HUAWEI'S 5G NETWORKS AND THE THREAT TO AMERICA'S NATIONAL SECURITY

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE
General Studies

by

CHRISTOPHER M. GOLDEN, DEPARTMENT OF THE ARMY
B.S., American Sentinel University, Aurora, Colorado, 2007

Fort Leavenworth, Kansas
2020

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED *(From - To)*
05-06-2020	Master's Thesis	AUG 2019 – JUN 2020

4. TITLE AND SUBTITLE

Huawei's 5G Networks and the Threat to America's National Security

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Christopher M. Golden

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(E.S.)

U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(E.S.)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

President Trump reversed America's long-standing stance of engagement by signing an executive order in 2019 to contain the identified threats of Huawei and other high-risk vendors with apparent ties to the Chinese government. The move prohibits U.S. companies from using technology from any company identified as a national threat. Was this the right decision to exclude these vendors from the rollout of 5G in America? The U.S. warned other countries about the threat of backdoors through high-risk vendor equipment. Other allies took heed, performed independent security assessments, and decided to allow these high-risk vendors onto their networks. A few allied nations sided with the United States and took similar actions to ban equipment from high-risk vendors. Internationally, the Chinese government pushed back using the World Trade Organization's ability to enforce international trade standards. Huawei also reacted by filing a lawsuit against the U.S. government alleging the unfair application of the National Defense Authorization Act.

15. SUBJECT TERMS

China, CCP, Huawei, 5G, technology, national security

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. PHONE NUMBER *(include area code)*
(U)	(U)	(U)	(U)	132	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: Christopher M. Golden

Thesis Title: Huawei's 5G Networks and the Threat to America's National Security

Approved by:

_____, Thesis Committee Chair
John H. Modinger, Ph.D.

_____, Member
Phillip G. Pattee, Ph.D.

_____, Member
Matthew Fuhrer, M.S.

Accepted this 12th day of June 2020 by:

_____, Director, Office of Degree Programs
Prisco R. Hernandez, Ph.D.

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

HUAWEI'S 5G NETWORKS – AMERICA'S NATIONAL SECURITY IMPACT, BY Mr. Christopher M. Golden, 132 pages.

President Trump reversed America's long-standing stance of engagement by signing an executive order in 2019 to contain the identified threats of Huawei and other high-risk vendors with apparent ties to the Chinese government. The move prohibits U.S. companies from using technology from any company identified as a national threat. Was this the right decision to exclude these vendors from the rollout of 5G in America? The U.S. warned other countries about the threat of backdoors through high-risk vendor equipment. Other allies took heed, performed independent security assessments, and decided to allow these high-risk vendors onto their networks. A few allied nations sided with the United States and took similar actions to ban equipment from high-risk vendors. Internationally, the Chinese government pushed back using the World Trade Organization's ability to enforce international trade standards. Huawei also reacted by filing a lawsuit against the U.S. government alleging the unfair application of the National Defense Authorization Act.

ACKNOWLEDGMENTS

First and foremost, I must thank my lovely wife, Aela, and my three children for their support and patience throughout the year while I spent time locked away, developing this thesis. I hope my example of hard work and effort was instilled in you as you move forward in your educational journeys. I dedicate this project to you.

Thank you to my research committee, Dr. John Modinger, Dr. Philip Pattee, and Mr. Matthew Fuhrer, for pushing me and providing guidance to help me reach the finish line of this year-long project.

Additional thanks go out to the Combined Arms Research Library staff, who saw me regularly and aided in finding relevant research material. Mr. Florian Kardoskee and Ms. Mary Noll were both extremely friendly and helpful throughout the year.

TABLE OF CONTENTS

Page

ACRONYMS

COA:	Course of Action
CCP:	Chinese Communist Party
DCMS:	Department for Digital, Culture, Media and Sport
EU:	European Union
FAS:	Feasibility, Acceptability, Suitability
HRV:	High-Risk Vendors
IoT:	The Internet of Things
IP:	Intellectual Property
LOE:	Line of Effort
NSA:	National Security Agency
NSS:	National Security Strategy
PLA:	People's Liberation Army
PoP:	Point of Presence
WTO:	World Trade Organization

ILLUSTRATIONS

Page

CHAPTER 1

INTRODUCTION

In the days of the Roman Empire, roads radiated out from the capital city, spanning more than 52,000 miles. The Romans built these roads to access the vast areas they had conquered. But, in the end, these same roads led to Rome's downfall, for they allowed the invaders to march right up to the city gates.[1]

— Robert Mueller, FBI Director, speech given in 2007

President Trump signed an executive order, *Securing the Information and Communications Technology and Services Supply Chain*, in 2019 that prohibits the purchase of foreign equipment owned by a foreign adversary due to a direct threat to national security. The President's action added several Chinese corporations to the U.S. Department of Commerce's Bureau of Industry and Security Entity list. This move primarily impacts Huawei, a Chinese company that is the world's top telecom supplier, by banning U.S. purchase of its equipment and blocking Huawei's ability to purchase U.S. products from such companies as Google, ARM, Intel, Qualcomm, and Microsoft.[2]

In 2012, the House Intelligence Committee released a report that discouraged American companies from purchasing telecommunication equipment from Huawei due to

[1] Benjamin Wittes, "John Carlin on 'Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats,'" *Lawfare*, last modified June 21, 2016, accessed May 10, 2020, https://www.lawfareblog.com/john-carlin-detect-disrupt-deter-whole-government-approach-national-security-cyber-threats.

[2] Zak Doffman, "Huawei Goes To Court To Fight 'Illegal' Ban As China Decides On Softer Approach," *Forbes*, last modified May 29, 2019, accessed March 8, 2020, https://www.forbes.com/sites/zakdoffman/2019/05/29/huawei-goes-legal-again-as-china-tells-its-officials-and-media-back-off-the-u-s/#38e81d7f6b3b.

a direct threat to national security.[3] The committee found Huawei unwilling to explain its relationship with the Chinese government adequately and a likely existing dependency on the Chinese government for support.[4]

America is one of the founding member countries in the World Trade Organization (WTO). The WTO is an international organization that establishes and enforces international trade rules.[5] The organization strives for lowering trade barriers, including customs and tariffs, and eliminating unfair, discriminatory methods to reduce the importation of foreign products. America backed a policy of international cooperation and engagement during these decades in supporting the WTO and its efforts to eliminate barriers to international trade in the multilateral trading system they govern.

President Trump reversed America's long-standing stance of engagement to contain the identified threats of Huawei and other high-risk vendors (HRV) with ties to the Chinese government. Internationally, China pushed back using the World Trade Organization's ability to enforce international trade standards. Other allies took heed, performed independent security assessments, and decided to allow these HRV onto their networks.

---

[3] Jay Greene and Shara Tibken, "Lawmakers to U.S. Companies: Don't Buy Huawei, ZTE," *CNET*, last modified October 8, 2012, accessed March 2, 2020, https://www.cnet.com/news/lawmakers-to-u-s-companies-dont-buy-huawei-zte/.

[4] Mike Rogers and Dutch Ruppersberger, *Investigative Report on the U.S. National Security Issues Posed by Telecommunication Companies Huawei and ZTE*, U.S. House of Representatives, Permanent Select Committee on Intelligence, October 8, 2012, i, https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=96.

[5] World Trade Organization, "What Is the WTO?," accessed February 15, 2020, https://www.wto.org/english/thewto_e/thewto_e.htm.

Huawei filed a lawsuit alleging the American Government's application of the National Defense Authorization Act to exclude its products as unfair and illegal.[6] Representatives for Huawei accuse the United States Government of abusing national security exceptions while undermining global trade rules established through the WTO. Song Liuping, the chief legal officer of Huawei, added that the U.S. government had not provided any evidence that Huawei is a security threat.

