. https://www.theregister.com/2020/06/16/cia_report_vault_7_leak/.

Nichols, Philip M. "To Whom Does a Defense Business Owe a Duty When There is an Opportunity to Pay a Bribe?." In *Ethical Dilemmas in the Global Defense Industry*, edited by Claire Finkelstein, Kevin Govern, and Daniel Schoeni, (pages tba). New York: Oxford University Press, 2020 (to be released).

Nietsche, Carisa and Bolton Smith. "Why Europe Won't Combat Huawei's Trojan Tech." National Security. *The National Interest*, October 2, 2019. https://nationalinterest.org/feature/why-europe-wont-combat-huaweis-trojan-tech-85041.

Nietsche, Carisa and Martijn Rasser. "Washington's Anti-Huawei Tactics Need a Reboot in Europe." Argument. *Foreign Policy*, April 30, 2020. https://foreignpolicy.com/2020/04/30/huawei-5g-europe-united-states-china/.

Nietzel, Michael T. "The U.S. Loses Ground to the Rest of the World in R and D Funding." Leadership. *Forbes*, October 22, 2019. https://www.forbes.com/sites/michaeltnietzel/2019/10/22/the-us-loses-ground-to-the-rest-of-the-world-in-r-and-d-funding/#637c3864202d.

"No Pay, No Gain: Huawei Outspends Apple on R&D for a 5G Edge." New Economy. *Bloomberg News*, April 25, 2019. https://www.bloomberg.com/news/articles/2019-04-25/huawei-s-r-d-spending-balloons-as-u-s-tensions-flare-over-5g.

Nuttall, Chris. "Ericsson Claims 5G Leadership Over Huawei." Technology Sector. *Financial Times*, February 13, 2020. https://www.ft.com/content/9cdf33f0-4e8e-11ea-95a0-43d18ec715f5.

O'Hanlon, Michael E. "Forecasting Change in Military Technology, 2020-2040." Research—Report. The Brookings Institution. September 2018. https://www.brookings.edu/research/forecasting-change-in-military-technology-2020-2040/.

O'Neill, Patrick Howell. "Apple Says China's Uighur Muslims were Targeted in the Recent iPhone Hacking Campaign." Computing. *MIT Technology Review*, September 6, 2019. https://www.technologyreview.com/2019/09/06/133138/apple-says-chinas-uighur-muslims-were-targeted-in-iphone-hacking-campaign/.

"O-RAN Alliance Overview." O-RAN Alliance. Accessed April 2, 2020. https://www.o-ran.org/.

Olenick, Doug. "Brexit Cybersecurity Implications Hold Steady During Transition Period." Security News. *SC Magazine*, January 31, 2020. https://www.scmagazine.com/home/security-news/brexit-cybersecurity-implications-hold-steady-during-transition-period/.

Oliver, Richard. "Partnership and Security: Advancing US/UK Defense Technology Relationship in the Era of Globalization." Event—Summary Transcript. Edited by Peter Bean. Wilson Center. July 12, 2005. https://www.wilsoncenter.org/event/partnership-and-security-advancing-the-usuk-defense-technology-relationship-the-era.

"Open standards, not sanctions, are America's Best Weapon Against Huawei." Leaders—5Geopolitics. *The Economist*, April 8, 2020. https://www.economist.com/leaders/2020/04/08/open-standards-not-sanctions-are-americas-best-weapon-against-huawei.

Orr, Gordon. "What Can We Expect in China in 2020?." Featured Insights – Commentary. McKinsey and Company. December 2019. https://www.mckinsey.com/featured-insights/china/what-can-we-expect-in-china-in-2020.

Osnos, Evan. "The Future of Americas Contest with China." A Reporter at Large. *The New Yorker*, January 6, 2020. https://www.newyorker.com/magazine/2020/01/13/the-future-of-americas-contest-with-china.

Owen, Malcolm. "Foxconn Investigating $43M Fraud Ring Involving Faulty iPhone Parts." Articles. Apple Insider. December 18, 2019. https://appleinsider.com/articles/19/12/18/foxconn-investigating-43m-fraud-ring-involving-faulty-iphone-parts.

Pandey, Erica. "U.S. Bans Could Make Huawei Stronger." Technology. *Axios*, March 5, 2020. https://www.axios.com/huawei-cybersecurity-china-decoupling-5g-11034740-797b-4f00-a17e-7b3265d8bbcd.html.