Is there any substantiating evidence to justify America's concerns to prohibit Chinese access to U.S. markets? Absolutely. The Chinese government continuously attempts to access American networks to steal intellectual property (IP) secrets, worth billions of dollars annually. China previously sold counterfeit network equipment masquerading as Cisco network routers to the Pentagon.[7] Technicians connected the gear to the Pentagon networks and later found the devices to be transmitting suspicious activity back to China.

In 2009, Vodaphone, Europe's largest mobile phone operator, found several vulnerabilities in Huawei equipment. The company identified the network weaknesses to Huawei, which did not create a corrective patch for over two years. Vodaphone also found vulnerabilities in Huawei's model of routers designed for home use. These vulnerabilities also supplied backdoor access to the network and connected local

[6] Doffman, "Huawei Goes To Court To Fight 'Illegal' Ban As China Decides On Softer Approach."

[7] Bill Gertz, "Chinese Telecoms Spy for Beijing through Computer Equipment, House Intelligence Committee Leaders Say," *Washington Free Beacon*, last modified September 14, 2012, accessed March 2, 2020, https://freebeacon.com/national-security/beijings-backdoors-2/.

machines. Huawei was reluctant to disable this vulnerability, as it also offered the ability to configure devices remotely. According to Stefano Zanero, a computer security professor, these vulnerabilities, along with the company's initial denial, have the characteristics of designed backdoors.[8]

In 2015, Amazon purchased servers for deployment on their networks from an American technology company, Supermicro.[9] Before deploying the servers on its network, Amazon hired a third-party security company to run security checks on the equipment. The results of the test results were suspicious, as the testers found an embedded microchip on the motherboard that was not part of the original blueprint design. The chip was smaller than a grain of rice and cleverly concealed on the board to avoid attention.

Amazon contacted U.S. authorities, who opened a classified investigation that determined the chips allowed unauthorized access into any network.[10] The investigation concluded that the installation of the spy chips occurred in the motherboard factories in China and that operatives from the People's Liberation Army (PLA) were to blame. This degree of deception should be a massive concern to American companies and the

[8] Jon Porter, "'Hidden Backdoors' Were Found in Huawei Equipment, Reports Bloomberg," *The Verge*, last modified April 30, 2019, accessed March 2, 2020, https://www.theverge.com/2019/4/30/18523701/huawei-vodafone-italy-security-backdoors-vulnerabilities-routers-core-network-wide-area-local.

[9] Jordan Robertson and Michael Riley, "China Used a Tiny Chip in a Hack That Infiltrated U.S. Companies," *Bloomberg*, October 4, 2018, accessed March 1, 2020, https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.

[10] Ibid.

Department of Defense when most of its electronic global supply chain runs through China, and the compromise happened at that level.

Supermicro servers held several government-related contracts. Their servers resided in DOD data centers, Navy ships, and supported CIA applications.[11] Additionally, Apple had over 7,000 of the Supermicro servers deployed across their networks. Apple has never publicly admitted to the enormous tampering fiasco. Still, insiders revealed that the discovery of the spy chips led to replacing all the compromised servers from its network within weeks and canceling its contract with Supermicro the following year. Federal investigations led to the discovery of Supermicro servers compromising over 30 key U.S. companies.

Amazon later investigated its Amazon Web Services server farm operation in Beijing.[12] The engineers found the motherboards compromised, but the spy chips embedded in the motherboard were even smaller and more advanced. These chips were thin enough to imbed between layers of the fiberglass motherboard, making a visible discovery impossible. Amazon was reluctant to remove the equipment due to concerns about alerting the attackers. Instead, the team monitored the activity on the chips. There were occasional communication checks between the attackers and the equipment, but no extraction of data. The attackers were saving the backdoor access for a later opportunity. Amazon ended up selling the entire server infrastructure to a Beijing company to dump future risks associated with potential data compromise.

---

[11] Robertson and Riley, "China Used a Tiny Chip in a Hack That Infiltrated U.S. Companies."

[12] Ibid.

These are just a few examples of China's attempt to gain backdoor access to American networks. Governments routinely try to gain access to foreign countries' systems for intelligence purposes. These exploits against America appear to be caused by the Chinese government, so why is America focused on a Chinese company?

The Huawei corporate headquarters is located in Shenzhen, China. They sell products in both domestic and foreign markets. The C.E.O. and founder of Huawei, Ren Zhengfei, was previously an engineer in the PLA in the 1990s.[13] The company got its start with the Chinese army as one of its primary customers over 30 years ago. Both Cisco and T-Mobile sued Huawei for stealing their IP.

The Chinese government requires every Chinese private company to create a Chinese Communist Party (CCP) branch with direct ties and communication back to the party.[14] There is a National Intelligence Law on the books since 2017 that asserts Chinese companies must cooperate with Chinese national authorities when requested for intelligence-gathering. International experts have proclaimed that the CCP is strengthening its bonds with private companies with an emphasis on those companies that sell technology. These assessments point to strong ties between Huawei and the CCP.

Why is there suddenly such a push to stop Huawei from selling 5G telecommunications equipment, and what exactly is 5G? Huawei is the global leader when it comes to 5G equipment. Based on all the previous detail regarding Chinese

---

[13] Lindsay Maizland and Andrew Chatzky, "Huawei: China's Controversial Tech Giant," Council on Foreign Relations, last modified February 12, 2020, accessed March 3, 2020, https://www.cfr.org/backgrounder/huawei-chinas-controversial-tech-giant.

[14] Ibid.

efforts to access American networks and the close ties between Chinese companies and the CCP, many countries are concerned about the potential security implications of allowing Huawei equipment within sensitive networks.

Since the inception of smartphones, there has been a demand for fast mobile networks. Nokia released the first mass-produced cell phone in 1992, but it only supplied the basic phone features and text service.[15] The phone network technology of this era was the second generation and received the abbreviation of "2G," which provided digital signal access for the first time, along with rudimentary encryption and the ability to transmit small data packets at a rate of up to 40 kilobits per second.

In the early 2000s, smartphones released to the public included built-in web browsers for internet access on the go. Customers wanted the ability to do more with their phones. Around this same time, 3G networks began replacing existing 2G network equipment. 3G data transfer speeds were over four times faster than 2G data speeds.[16] For the first time, video streaming became a possibility for smartphone users on the go using mobile 3G networks. The end of the 3G era saw the initial launch of the iPhone in 2007. The iPhone introduced users to an application store, the ability to purchase movies and music online, and stream media content over mobile networks. High-speed internet demand was at an all-time high.

---

[15] Bainbridge, "From 1G to 5G: A Brief History of the Evolution of Mobile Standards," last modified December 1, 2018, accessed March 1, 2020, https://www.brainbridge.be/news/from-1g-to-5g-a-brief-history-of-the-evolution-of-mobile-standards.

[16] Ibid.

In 2009, the fourth generation of mobile telecommunications equipment deployed. 4G allowed for high-definition streaming of media and higher data transfer speeds. The emphasis on 4G networks also required customers to purchase new smartphones that supported 4G networks. The previous transition from 2G to 3G only required phone owners to swap out their sim-cards. 4G still has its downfalls. Connectivity and range issues still regularly occur, preventing access to mobile customers. There is also a small latency of 40-60 milliseconds that prevent real-time responses.[17] The majority of mobile phones and mobile telecommunication networks today use 4G technology.

Verizon was the first company to release the next-generation network technology in April of 2019. 5G again requires customers to purchase a new phone that supports the latest mobile technology.[18] The 2020 release cycle of new cellular phones will expand the market of 5G users.