Pancevski, Bojan. "U.S. Officials Say Huawei Can Covertly Access Telecom Networks." World. *The Wall Street Journal*, February 12, 2020. https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256.

Panettieri, Joe. "Huawei: Banned and Permitted in Which Countries? List and FAQ." ChannelE2E and After Nines Inc. Accessed March 10, 2020. https://www.channele2e.com/business/enterprise/huawei-banned-in-which-countries/.

Park, Ju-min. "Samsung Ends Mobile Phone Production in China." Technology News. *Reuters*, October 2, 2019. https://www.reuters.com/article/us-samsung-elec-china/samsung-ends-mobile-phone-production-in-china-idUSKBN1WH0LR.

Parker, George and Daniel Thomas. "UK Looks to Wean Itself Off Chinese Imports." UK Trade. *Financial Times*, June 9, 2020. https://www.ft.com/content/dc22913c-4abd-4258-89fb-e45a4342e2a6.

Pawlak, Patryk and Panagiota-Nayia Barmpaliou. "Politics of Cybersecurity Capacity Building : Conundrum and Opportunity." *Journal of Cyber Policy* 2, no. 1 (2017): 123-144. https://doi.org/10.1080/23738871.2017.1294610.

Pawlyk, Oriana and Richard Sisk. "Lawmakers Consider Blocking Some F-35 Deployments Over Huawei 5G Network: Reports." News. *Military.com*, May 13 2020. https://www.military.com/daily-news/2020/05/13/lawmakers-consider-blocking-some-f-35-deployments-over-huawei-5g-network-reports.html.

Pearlstine, Norman, David Pierson, Robyn Dixon, David S. Cloud, Alice Su, and Max Hao Lu. "The Man Behind Huawei." *The Los Angeles Times*, April 10, 2019. https://www.latimes.com/projects/la-fi-tn-huawei-5g-trade-war/.

Pearson, Erin. "Melbourne Teen Hacked into Apple's Secure Computer Network, Court Told." Crime. *The Age*, August 16, 2018. https://www.theage.com.au/national/victoria/melbourne-teen-hacked-into-apple-s-secure-computer-network-court-told-20180816-p4zxwu.html.

Peeters, Christian. "Huawei Ban Creates Challenge for Int'l Antritrust Enforcement." Expert Analysis–Opinion. *Law360*, May 30, 2019. https://www.law360.com/articles/1164251/huawei-ban-creates-challenge-for-int-l-antitrust-enforcement.

Perlow, Jason. "Paranoia Will Destroy Us: Why Huawei and Other Chinese Tech is Not Spying on Americans." Tech Broiler. *ZDNet,* May 20, 2019. https://www.zdnet.com/article/paranoia-will-destroy-you-why-chinese-tech-isnt-spying-on-us/.

Pfefferkorn, Riana. "Security Risks of Government Hacking." The Center for Internet and Society, Stanford Law School. September 2018. https://cyberlaw.stanford.edu/files/publication/files/2018.09.04_Security_Risks_of_Government_Hacking_Whitepaper.pdf.

Pomerleau, Mark. "Two Years in, How Has a New Strategy Changed Cyber Operations?." CyberCon. *Fifth Domain*, November 11, 2019. https://www.fifthdomain.com/dod/2019/11/11/two-years-in-how-has-a-new-strategy-changed-cyber-operations/.

Pomerleau, Mark. "The Pentagon is Handling Cyber Vulnerabilities Inconsistently." DoD. *Fifth Domain*, March 17, 2020. https://www.fifthdomain.com/dod/2020/03/17/the-pentagon-is-handling-cyber-vulnerabilities-inconsistently/.

Poon, Aries. "In Taiwan, Five Ex-Foxconn Employees are Indicted." Business. *The Wall Street Journal*, May 21, 2014. https://www.wsj.com/articles/five-former-foxconn-employees-indicted-for-accepting-bribes-1400651370?tesla=y.

Pothier, Fabrice and David Fernandez. "China-EU: Living Up to the Ten Actions?." Ramussen Global. May 2020. https://rasmussenglobal.com/wp-content/uploads/2020/05/EU-China-_audit_Rasmussen_Global.pdf.

Prince, Conrad. "The Coronavirus Pandemic and the Cyber Landscape." Commentary. RUSI. April 20, 2020. https://rusi.org/commentary/coronavirus-pandemic-and-cyber-landscape.

Prince, Conrad and James Sullivan. "The UK Cyber Strategy: Challenges for the Next Phase." Briefing Papers. RUSI. June 27, 2019. https://rusi.org/publication/briefing-papers/uk-cyber-strategy-challenges-next-phase.

Rasser, Martijn. "Setting the Stage for U.S. Leadership in 6G." Cyber & Technology. *Lawfare*, August 13, 2019. https://www.lawfareblog.com/setting-stage-us-leadership-6g.

Rasser, Martjijn. "Technology Alliances Will Help Shape Our Post-Pandemic Future." Opinion. *C$ISRNET*, April 14, 2020. https://www.c4isrnet.com/opinion/2020/04/14/technology-alliances-will-help-shape-our-post-pandemic-future/.

Raymond, Mark and Laura Denardis. "Multistakeholderism: Anatomy of an Inchoate Global Institution." *International Theory* 7, no. 3 (2015): 572-616. https://doi.org/10.1017/S1752971915000081.

Rayner, Gordon. "Boris Johnson Gives Clearest Indication Yet He Will Ban Huawei After Election." Politics. *The Telegraph*, December 4, 2019. https://www.telegraph.co.uk/politics/2019/12/04/boris-johnson-gives-clearest-indication-yet-will-ban-huawei/.

Reardon, Marguerite. "Nokia and Ericsson Pitch Themselves as Huawei 5G Alternative." *CNET*, March 4, 2020. https://www.cnet.com/news/nokia-and-ericsson-pitch-themselves-as-huawei-5g-alternative/.

Reichert, Corinne. "Huawei Gets Another 45-Day Reprieve from Commerce Department." *CNET*, February 14, 2020. https://www.cnet.com/news/huawei-gets-another-45-day-reprieve-from-commerce-department/.

Reichert, Corinne and Marguerite Reardon. "Huawei Says US Ban Will 'Significantly Harm' American Jobs, Companies." *CNET*, May 16, 2019. https://www.cnet.com/news/huawei-says-blacklisting-will-significantly-harm-american-companies-jobs/.

Reichert, Corinne and Sean Keane. "Huawei Says Trump's Ban Will Hurt US 5G Deployment." *CNET*, May 16, 2019. https://www.cnet.com/news/trump-effectively-bans-huawei-with-national-security-order/.

Reinsch, William Alan. "Walk the Line." Commentary. CSIS. February 3, 2020. https://www.csis.org/analysis/walk-line.

Rempfer, Kyle. "DoD Bought Phony Military Gear Made in China, Including Counter-Night Vision Clothing that Didn't Actually Work." News—Your Military. *Military Times*, May 30, 2019. https://www.militarytimes.com/news/your-air-force/2019/05/30/dod-bought-phony-military-gear-made-in-china-including-counter-night-vision-clothing-that-didnt-actually-work/.

Renard, Thomas. "EU Cyber Partnerships: Assessing the EU Strategic Partnerships with Third Countries in the Cyber Domain." *European Politics and Society* 19, no. 3 (2018). https://doi.org/10.1080/23745118.2018.1430720.

"Required Readings." Conferences—Ethical Dilemmas in the Global Defense Industry. Center for Ethics and the Rule of Law. University of Pennsylvania Law School. April 9, 2015. https://www.law.upenn.edu/institutes/cerl/conferences/ethicaldilemmas/required-readings.php.

Ribeiro, John. "U.S. Slaps Qualcomm With Multi-Million Dollar Fine Over China Corruption Allegations." News—Legal. *PCWorld*, March 2, 2016. https://www.pcworld.com/article/3040157/qualcomm-fined-in-the-us-over-china-corruption-allegations.html.

"Risks of Intelligence Pathologies in South Korea." Asia, Report 259. International Crisis Group. August 5, 2014. https://www.crisisgroup.org/asia/north-east-asia/korean-peninsula/risks-intelligence-pathologies-south-korea.

Roberts, Peter and Sidharth Kaushal. "Competitive Advantage and Rules in Persistent Competitions." Occasional Papers. RUSI. April 29, 2020. https://www.rusi.org/publication/occasional-papers/competitive-advantage-and-rules-persistent-competitions.

Rodrik, Dani. "Capitalism with US and Chinese Characteristics can Peacefully Coexist – If we Give Up on 'Hyper-Globalism'." Comment—Opinion. *South China Morning Post*, April 12, 2019. https://www.scmp.com/comment/insight-opinion/article/3005674/capitalism-us-and-chinese-characteristics-can-peacefully.

Rodrik, Dani. "Globalization's Wrong Turn and How it Hurt America." *Foreign Affairs* 98, no. 4 (July/August 2019): 26-33. https://drodrik.scholar.harvard.edu/files/dani-rodrik/files/globalizations_wrong_turn.pdf.