What is the significant difference in 5G when compared to older technologies? The networks are faster, with far less latency, and most importantly, it will support "the internet of things" (IoT). IoT is the next big technological revolution. It will allow for billions of different devices to connect seamlessly and share data globally. Some examples of this include smart refrigerators, ovens, and lights. These kinds of devices reside in what is known as a smart home. A smart fridge could scan the food within and determine what provisions are low to warn the owner to purchase milk on their way

[17] Bainbridge, "From 1G to 5G: A Brief History of the Evolution of Mobile Standards."

[18] Ibid.

home. It could also share information with doctors to help determine the diet of a patient. Smart homes also allow homeowners to remotely modify the temperature of their home, determine whether the stove is still on, view suspicious activities via cameras, turn on lights, run a bath, etc.[19]

Around the globe, telecommunication companies want to integrate 5G technologies into their networks to provide their customer base with the latest technology. Only a few telecommunication technology manufacturers sell 5G equipment. Huawei is the global leader in 5G technologies. As seen below in FIGURE 1, Huawei leads the world in patents for 5G technologies with 1,554 registered patents, with Nokia close behind with 1,427 patents, and Samsung with 1,316.[20] The first American company to make the patent list is Qualcomm, with 846 patents.

[19] Bainbridge, "From 1G to 5G: A Brief History of the Evolution of Mobile Standards."

[20] Maizland and Chatzky, "Huawei: China's Controversial Tech Giant."

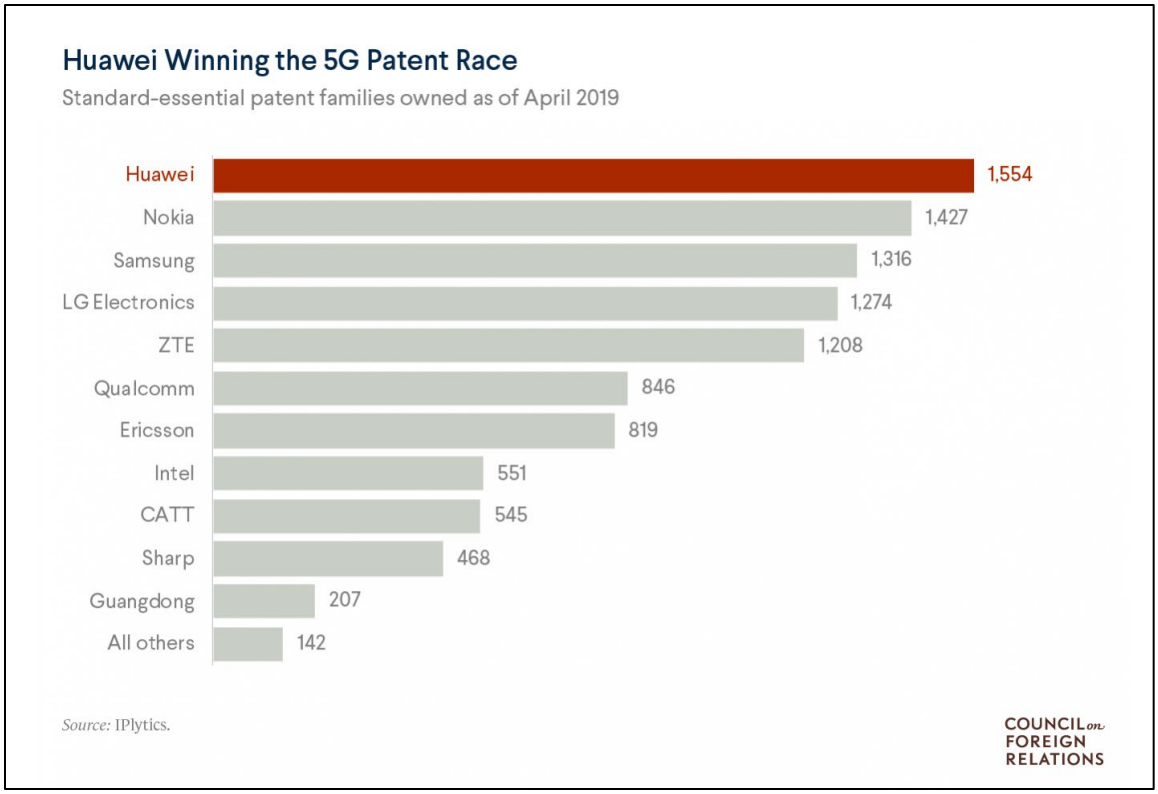

Figure 1. Huawei Winning the 5G Patent Race

Source: Lindsay Maizland and Andrew Chatzky, "Huawei: China's Controversial Tech Giant," Council on Foreign Relations, last modified February 12, 2020, accessed March 3, 2020, https://www.cfr.org/backgrounder/huawei-chinas-controversial-tech-giant/.

The purpose of this study is to demonstrate that President Trump's containment strategy to reduce the threat of Chinese unauthorized access to critical American networks was necessary and effective. The research will reveal what kind of threat Huawei telecommunication equipment poses on American and allied national security. Once identified, several approaches will undergo in-depth analysis to determine the best way forward for America to deal with the issue of China. National security is the utmost priority with all the recommended approaches presented in chapter 4.

Research Focus

This thesis will attempt to detail: The use of Chinese telecommunication and networking infrastructure, collectively referred to as 5G, represents a clear and menacing threat to the national security of America, its allies, and partners. Washington must thwart this advance. Secondary supporting questions include:

1. Why is Chinese technology a threat to national security?
2. Are there any historical examples of these threats?
3. How are countries handling their rollout of 5G?

Assumptions

These assumptions apply throughout the thesis:

1. China is pushing for further economic growth and power, potentially while exploiting other nation-states.
2. There is limited trust between the U.S. and Chinese governments.

Limitations and Scope

Information and data used to develop this thesis was limited to open-source material and will not dive into classified content whatsoever. The author's capability to write an advanced thesis of this magnitude is limited to guidance and instruction received while attending the Army Command and General Staff College (CGSC) and previous writing accomplished at the undergraduate level.

The scope of reading sources and content of the project is entirely open-source and will not tackle classified information of any type. The study will assess feasibility, suitability, and acceptability of recommended Courses Of Action (COAs) based off of the

international relations strategic stances of engagement, containment, and a blended solution of the two variants.

Significance of the Study

The research within this thesis will raise awareness about alternate solutions to handle foreign network equipment integration with consideration to national security threats and the acceptability by other nations and the World Trade Organization. President Trump's actions halted the danger for now, but is it the best way forward? The results could aid U.S. allies in developing their national strategies to deliver a unified international front. Additionally, these results could help U.S. companies determine the repercussions of partnering with Chinese companies.

CHAPTER 2

LITERATURE REVIEW

This study will focus on multiple sources of information regarding China throughout this chapter. The literature used throughout the research includes academic books, official government documents, professional peer-reviewed journals and publications, and reputable websites. Since many countries are still deciding whether to allow Chinese telecommunications equipment, web articles are used extensively because they offer the most recent developments regarding these decisions. The organization of the material first provides an overarching view of 5G technologies, and many of the top Chinese experts' opinions on China, then addresses the supporting questions of this thesis, which include:

1. Why is Chinese technology a threat to national security?
2. Are there any historical examples of these threats?
3. How are countries handling their rollout of 5G?

As briefly mentioned in chapter one, 5G is the fifth generation of telecommunications technology for cellular networks. The equipment is cutting-edge technology that allows for faster connections with less latency and allows for the envisioned future of IoT. Potentially billions of different devices will connect to simplify our lives. In the future's smart home, the lights, heating, media, air conditioning, and security systems are all accessible remotely while away from home. In the healthcare realm, the ability to remotely monitor the health of a patient and provide live data to a doctor will become a reality. This ability allows a patient to receive expert medical guidance without ever having to visit a doctor's office. Mobile health capabilities offered

through IoT can end up saving $305 billion by eliminating redundancies and other unnecessary expenses.[21]

5G networks will accommodate not only faster cell phone connectivity, but potentially a wealth of Personal Health Information (PHI) along with Personally Identifiable Information (PII) shared via mobile health capabilities or the IoT. Networks transmitting this type of content must be highly secure to protect from hacking and unauthorized backdoor stealth of valuable personal information.