Rogers, James, Andrew Foxall, Matthew Henderson, Sam Armstrong, Gisela Stuart, Michael Danby, Andrew Hastie, Peter Mackay, Marco Rubio, and Bob Seely. "Breaking the China Supply Chain: How the 'Five Eyes' Can Decouple from Strategic Dependency." White Paper. Henry Jackson Society. May 2020. https://henryjacksonsociety.org/wp-content/uploads/2020/05/Breaking-the-China-Chain.pdf.

Rosenberg, Mark Y. "Experts Get Multipolarity All Wrong." *Foreign Policy*, June 24, 2019. https://foreignpolicy.com/2019/06/24/experts-get-multipolarity-all-wrong/.

Rosenberg, Matt. "The Number of Countries in the World." Geography. *ThoughtCo*. DotDash Publishing Company, February 27, 2020. https://www.thoughtco.com/number-of-countries-in-the-world-1433445.

Samuel, Juliet. "Sorry Boris, France Shows There is an Alternative to Huawei After All." News. *The Telegraph*, February 2020. https://www.telegraph.co.uk/news/2020/02/01/sorry-boris-france-shows-alternative-huawei/.

Sandle, Paul and Jack Stubbs. "Defying Trump, UK's Johnson Refuses to Ban Huawei from 5G." Technology News. *Reuters*, January 27, 2020. https://www.reuters.com/article/us-britain-usa-huawei/defying-trump-uks-johnson-refuses-to-ban-huawei-from-5g-idUSKBN1ZR02G.

Sanger, David E. and Nicole Perlroth. "N.S.A. Breached Chinese Servers Seen as Security Threat." Asia Pacific. *The New York Times*, March 22, 2014. https://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html?partner=rss&emc=rss&_r=1.

Sanger, David E. and David McCabe. "Huawei is Winning the Argument in Europe, as the U.S. Fumbles to Develop Alternatives." Politics. *The New York Times*, February 17, 2020. https://www.nytimes.com/2020/02/17/us/politics/us-huawei-5g.html.

Sanger, David E. and Nicole Perlroth. "U.S. Accuses North Korea of Cyberattacks, a Sign that Deterrence is Failing." Asia Pacific. *The New York Times*, April 15, 2020. https://www.nytimes.com/2020/04/15/world/asia/north-korea-cyber.html.

Satariano, Adam. "Britain Defies Trump Plea to Ban Huawei from 5G Network." Technology. *The New York Times*, January 28, 2020. https://www.nytimes.com/2020/01/28/technology/britain-huawei-5G.html.

Schaake, Marietje and Mathias Vermeulen. "Towards a Values-Based European Foreign Policy to Cybersecurity." *Journal of Cyber Policy* 1, no. 1 (2016): 75-84. https://doi.org/10.1080/23738871.2016.1157617.

Schiavenza, Matt. "China's Dominance in Manufacturing—in One Chart." China. *The Atlantic*, August 5, 2013. https://www.theatlantic.com/china/archive/2013/08/chinas-dominance-in-manufacturing-in-one-chart/278366/.

Schmitz Jr., James A. "The Cost of Monopoly: A New View." Article. Federal Reserve Bank of Minneapolis, July 12, 2016. https://www.minneapolisfed.org/article/2016/the-costs-of-monopoly-a-new-view.

Schneier, Bruce. "China isn't the Only Problem With 5G." Argument. *Foreign Policy*, January 10, 2020. https://foreignpolicy.com/2020/01/10/5g-china-backdoor-security-problems-united-states-surveillance/.

Schneider Jr, William. "Why 5G is a Big Deal for Militaries Throughout the World." Opinion. *C4ISRNET*, February 5, 2019. https://www.c4isrnet.com/opinion/2019/02/05/why-5g-is-a-big-deal-for-militaries-throughout-the-world/.

Schousboe, Laura. "The Pitfalls of Writing About Revolutionary Defense Technology." Commentary. *War on the Rocks*, July 15, 2019. https://warontherocks.com/2019/07/the-pitfalls-of-writing-about-revolutionary-defense-technology/.

Seaman, John. (Editor.). "Covid-19 and Europe China Relations: A Country-Level Analysis." Special Report. European Think-Tank Network on China. French Institute of International Relations. April 29, 2020. https://merics.org/en/report/covid-19-and-europe-china-relations.

"Search: 'Huawei Cyber Security Evaluation Centre Oversight Board'." Gov.uk. Accessed March 30, 2020. https://www.gov.uk/search/all?keywords=%22Huawei+Cyber+Security+Evaluation+Centre+Oversight+Board%22&order=relevance.

Sears, Nathan A. "China, Russia, and the Long 'Unipolar Moment': How Balancing Failures are Actually Extending US Hegemony." *The Diplomat*, April 27, 2016. https://thediplomat.com/2016/04/china-russia-and-the-unipolar-moment/.

"Security-by-Design Framework Version: 1.0." Cyber Security Agency of Singapore. Accessed July 20, 2019. https://www.csa.gov.sg/-/media/csa/documents/legislation_supplementary_references/security_by_design_framework.pdf.

Seely, Bob, Peter Varnish Obe, and John Hemmings. "Defending Our Data: Huawei, 5G, and the Five Eyes." Asia Studies Centre. Henry Jackson Society. May 2019. https://henryjacksonsociety.org/wp-content/uploads/2019/05/HJS-Huawei-Report-A1.pdf.

Shi, Wei. "Nokia-Branded Phones Sent Personal Data from Norway to China." News. *Telecoms.com*, March 22, 2019. https://telecoms.com/496471/nokia-branded-phones-sent-personal-data-from-norway-to-china/.

Shi, Wei. "HMD Moves Nokia Phone User Data Storage to Finland." News. *Telecoms.com*, June 19, 2019. https://telecoms.com/498007/hmd-moves-nokia-phone-user-data-storage-to-finland/.

Shipman, Tim. "Ben Wallace Interview: We Can't Rely on US." News. *The Sunday Times*, January 12, 2020. https://www.thetimes.co.uk/edition/news/ben-wallace-interview-we-cant-rely-on-us-pmwcgv398?wgu=270525_54264_15817040629028_276d8c4cf9&wgexpiry=1589480062&utm_source=planit&utm_medium=affiliate&utm_content=22278.

Silver, Laura, Kat Devlin, and Christine Huang. "China's Economic Growth Mostly Welcomed in Emerging Markets, but Neighbors Wary of its Influence." Pew Research Center: Global Attitudes and Trends. The Pew Charitable Trusts, December 5, 2019. https://www.pewresearch.org/global/2019/12/05/chinas-economic-growth-mostly-welcomed-in-emerging-markets-but-neighbors-wary-of-its-influence/.

Simpson, David. "FCC White Paper: Cybersecurity Risk Reduction." Report. Public Safety & Homeland Security Bureau—Federal Communications Commission. January 18, 2017. https://www.fcc.gov/document/fcc-white-paper-cybersecurity-risk-reduction.

Smeets, Max. "Cyber Command's Strategy Risks Friction With Allies." Cybersecurity and Deterrence. *Lawfare*, May 28, 2019. https://www.lawfareblog.com/cyber-commands-strategy-risks-friction-allies.

Smith, Julianne and Garima Mohan. "In a Crisis, a Fumbling America Confirms Europe's Worst Fears." Commentary. *War on the Rocks*, April 23, 2020. https://warontherocks.com/2020/04/in-a-crisis-a-fumbling-america-confirms-europes-worst-fears/.

Smith, Norman. "Huawei: Government Wins Vote After Backbench Rebellion." Politics. *BBC News*, March 10, 2020. https://www.bbc.com/news/uk-politics-51806704.

Soderpalm, Helana and Olof Swahnberg. ""Ericsson Has Dismissed 50 Employees Following U.S. Corruption Probe." Business News. *Reuters*, October 18, 2018. https://www.reuters.com/article/us-ericsson-probe/ericsson-has-dismissed-50-employees-following-u-s-corruption-probe-idUSKCN1MS1R4.

Solon, Olivia. "iPhone Spyware Lets Police Log Suspects' Passcodes when Cracking Doesn't Work." Tech—Security. *NBC News*, May 18, 2020. https://www.nbcnews.com/tech/security/iphone-spyware-lets-cops-log-suspects-passcodes-when-cracking-doesn-n1209296.

Soo, Zen, Zheping Huang, Sarah Dai, and Li Tao. "SCMP Series: The Battle Over 5G." *South China Morning Post*, February-June, 2019. https://series.scmp.com/5g/.

"Special Issue: Comparative Industrial Policy and Cyber Security." *Journal of Cyber Policy* 3, no. 3 (2018): 287-469. https://www.tandfonline.com/toc/rcyb20/3/3.