According to Bill Gertz's book, *Deceiving the Sky: Inside Communist China's Drive for Global Supremacy*, China is researching IoT systems to find vulnerabilities. The Chinese government has the potential to exploit any found vulnerabilities. Imagine hackers having access to crash self-driving vehicles, feed false medical information to doctors, or dispense an overdose of medication to a patient. The author warns China is focusing its research on developing new cyberattack tools for surveillance and military reconnaissance purposes.[22]

Michael Pillsbury is one of the leading theorists on Chinese strategy. He is currently the Director of Chinese strategy for the Hudson Institute. President Trump recognized him as one of the primary authorities regarding China. He previously worked

---

[21] Corey Stern, "Goldman Sachs Says a Digital Healthcare Revolution Is Coming — and It Could Save America $300 Billion," *Business Insider*, last modified June 29, 2015, accessed March 20, 2020, https://www.businessinsider.com/goldman-digital-healthcare-is-coming-2015-6.

[22] Bill Gertz, *Deceiving the Sky: Inside Communist China's Drive for Global Supremacy*, (New York, NY: Encounter Books, 2019), chap. 11.

for the defense department and the senate.[23] In his career as an author, he has written three books with China as the subject.

In the book *The Hundred-Year Marathon: China's Secret Strategy to Replace America as the Global Superpower,* by Michael Pillsbury, the author holds a very untrusting view of China and its openness regarding their real aspirations.[24] The author postulates that Sun Tzu's writings are the basis for today's Chinese strategy. Sun Tzu famously states that an enemy must be kept complacent, while never inciting a stronger opponent, and true intentions must be concealed until powerful enough to surprise an enemy.[25] Another critical principle the author covers of Sun Tzu is that if an opponent is superior, steal their ideas and technology.[26] China has been very successful with this strategy and has stolen billions of dollars of U.S. trade secrets through insiders, bribes, and cyber-theft. Pillsbury concludes his book by stressing that the most crucial first step for America to take is to recognize the moves that China is making to surpass our economy before it is too late.[27]

In Graham Allison's book, *Destined for War: Can America and China Escape Thucydides' Trap,* the author references the Peloponnesian war between Athens and

---

[23] Michael Pillsbury, "Michael Pillsbury," michaelpillsbury.net.

[24] Michael Pillsbury, *The Hundred-Year Marathon: China's Secret Strategy to Replace America as the Global Superpower* (New York, NY: Henry Holt and Company, LLC, 2015).

[25] Ibid., 35.

[26] Ibid.

[27] Ibid., 235.

Sparta. This historical war is his baseline for what could happen similarly between China and the U.S. as Americans feel threatened by China's sudden global rise.[28] He declares that war is not inevitable between the two nations.[29] The author recognizes that China does play unfairly in the global markets, and open engagement may not lead to the perfect solution for both countries.

Throughout the book, the author reviews sixteen cases regarding the relationships between superpowers. Twelve of these cases conclude in war. The author makes a comparison of the current US-China situation to that of Great Britain and Germany before the buildup of World War I.[30]

Allison claims that the United States must change their perceptions regarding China's rise to avoid war, which there are several ways to accomplish. But first, recognition that the American strategy towards China that has been in place since the Cold war is conflicted.[31] Both the Department of State and Treasury follow a policy of engagement with China while overlooking unfair Chinese practices. The Department of

---

[28] Graham Allison, *Destined for War: Can America and China Escape Thucydides's Trap?* (Boston, MA: Houghton Mifflin Harcourt, 2017), 26, accessed February 15, 2020, https://www.amazon.com/Destined-War-America-Escape-Thucydidess/dp/1328915387/ref=sr_1_1?keywords=destined+for+war&qid=1581800692&sr=8-1.

[29] James Cricks, review of *Destined for War: Can America and China Escape Thucydides's Trap?* by Graham Allison (Washington, DC: National Defense University Press, 2017), https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-87/jfq-87_101-102_Cricks.pdf.

[30] Ibid.

[31] Allison, *Destined for War: Can America and China Escape Thucydides's Trap?*, 132.

Defense takes a hedging strategy with China that seeks to strengthen military presence in Asia with countries that surround China while planning for a worst-case scenario that China becomes the next Germany before the world wars.[32] It's a conflicted good-cop / bad-cop scenario.

Considerations for this archaic strategy are necessary. One possibility is accommodation. America must ultimately recognize the rise of China as a superpower and agree to make the best of the situation while avoiding military conflict.[33] An example of this is how Britain accepted America's rise during the late 19th century to prevent further conflict.[34] Today, they are considered close allies. This example, of course, is a best-case scenario. Historically, this failed with the Yalta agreement, where Stalin agreed to allow elections in his country in exchange for a favorable border agreement post-WWII. Stalin dishonored the deal in the end.[35]

The author supplies another strategy to undermine China from within. There is a myriad of weaknesses in the Chinese armor that are ripe for exploitation. A campaign to reveal the historic fraud associated with Communism could disrupt their government's stability. Another choice is to demonstrate the advantages of democracies while using Taiwan and Hong Kong as successful case studies before further Chinese meddling.[36]

---

[32] Allison, *Destined for War: Can America and China Escape Thucydides's Trap?*, 133.

[33] Ibid., 134.

[34] Ibid.

[35] Ibid.

[36] Ibid., 135.

America could encourage dissent in China. There are many young, open-minded Chinese that come to America to study that receive visibility to the freedoms and human rights standards in America that could be the foundation for dissent once returning to China. Also, for consideration are the pockets of existing resistance to Chinese rule in Tibet, Xinjiang, Taiwan, and Hong Kong that could oppose China's efforts to absorb them. If America could somehow disrupt the stability of the Chinese government and have them focus on internal security and stability, it could delay or weaken China's efforts to oppose America.[37] China, however, has already gone a long way in minimizing some of these threats by developing the Great Firewall of China that extensively censors and blocks access to information that challenges the Chinese narrative.

Negotiating for long-term peace is another consideration. With American and China coming to an impasse where each side cannot accept the other's terms, they can negotiate agreements to slow development in areas that are highly debatable so each country can refocus on other areas.[38] As an example, the states could agree to limit cyberattacks or restrict interference in each country's politics. The U.S. could limit their criticism of the extensive violations of human rights in China in exchange for China to halt its efforts of stealing industrial secrets from America.[39] Agreements such as this allow each country to focus its financing in other areas instead of pouring billions of

[37] Allison, *Destined for War: Can America and China Escape Thucydides's Trap?*, 135.

[38] Ibid., 136.

[39] Ibid.

dollars into efforts to outdo their opposition's developments. This type of negotiation makes sense as tension grows between the two countries.

Another possible option is for China and the U.S. to strengthen their relationship.[40] Several global issues need strong partnerships between world leaders to address. Some of these include global warming, terrorism, and global epidemics such as SARS and the recent Coronavirus that both originated in China. The U.S. and China could lead the charge to improve these conditions through partnerships that build trust and relationships between the two countries as they focus on unified tasks.[41]

Allison closes out his book by concluding that each country needs to focus on their domestic issues as the priority to build the realization that many of these internal issues are truly global, and cooperation is vital to make progress while also improving relationships.[42]

Why is Chinese technology a threat to national security?

According to *the Investigative Report on the U.S. National Security issues posed by Chinese Telecommunications Companies Huawei and ZTE*, by Chairman Mike Rogers and Dutch Ruppersberger to the U.S. House of Representatives in 2012, spokespersons for both companies were evasive when questioned regarding their relationship with the

[40] Allison, *Destined for War: Can America and China Escape Thucydides's Trap?*, 137.