Statt, Nick. "US Pushing Tech and Telecom Industries to Build 5G Alternative to Huawei." Policy. *The Verge*, February 5, 2020. https://www.theverge.com/2020/2/5/21124888/us-5g-huawei-white-house-trump-china-alternative-telecom-standard.

Stecklow, Steve. "Exclusive: Newly Obtained Documents Show Huawei Role in Shipping Prohibited U.S. Gear to Iran." Technology News. *Reuters*, March 2, 2020. https://www.reuters.com/article/us-huawei-iran-sanctions-exclusive/exclusive-newly-obtained-documents-show-huawei-role-in-shipping-prohibited-u-s-gear-to-iran-idUSKBN20P1VA.

Suciu, Peter. "Tom Cotton is Trying to Block F-35 Deployment to the UK (Due to Huawei Worries)." Blog—The Buzz. *The National Interest*, May 8, 2020. https://nationalinterest.org/blog/buzz/tom-cotton-trying-block-f-35-deployment-uk-due-huawei-worries-152251.

Sullivan, James and Rebecca Lucas. "5G Cyber Security: A Risk Management Approach." The Globalisation of Technology Occasional Paper. RUSI. February 14, 2020. https://rusi.org/publication/occasional-papers/5g-cyber-security-risk-management-approach.

"Supply Chain Risk Management." The National Counterintelligence and Security Center. Office of the Director of National Intelligence. Accessed March 15, 2020. https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-supply-chain-threats.

Sutherland, Ewan. "The Strange Case of US v. ZTE: A Prosecution, a Ban, a Fine and a Presidential Intervention." *Digital Policy, Regulation and Governance* 21, no. 6 (2019): 550-573. https://doi.org/10.1108/DPRG-04-2019-0029.

Swaine, Michael D. "A Relationship Under Extreme Duress: U.S.-China Relations at a Crossroads." The Carter Center, January 16, 2019. https://www.cartercenter.org/resources/pdfs/peace/china/china-program-2019/swaine.pdf.

Taylor, Trevor and Rebecca Lucas. "Management of Cyber Security in Defense Supply Chains." *RUSI News Brief,* April 24, 2020. https://www.rusi.org/publication/rusi-newsbrief/management-cyber-security-defence-supply-chains.

Telegraph Reporters. "Donald Trump Could 'Limit Sharing of US Intelligence With the UK 'if Britain ' Fails to Ban Huawei." Technology Intelligence. *The Telegraph,* May 31, 2019. https://www.telegraph.co.uk/technology/2019/05/31/donald-trump-could-limit-sharing-us-intelligence-uk-britain/.

Thayer, Bradley A. and John M. Friend. "The World According to China: Understanding the World China Seeks to Create by 2049, When the PRC Turns 100." *The Diplomat*, October 3, 2018. https://thediplomat.com/2018/10/the-world-according-to-china/.

"The Prague Proposals." Government of the Czech Republic. March 5, 2019. https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/.

"The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028." TRADOC Pamphlet 525-7-8. Department of the Army. February 22, 2010. https://fas.org/irp/doddir/army/pam525-7-8.pdf.

Thompson, Loren. "Qualcomm Antitrust Case Raises Far-Reaching National Security Concerns." Business. *Forbes*, January 28, 2020. https://www.forbes.com/sites/lorenthompson/2020/01/28/qualcomm-antitrust-case-raises-far-reaching-national-security-concerns/#1d9399f669ea.

Ting-Fang, Cheng, and Lauly Li. "Chip Titan TSMC Caught in Crossfire between US and China." Business—Company in Focus. *Nikkei Asian Review*, May 15, 2020. https://asia.nikkei.com/Business/Company-in-focus/Chip-titan-TSMC-caught-in-crossfire-between-US-and-China.

Tisdale, Susan M. "Cybersecurity: Challenges From a Systems, Complexity, Knowledge Management and Business Intelligence Perspective." *Issues ion Information Systems* 16, no. 3 (2015): 191-198. https://iacis.org/iis/2015/3_iis_2015_191-198.pdf.

Tisdale, Susan M. "Architecting a Cybersecurity Management Framework." *Issues in Information Systems* 17, no. 4 (2016): 227-236. https://iacis.org/iis/2016/4_iis_2016_227-236.pdf.

Townsend, Will. "Who is 'Really' Leading in Mobile 5G, Part 6: Policy, Regulation and Consortia." *Forbes*, October 12, 2019. https://www.forbes.com/sites/moorinsights/2019/10/12/who-is-really-leading-in-mobile-5g-part-6-policy-regulation-and-consortia/#6f08dffd2755.