[41] Ibid., 138.

[42] Ibid., 143.

CCP.[43] The Chinese government requires every Chinese private company to create a CCP branch with direct ties and communication back to the party.[44] There is a National Intelligence Law on the books since 2017 that asserts Chinese companies must cooperate with Chinese national authorities when requested for intelligence-gathering. International experts have proclaimed that the CCP is strengthening its bonds with private companies with an emphasis on those companies that sell technology. These assessments point to strong ties between Huawei and the CCP.

The Trilateral Cyber Security Commission authored a report in December 2019 regarding the recommendations for the U.S. and Japan on meeting the challenges of 5G. The primary concern for 5G infrastructure the commission discusses is quite like the U.S. House of Representatives report above. Huawei obtains state-sponsored subsidies from the Chinese government (a violation of the WTO). The company has a close relationship with Chinese government leadership. There is also the Chinese National Intelligence law, which forces Chinese companies to work with state intelligence agencies that could lead to companies opening back doors. The report also stresses that 5G infrastructure must be secure to minimize exploitation by malevolent aggressors. The multiple vulnerabilities found in Huawei equipment, intentional or not, historically do not receive patches quickly by the company.[45]

---

[43] Rogers and Ruppersberger, *Investigative Report on the U.S. National Security Issues Posed by Telecommunication Companies Huawei and ZTE*, 10.

[44] Maizland and Chatzky, "Huawei: China's Controversial Tech Giant."

[45] Trilateral Cyber Security Commission, "National Security Strategy For 5G: Findings & Recommendations on Meeting the 5G Challenge," Trilateral Cyber Security

In Kimberly Orinx's publication*, A Chinese Fox against an American Hedgehog in Cyberspace*, the author discusses how President Trump reinterpreted the U.S. National Security Strategy (NSS) with a new focus on using hard power when dealing with China and other global powers.[46] She believes that these tactics will only work in the short-term and that other tactics are necessary to influence over the long run, such as socialization and persuasion.[47] The paper proclaims the best way to beat your rival is by depriving them of their freedom of movement. When an opponent's global environment is shaped, their decline is all but ensured, along with your nation's growth.[48] China understands how to shape its opponents very effectively. One method used is cyberattacks to exploit its enemies. China can use its cyber capabilities to disrupt critical infrastructure in America.[49] China extensively uses its cyber capabilities to exploit information, whereas America uses cyber primarily in a defensive nature.

The Chinese perspective of war goes beyond the use of military forces and expands into the recognition and control of politics, technological, social, and economic trends.[50] This perspective is considered information operations, which again, America

---

Mission, December 2019, 14, https://spfusa.org/wp-content/uploads/2019/12/TCSC-National-Security-Strategy-for-5G-Dec-2019.pdf.

[46] Kimberly Orinx and Tanguy Struye de Swielande, "A Chinese Fox against an American Hedgehog in Cyberspace?," *Military Review* (2019): 1.

[47] Ibid.

[48] Ibid., 59.

[49] Ibid.

[50] Ibid., 60.

recognizes primarily as a wartime activity. China continuously controls and manages the flow of information and propaganda within its country to support its narrative and minimize domestic threats. China also reduces the external influence of its citizens with its great firewall, which minimizes informational "pollutants."[51] Beijing holds an annual World Internet Conference that promotes China's digital authoritarian views as an alternative to the liberal model that is the norm for the majority of the world. Other countries implementing the Chinese model could eliminate opposing views, rebellion, and internal strife.[52] To close her paper, the author recommends pushing an open internet with its allies and America changing its lens to include cyber power in their peacetime strategy.[53] This publication falls in the category of congagement because it focuses on changes needed internally in America, not how the U.S. deals with China.

Theodore H. Moran, the Marcus Wallenberg Chair at the School of Foreign Service at Georgetown University, authored several books on the topics of globalization, foreign investments, and international risk management. From 1993-1994, he was also a senior advisor of economics for the Department of State. In his publication, *Three Threats: An Analytical Framework for the CFIUS Process*, the author discusses three

[51] Orinx and de Swielande, "A Chinese Fox against an American Hedgehog in Cyberspace?," 63.

[52] Ibid., 64.

[53] Ibid., 65.

areas of concern for the Committee on Foreign Investment in the United States (CFIUS).[54]

The first threat is the possibility that foreign acquisition of a U.S. company could make America reliant on vital goods or services that undergo intentional delays or denial. Foreign manipulation could severely impact essential American operations. During Operation Desert Shield, the U.S. military required essential electronics for search and rescue operations. Of these parts, several came from foreign suppliers.[55] While there was no detection of foul play, the potential was there to affect vital military actions.

The next threat that Moran discusses is the threat of a foreign acquisition leaking technological capabilities to its government. An international company in this situation suddenly gains access to technology and expertise that could be shared. Not only that, but any vulnerabilities found have the potential for sharing and exploitation by the foreign government. One example of this is the Chinese company Lenovo's acquisition of IBM's laptop sector. His study shows evidence that Chinese investment in IBM bolstered the capabilities and effectiveness of other companies in China.[56]

Moran exclaims the last threat is a foreign acquisition that leads to the infiltration of critical services that are vital to the U.S. economy. If an international company was able to buy a key network provider such as AT&T or a network equipment provider such

---

[54] Theodore Moran, *Three Threats: An Analytical Framework for the CFIUS Process* (Washington, DC: Peterson Institute for International Economics, 2009).

[55] Ibid., 11.

[56] Ibid., 18.

as Cisco, the threat to national security could have substantial implications.[57] This threat directly ties to the potential danger of integrating Chinese 5G equipment.

A notable example Moran provides that hits on all three of the threats is the proposed acquisition of 3Com by Bain with a 16.5% minority holding of Huawei. 3Com produces a variety of different network-related products, including network switches, network cards for computers, routers, Wi-Fi equipment, and network security software solutions such as TippingPoint. Under this proposition, three of the eleven board members are hand-picked by Huawei.

With the myriad of various products that 3Com offers, it presents the full trifecta of threats. For threat I, denial of access, China can block exports to other countries. The proposed deal provides Chinese ownership with a minority stake, but most of 3Com products are assembled in China by Huawei-owned H3C. The Chinese government has the potential to dictate the shipping of 3Com manufactured products to the U.S. in a future foreign policy standoff.[58]

Threat II, leakage of sensitive technology, offers the opportunity for the Chinese government to freely access American IP and share its findings with other Chinese companies. While most of the products 3Com produces offer a tremendous deal of groundbreaking advancements, their integrated security and intrusion detection software, TippingPoint, does.[59] The Chinese government does stand to take advantage of learning

---

[57] Moran, *Three Threats: An Analytical Framework for the CFIUS Process,* 23.

[58] Ibid., 26.

[59] Ibid., 27.

more about this software and either integrating its capabilities into similar Chinese software to assist in bringing Chinese software firms up to peer status or in finding vulnerabilities in the software code.

Sabotage and espionage are the third threat that Moran discusses. U.S. government and military agencies extensively use TippingPoint for network intrusion security and threat reduction purposes. With China having access to the source code, there is potential for the insertion of a backdoor for surveillance or sabotage of essential American services.[60] This capability for CCP to know of vulnerabilities for exploitation and the possibility to access military networks is a considerable threat.

Fortunately, this acquisition never occurred. The leading company that wanted to purchase 3Com withdrew its proposal in 2008.[61] It did, however, offer security analysts an excellent opportunity to discuss the potential threats from Chinese ownership of American companies.

China previously attempted to build partnerships and acquire American telecommunication companies. China tried to purchase Lattice Semiconductor in 2017. In 2018, a company from Singapore with strong ties to China attempted to buy Qualcomm in a hostile takeover. The CFIUS prevented these sales from occurring.[62] The potential is

---

[60] Moran, *Three Threats: An Analytical Framework for the CFIUS Process*, 28.

[61] Ibid.

[62] The Economist, "Security Alert - CFIUS Intervenes in Broadcom's Attempt to Buy Qualcomm," last modified March 8, 2018, accessed March 11, 2020, https://www.economist.com/business/2018/03/08/cfius-intervenes-in-broadcoms-attempt-to-buy-qualcomm.

there for intentional backdoors into products from American companies if key stakeholders have ties to the CCP.

Erica Borghad works at the Army Cyber Institute of West Point as an Assistant Professor. She authored an article published on the Council of Foreign Relations website discussing the threat of 5G at the government and military level. 5G is a modern technology that has massive implications for the future of warfare. Outside of the apparent improvements in communications, 5G also enhances the real-time capabilities of robotics and artificial intelligence. In areas such as Africa and parts of Europe, Huawei's telecommunication equipment has already begun expansion into those markets. In a future battlefield environment where military assets have a significant reliance on 5G to operate, the telecommunication infrastructure must be trusted and reliable. With the close relationship previously mentioned between Chinese companies and their government, it is feasible to consider the Chinese government leveraging native telecommunication equipment to capture or block essential military communications.[63]

Considering the last major war fought on American soil was the civil war in 1865, there is a strong chance that future conflicts will occur in foreign locations with established Chinese telecommunication equipment. This threat has enormous implications for the future of warfare and could give our enemy an asymmetric advantage. Many experts predict that the future of war will rely less on soldiers to

[63] Erica Borghard and Shawn Lonergan, "The Overlooked Military Implications of the 5G Debate," Council on Foreign Relations, last modified April 25, 2019, accessed March 11, 2020, https://www.cfr.org/blog/overlooked-military-implications-5g-debate.

perform the fighting and more on autonomous drones.[64] Real-time networking is critical for communication needed for these systems to ensure precision, accuracy, and timeliness.

John P. Carlin served as the U.S. Assistant Attorney General for the National Security Division and served as Chief of Staff at the FBI under Robert Mueller. His book, *Dawn of the Code War*, provides substantial insight into the threat of China. America's national security goes far beyond the realm of the Federal Government and military networks. Defense contracting companies, while having close ties to federal and military governments, develop sensitive government products on company networks that routinely connect to the public internet. Whenever a networked computer connects to the open web, the threat of exploitation and theft increases significantly.[65]

Today's critical infrastructure in America now relies on transmission through telecommunication equipment. These include power grids, natural gas, oil, water systems, banking, and financial systems.[66] All of these rely upon electronic structures that connect through the internet, which significantly increases remote threats. If back

---

[64] Sydney J. Freedberg Jr., "Elon Musk: 'Radical Innovation' Needed To Beat China Militarily," *Breaking Defense*, last modified February 28, 2020, accessed March 11, 2020, https://breakingdefense.com/2020/02/elon-musk-radical-innovation-needed-to-beat-china-militarily/.

[65] John Carlin and Garrett Graff, *Dawn of the Code: America's Battle Against Russia, China, and the Rising Global Cyber Threat* (New York, NY: Hachette Book Group, 2018), chap. 5.

[66] Rogers and Ruppersberger, *Investigative Report on the U.S. National Security Issues Posed by Telecommunication Companies Huawei and ZTE*, 1.

doors exist in telecommunication equipment, ease of exploitation and havoc on critical infrastructures can occur.

The Office of the Secretary of Defense's Annual Report to Congress in 2019 shows concern for the growing Chinese might. The report stresses that China is quickly growing its military power and becoming a concern in the Pacific.[67] Their Made in China 2025 plan pushes for increased reliance on domestically produced technology. After the backlash from the contents of this report, China relaxed its language regarding its goals.[68] Most significantly, the paper notes that Chinese leaders are now using the elements of Diplomatic, Information, Military, Economic to influence and achieve objectives.

Michael Maloof is a former security policy analyst from the Office of the Secretary of Defense with 30 years of federal service in the DoD, where he worked as the director of technology and security operations involving national security concerns. His article states that the Chinese government has widespread access to nearly 80 percent of global internet traffic. He says cooperation of the companies Huawei and ZTE provides this clandestine access. These companies purposefully supply backdoors to their equipment. The two companies combined have network equipment installed in 140 countries. Maloof states that the only safeguard is military-grade encryption, but Chinese hackers continuously try to decrypt valuable encrypted content. The author also says any U.S. company that works with a foreign company connected to Huawei equipment

---

[67] Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments involving the People's Republic of China 2019* (U.S. Department of Defense), i, accessed October 19, 2019, https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf.

[68] Ibid.

potentially has all their communication compromised, including allied nations such as Great Britain, Mexico, and South Korea. Chinese telecommunication is incredibly attractive to many countries because of its advanced technology and low costs. Both companies receive subsidized deals from Chinese banks, which do not request payment for years, under the guidance of the Chinese government.[69]

The threats discussed above are just some of the potential ways in which our enemies could exploit America and its allies. To show these vulnerabilities not only exist but are frequently exploited, it is best to provide details regarding actual cases of Chinese hacking and stealth efforts.

Are there any historical examples of these threats?

In the book *Dawn of the Code*, Carlin discusses the massive jump China took from being a 19th-century agricultural economy to a 21st-century technological leader in the mere span of two generations. General Alexander, former head of the National Security Agency and U.S. Cyber Command, calls China's actions "the greatest transfer of wealth in history."[70] The book estimates that the loss to American business is approximately $250 billion annually. On top of the loss from sales and company stock market value, this cybertheft calculates a loss of roughly 200,000 jobs each year.

[69] Michael Maloof, "China: 'Pervasive Access' to 80% of Telecoms," *WND*, last modified July 1, 2012, https://www.wnd.com/2012/07/chinese-have-pervasive-access-to-80-of-worlds-telecoms/.

[70] Carlin and Graff, *Dawn of the Code: America's Battle Against Russia, China, and the Rising Global Cyber Threat*, chap. 2.

Carl Roper, author of the book *Trade Secret Theft, Industrial Espionage, and the China Threat*, worked for the U.S. government as a security specialist for the Department of Defense Security Institute (DODSI) and is known for developing the DODSI risk management course. He is also a retired U.S. Army Counterintelligence special agent.[71] Roper's book focuses on China's rise over the past five decades and how it evolved from a peasant nation to today's booming country with comparable educational standards and a military more massive than the entirety of Europe's. This transformation did not just happen overnight. China took extensive shortcuts to advance the development of the country in such a brief period. This progression occurred primarily through the targeted stealth of American IP.

In a congressional research service report to congress updated in 2006, a U.S. representative of the Intelligence community reported that an internal damage assessment determined China obtained classified U.S. nuclear weapons program information to aid in advancing its program. The information stolen included data regarding various nuclear-capable vehicles and the Trident II submarine that can launch atomic warheads.[72] China jumped ahead in its efforts to become a near-peer adversary.

In 1996, FBI Director Luis Freeh warned that the U.S. high-tech sector is the primary focus for information gathering by the Chinese. These targets include semiconductors, defense technology, energy knowledge, and, most importantly, to this thesis, telecommunications equipment, and the technology behind it that the National

---

[71] Carl Roper, *Trade Secret Theft, Industrial Espionage, and the China Threat* (Boca Raton, FL: CRC Press, 2014), xi.

[72] Ibid., 1.