Trump, Donald J. "Executive Order on Securing the Information and Communications Technology and Services Supply Chain." Executive Orders – Infrastructure and Technology. The White House. May 15, 2019. https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

Trump, Donald J. "National Strategy to Secure 5G of the United States of America." The White House. March 2020. https://www.whitehouse.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf.

Turner Lee, Nicol. "Navigating the U.S.-China 5G Competition." Report. Global China. The Brookings Institution. April 2020. https://www.brookings.edu/research/navigating-the-us-china-5g-competition/.

Tzogopoulos, George N. "Coronavirus, Security, and the Cyber-Order." Perspectives Papers. Begin-Sadat Center for Strategic Studies. April 21, 2020. https://besacenter.org/perspectives-papers/coronavirus-security-and-the-cyber-order/.

"UK Telecoms Supply Chain Review Report." Notice. Department for Digital, Culture, Media & Sport. HM Government. July 22, 2019. https://www.gov.uk/government/publications/telecoms-supply-chain-review-terms-of-reference.

U.S. Cyberspace Solarium Commission. Chaired by Angus King and Mike Gallagher. "Report." US Congress. March 11, 2020. https://www.solarium.gov/report.

Vaswani, Karishma. "Huawei: The Story of a Controversial Company." *BBC News*, March 6, 2019. https://www.bbc.co.uk/news/resources/idt-sh/Huawei.

Venard, Bertrand. "Lessons From the Massive Siemens Corruption Scandal One Decade Later." Economy + Business. *The Conversation*, December 13, 2018. https://theconversation.com/lessons-from-the-massive-siemens-corruption-scandal-one-decade-later-108694.

Voo, Julia and Cindy Gao. "U.S.-China Cyber Competition and Cooperation with Julia Voo." By Joanna Chiu. Podcasts—NuVoices. *SupChina*, April 3, 2020. Audio, 54m:33s. https://supchina.com/podcast/u-s-china-cyber-competition-and-cooperation-with-julia-voo/.

Weber, Valentin. "Making Sense of Technological Spheres of Influence." Strategic Updates. LSE IDEAS. March 31, 2020. http://www.lse.ac.uk/ideas/publications/updates/technological-spheres-of-influence.

Weiss, Jessica Chen. "Understanding and Rolling Back Digital Authoritarianism." Commentary. *War on the Rocks*, February 17, 2020. https://warontherocks.com/2020/02/understanding-and-rolling-back-digital-authoritarianism/.

Wheeler, Tom and Robert D. Williams. "Keeping Huawei Hardware Out of the U.S. Is Not Enough to Secure 5G." Huawei. *Lawfare*, February 20, 2019. https://www.lawfareblog.com/keeping-huawei-hardware-out-us-not-enough-secure-5g.

Wheeler, Tom. "5G in Five (not so) Easy Pieces." Report. The Brookings Institution. July 9, 2019. https://www.brookings.edu/research/5g-in-five-not-so-easy-pieces/.

Wheeler, Tom and David Simpson. "Why 5G Requires New Approaches to Cybersecurity: Racing to Protect the Most Important Network of the 21st Century." Report. The Brookings Institution. September 3, 2019. https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/.

Wheeler, Tom. "Moving from 'Secret Sauce' to Open Standards for 5G." TechTank. The Brookings Institution. February 18, 2020. https://www.brookings.edu/blog/techtank/2020/02/18/moving-from-secret-sauce-to-open-standards-for-5g/.

"Why Competition and Consumer Protection Matter." Department of International Trade and Commodities—Competition Law. United Nations Conference on Trade and Development. Accessed April 17, 2020. https://unctad.org/en/Pages/DITC/CompetitionLaw/why-competition-matters.aspx.

Widener, Laura. "Trump Says 'We Could Cut Off Whole Relationship' with China; Among Options." *American Military News*, May 14, 2020. https://americanmilitarynews.com/2020/05/trump-says-we-could-cut-off-whole-relationship-with-china-among-options/.

Williams, Darrell. "US Logistics Boss Talks Risks to the Supply Chain and Protective Measures." By Jill Aitoro. Interviews. *DefenseNews*, October 28, 2019. https://www.defensenews.com/interviews/2019/10/28/us-logistics-boss-talks-risks-to-the-supply-chain-and-protective-measures/.