Information Infrastructure runs on. Freeh also states that products from these sectors directly tie into classified government products, dual-use technology in use in both the public and government sectors, and the primary focus of American research and development. Successful theft in these areas could affect both American international competitiveness and national security.[73]

A huge concern, according to Roper, is the fact that China has its own independent rules about patents that do not align with international patent standards. China has a "first to patent" law, which does not account for other global patents. This rule gives Chinese companies the initiative to seek out foreign company's IP, make minor modifications to it, then patent it in China with zero repercussions. That is why it is not surprising to see Chinese products on the market shortly after successful products hit the market, but at a much lower price point because of Chinese companies' ability to forego research and development and ignore international standards.[74]

The Alliance for American Manufacturing provided a case for Roper's book regarding a Chinese tire manufacturer that bribed Goodyear employees to enter their facilities and take photos of proprietary processes. The Chinese company would have benefited from not having to invest the time and resources into the research and development. Within years, Goodyear could have faced layoffs as sales decreased from cheaper Chinese products that were identical to their own but sold for far less. Government authorities arrested the Chinese spies before they could transfer the

---

[73] Roper, *Trade Secret Theft, Industrial Espionage, and the China Threat*, 4.

[74] Ibid., 6.

information back to China. Roper stresses that when Chinese spies are caught, there are never any direct links back to the Chinese government.[75]

In February of 2013, President Obama's administration released a report titled *The Administration Strategy on Mitigating the Theft of Trade Secrets*. In the statement, it highlighted several large-scale occurrences of trade secret theft. The report offered a total of nineteen separate reports of IP theft. Of the nineteen, sixteen pointed to Chinese involvement.[76]

Bill Gertz is a writer and columnist for the Washington Times. He authored several books over the past two decades on the topic of China. In his book *Deceiving the Sky: Inside Communist China's Drive for Global Supremacy*, the author covers several of China's successful attempts to steal vital American secrets to accelerate its military technological capabilities. Much of China's efforts were shrouded in mystery until Donald Trump became President in 2016 when the national strategy transitioned from engaging with China to the containment of China. A public report from the U.S. Trade Representative (USTR) Office divulged details of Chinese espionage.[77]

In 2009, Su Bin, a Chinese and Canadian dual-citizen, coordinated with two PLA officers to identify key employees working for Boeing on the C-17 program. The Chinese hacker team sent malicious emails that installed hacking software through phishing attacks. The hackers extracted 85,000 files on the C-17. The C-17 took over a decade to

---

[75] Roper, *Trade Secret Theft, Industrial Espionage, and the China Threat,* 6.

[76] Ibid., 31.

[77] Gertz, *Deceiving the Sky: Inside Communist China's Drive for Global Supremacy*, chap. 6.

develop and cost more than $40 billion to the American taxpayers. The successful theft of American technology cost the Chinese government less than a million dollars to obtain, saved them decades of research and development, and billions of dollars. Within a decade, China released the Xian Y-20 transport jet, which looks like a near clone of the American C-17.[78]

During the prosecution of Su Bin, the court documents also revealed China successfully stole F-35 fighter secrets from Lockheed Martin. China used the information to build their J-20 fighter. Side by side, the two jets look surprisingly similar.[79]

According to Carlin's book, *Dawn of the Code War*, a sizable portion of government agencies were victims of hacks. The House and Senate both were casualties of data leaks. In 2006, the Department of Commerce had data of 26,000 of its employees hacked. The Department of Defense had information regarding its most prized weapon systems stolen. Hackers accessed the Department of Energy networks and extracted data regarding nuclear techniques. NASA announced in 2012 that Jet Propulsion Laboratory was hacked by Chinese hackers that had full root access to their systems.[80] These breaches were significant, but just small potatoes compared to China's attack on the Office of Personnel Management (OPM).

---

[78] Gertz, *Deceiving the Sky: Inside Communist China's Drive for Global Supremacy*, chap. 6.

[79] Ibid.

[80] Carlin and Graff, *Dawn of the Code: America's Battle Against Russia, China, and the Rising Global Cyber Threat*, chap. 3.

Carlin has a full chapter devoted to the successful exploitation of the Office of Personnel Management in his book. An I.T. contractor working for OPM found copious amounts of suspicious encrypted traffic exiting the OPM network with a destination of opmsecurity.org. The domain name appeared to belong to OPM. Fortunately, the contractor, recognized the domain was not an official OPM website. He ran a malware detection tool to identify spyware on the OPM networks. Upon further investigation, the hackers had access to the systems for over a year. The group was compressing sensitive files, then encrypting them to bypass the network monitoring tools on the networks to get the content out to their domain for collection. Once the investigation was complete, the findings identified malware that allowed for gathering keystrokes, the ability to access computer cameras and microphones, and root access of infected systems that spread to every computer on the network. The spies had keys to access any doorway in the kingdom. The experts were able to trace the files and the network infrastructure back to a Chinese cybersecurity company, Topsec, which received half of its funding from the PLA.[81]

The OPM cyber experts planned to remove the enemy's access in quick succession. They changed all the administrative account passwords and took the systems offline while they eliminated all the malware. The OPM team felt confident that they removed the external threat. The Chinese hackers found another way into the system through a government contractor's credentials. Two-factor authentication was a recommended security solution to tighten security, but OPM still did not implement the

[81] Carlin and Graff, *Dawn of the Code: America's Battle Against Russia, China, and the Rising Global Cyber Threat*, chap. 8.

recommendations in time. The hackers, knowing they had limited time, moved quickly to extract the most treasured information. The result was the theft of millions of military and government employee personal data. This crime included names, addresses, health insurance information, pay statements, social security numbers, and service of veterans.[82]

Along with this personal data, the hackers also extracted 5.6 million fingerprints and the SF-86 forms used to obtain security clearances. These documents included family members and connections to foreign officials. It was a real treasure trove of data for the Chinese intelligence community to sift through to identify anyone associated with the U.S. government and find ways to exploit.[83]

Not only were government agencies at risk, but also commercial ones as well. In 2015, the health care company Anthem suffered a massive data breach. The content pilfered included the personal details for over 78 million patients, including their names, email addresses, Social Security numbers, dates of birth, and household income. Anthem was at fault for not encrypting its customer database. If the hackers desired financial gain, each record could retrieve around $40 on the dark web. While proof was never significant enough to pinpoint the blame on China, none of the files taken from the hack ever appeared online. That points to the hackers having a different intended purpose for the patient data. Bloomberg reported that Chinese hackers were the root of the attacks and intended to use the data to find information regarding the personal lives of government employees and defense contractors. Coupled with the OPM hack mentioned above, the

---

[82] Carlin and Graff, *Dawn of the Code: America's Battle Against Russia, China, and the Rising Global Cyber Threat*, chap. 8.

[83] Ibid.

Chinese government had more information regarding American government personnel than most U.S. employers could access.[84]

Chris Demchak published a paper for the U.S. Naval War College regarding Chinese exploitation of North American networks. In his paper, he discusses how China Telecom has ten internet Point of Presence (PoPs) since the early 2000s. Eight of the PoPs exist in America and two in Canada. Following the 2015 agreement between President Obama and Xi Xing Ping, hacking efforts from the two countries appeared to diminish the threat to each nation's security successfully. After the agreement, the author found an increase in network traffic redirected to China before reaching its ultimate destination. These man-in-the-middle attacks resulted in over six months of network traffic between Canada to Korean government websites stopping in China first before arriving at the recipient in 2016. Network protocols regularly route traffic to the shortest and fastest network distances using Border Gateway Protocol (BGP). BGP hijacks effectively route traffic through designated locations that delay transmissions. Traffic routed through China could be reproduced for hackers to later decrypt and read with no red flags set off from intrusion detection systems. That same year, web traffic from America to banks in Milan, Italy, also became rerouted to China. The author also notes that China does not reciprocate whatsoever. Although China has PoPs throughout North America, there are no allied PoPs in China.[85]

---

[84] Carlin and Graff, *Dawn of the Code: America's Battle Against Russia, China, and the Rising Global Cyber Threat*, chap. 8.