Wilson, Clay and Nicole Drumhiller. "US-China Relations: Cyber Espionage and Cultural Bias." In *National Security and Counterintelligence in the Era of Cyber Espionage*, edited by Eugenie de Silva, 28-47. Hershey, PA, US: Information Science Reference, 2016.

Wong, Catherine. "Thucydides Trap Author Graham Allison says China and US Must Work Together and Not End Up on Path that Leads to War." Diplomacy. *South China Morning Post*, December 20, 2018. https://www.scmp.com/news/china/diplomacy/article/2178905/thucydides-trap-author-says-china-and-us-must-work-together-and.

Woo, Stu and Dustin Volz. "U.S. Considers Requiring 5G Equipment for Domestic Use Be Made Outside China." Tech. *The Wall Street Journal*, June 23, 2019. https://www.wsj.com/articles/u-s-considers-requiring-5g-equipment-for-domestic-use-be-made-outside-china-11561313072.

Wu, Tim. "The Oligopoly Problem." Annals of Technology. *The New Yorker*, April 15, 2013. https://www.newyorker.com/tech/annals-of-technology/the-oligopoly-problem.

X., Z. (Editor). "Norway's Telenor Says to Continue Using Huawei Equipment for 5G." *XinHuaNet*, December 14, 2019. http://www.xinhuanet.com/english/2019-12/14/c_138631613.htm.

Xinbo, Wu. "U.S. Security Policy in Asia: Implications for China-U.S. Relations." Report. The Brookings Institution. September 1, 2000. https://www.brookings.edu/research/u-s-security-policy-in-asia-implications-for-china-u-s-relations/.

Yang, Heekyong. "Samsung Sets Up Anti-Corruption Panel as Chief Faces Trials." Technology News. *Reuters*, January 8, 2020. https://www.reuters.com/article/us-samsung-group-compliance/samsung-sets-up-anti-corruption-panel-as-chief-faces-trials-idUSKBN1Z80DR.

Yap, Chuin-Wei, Dan Strumpf, Dustin Volz, Kate O'Keeffe, and Aruna Viswanatha. "Huawei's Yearslong Rise is Littered With Accusations of Theft and Dubious Ethics." Tech. *The Wall Street Journal*, May 25, 2019. https://www.wsj.com/articles/huaweis-yearslong-rise-is-littered-with-accusations-of-theft-and-dubious-ethics-11558756858.

Yap, Chuin-Wei. "State Support Helped Fuel Huawei's Global Rise." Tech. *The Wall Street Journal*, December 25, 2019. https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736.

Yu, Eileen. "Huawei: Easier to Bribe Telco Staff than to Build Backdoors." Blog—By the Way. *ZDNet*, October 23, 2019. https://www.zdnet.com/article/huawei-easier-to-bribe-telco-staff-then-build-backdoors/.

Zacks, Aviva. "What is a Backdoor and How to Protect Against it." Blog. Safety Detectives. September 2, 2018. https://www.safetydetectives.com/blog/what-is-a-backdoor-and-how-to-protect-against-it/.

Zenko, Micah. *Red Team: How to Succeed by Thinking Like the Enemy*. New York: Basic Books, 2015.

Zetter, Kim. "Attackers Stole Certificate from Foxconn to Hack Kaspersky with Duqu 2.0." *WIRED*, June 15, 2015. https://www.wired.com/2015/06/foxconn-hack-kaspersky-duqu-2/.

Zhou, Amy. "Huawei or the Highway." World. *Harvard Political Review*, March 5, 2020. https://harvardpolitics.com/world/huawei-or-the-highway/.

Zibreg, Christian. "Corrupt Apple Manager Who Leaked Order Secrets to Asian Suppliers Brought to Justice." Apple. *Geek.com*, August 16, 2010. https://www.geek.com/apple/corrupt-apple-manager-who-leaked-order-secrets-to-asian-suppliers-brought-to-justice-1277412/.

Zoellick, Robert B. "Can American and China be Stakeholders?." Transcript – U.S.-China Business Council. The Carnegie Endowment for International Peace, December 4, 2019. https://carnegieendowment.org/2019/12/04/can-america-and-china-be-stakeholders-pub-80510.

"ZTE." News—Topics. Anti-Corruption Digest. Accessed March 3, 2020. https://anticorruptiondigest.com/news-topics/zte/#axzz6Hk3lzgYv.

Zweig, David and Siqin Kang. "America Challenges China's National Talent Programs." Report. CSIS. May 5, 2020. https://www.csis.org/analysis/america-challenges-chinas-national-talent-programs.