[85] Chris Demchak and Yuval Shavitt, "China's Maxim - Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking," Scholar Commons,

Today, Huawei is expanding its telecommunication market by aiding foreign countries in setting up its 5G network infrastructure. A recent Reuters news report covers the arrest of two individuals in Poland arrested on spying charges. One of the individuals arrested was a former Polish security official, and the other was an employee of Huawei. While the details of the arrests are classified, Norway was considering joining the other western nations in their ban on Chinese equipment on their 5G backbones. Huawei quickly attempted to separate themselves from the incident by firing the employee and stating that they did not support the employee's actions in any way.[86] The U.S. signed a pact with the Polish Government to increase American military presence in the country a few months before the arrests occurred.[87] Could there be a tie between the two events?

In Gertz's book *Deceiving the Sky: Inside Communist China's Drive for Global Supremacy*, the author supplies an entire chapter that covers the threat of Huawei. Within the chapter, Mosher, the President of the Population Research unit, states that Huawei is not a commercial company; they are an arm of the CCP. He compares Huawei with the Chinese Government to Alfried Krupp, the German steelmaker, and his relationship with the German government. Mosher states that the German steel company was an arm of the

---

2018, 4–8, https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1050&context=mca.

[86] Joanna Plucinska, Karol Witenberg, and Jack Stubbs, "Poland Arrest Huawei Employee, Polish Man on Spying Allegations," *Reuters*, last modified January 11, 2020, accessed March 12, 2020, https://www.reuters.com/article/us-poland-security/poland-arrests-huawei-employoee-polish-man-on-spying-allegations-idUSKCN1P50RN.

[87] Jaroslaw Adamowski, "US, Polish Presidents Sign Pact to Boost American Military Presence in Poland," *DefenseNews*, last modified September 24, 2019, https://www.defensenews.com/global/europe/2019/09/24/us-polish-presidents-sign-pact-to-boost-american-military-presence-in-poland.

Nazi machine, just as Huawei is a champion of China's plan to dominate the global communications market.[88]

China's recently enacted National Intelligence laws that force companies to cooperate with the government, as necessary. The fact that the Chinese government requests for user data through Chinese telecommunications providers, such as Huawei and ZTE domestically, should be a concern for countries accepting equipment from these companies. There is a strong possibility these same access points exist on Huawei telecommunications gear installed outside of China.[89]

In 2015, T-Mobile sued Huawei for economic espionage. Huawei engineers visited a T-Mobile lab and covertly took photos of proprietary equipment that T-Mobile engineers used to stress-test new equipment. One of the Huawei engineers even took one of the electronic "fingers" used in testing the equipment. Huawei responded to the allegations by stating their employees went rogue and stole T-Mobile's information on their own.[90] Investigators revealed emails between the Huawei employees and their company, where Huawei encouraged the stealth of valuable knowledge and even provided bonuses to employees based on the overall value of the stolen information. Huawei intended to obtain information illegally to improve its internal operations and technological capabilities.[91]

---

[88] Gertz, *Deceiving the Sky: Inside Communist China's Drive for Global Supremacy*, chap. 11.

[89] Ibid.

[90] Ibid.

[91] Roger Cheng, "Huawei's Legal Troubles Take a Twist with T-Mobile's Torture-Test Robot," *CNET*, last modified January 29, 2019, accessed March 21, 2020,

In a recent Wired.com article by Jon Fingas, the author discusses a new effort by China and Huawei to make foundational changes to the way the internet works. The changes push a new network protocol that is more efficient than existing TCP/IP standards but also provides added measures for centralized control. One of the command options allows for disabling a section of a network or a single connection, which worries civil liberties advocates, as it could be used by an authoritarian regime to censor freedom of speech. Experts are also concerned about the potential to require individuals to authenticate to use the internet, which links people directly to their internet connections and allows governments to track names instead of IP addresses.[92]

The Trilateral Cyber Security Commission's NSS provides several instances of the unfair practices of Huawei. In 2003, Huawei confessed in a U.S. court of stealing Cisco router code for use in its products. Instead of building its code, Huawei simply copied a competitor's. In 2007, a Chinese engineer for Motorola was apprehended at O'Hare airport with a briefcase full of sensitive Motorola documents, a hefty sum of cash, and a 1-way ticket to Beijing. The engineer had plans to join Huawei upon arrival in China. In 2018, the Department of Justice indicted Huawei for selling sanctioned goods to Iran. America accuses Huawei of lying about its lenders and acting as an intermediary for the

---

https://www.cnet.com/news/how-a-torture-test-robot-figures-into-the-legal-assault-on-huawei/.

[92] Jon Fingas, "China, Huawei Propose Internet Protocol with a Built-in Killswitch," *Engadget*, accessed March 30, 2020, https://www.engadget.com/2020-03-30-china-huawei-new-ip-proposal.html.

purchase of U.S. goods for Iran. In 2019, the Department of Justice indicted a Chinese professor from Texas University for stealing IP secrets for Huawei.[93]

Guo Wegui is an exiled Chinese billionaire. He holds a tremendous amount of knowledge about the internal processes of the Chinese system. Guo warns that Huawei poses as a commercial business but is controlled by a branch of the CCP within China led by Jiang Zemin, a former Party General Secretary. In this relationship, Huawei works directly with the Ministry of State Security and Chinese Military Intelligence.[94]

As revealed above, Huawei has historical ties to the Chinese government. Not only that, China successfully infiltrated secure American networks multiple times in the past to advance its technological capabilities by simply stealing American IP. Huawei's behavior reveals that the company does not object to illegal actions to gain a competitive advantage. Trump's actions appear sensible based on the evidence.

How are countries handling their rollout of 5G?

Under a policy of engagement, several countries agreed to install Chinese telecommunication technology in their efforts to upgrade their infrastructure to support 5G. The United Kingdom, France, Belgium, New Zealand, Germany, and the European Union (EU) all support Chinese 5G equipment, but with constraints due to the questionable relationships of Chinese companies with their government, and America's efforts to warn countries against installing high-risk equipment.

---

[93] Trilateral Cyber Security Commission, "National Security Strategy For 5G: Findings & Recommendations on Meeting the 5G Challenge," 12–13.

[94] Gertz, *Deceiving the Sky: Inside Communist China's Drive for Global Supremacy,* chap. 11.

The United Kingdom recently decided to accept Huawei telecommunication equipment on its networks. However, there are limitations to the extent of Huawei integration as part of the U.K.'s risk mitigation strategy. All networks in the U.K. have a limit of 35 percent of the network equipment coming from HRV, which includes Huawei. The U.K.'s core Critical National Infrastructure and its sensitive military networks do not authorize Huawei equipment use. Additionally, the U.K. cannot purchase network analytic equipment, authentication systems, and data management systems from HRVs whatsoever. The U.K.'s National Cyber Security Center (NCSC) was vital in supplying information to the Prime Minister to aid in his decision.[95]

The U.K.'s NCSC performed a thorough evaluation and published annual reports regarding their work with Huawei. Huawei launched the Huawei Cyber Security Evaluation Center (HCSEC) in England with the intent of cooperating with the U.K. government. HCSEC supplied a lab for the NCSC to evaluate the security of Huawei equipment. NCSC's findings in its 2019 inspection discovered several significant security risks in Huawei's buggy code loaded on their telecommunication equipment. These were the same findings as in 2018. Huawei made no corrective measures to eliminate the issues found in its firmware. NCSC also found the cybersecurity and coding to be low quality and the company's processes challenging to understand.[96]

---

[95] Matt Burgess, "The UK Just Approved Huawei 5G Equipment. Here's Why," *Wired UK*, January 28, 2020, accessed March 21, 2020, https://www.wired.co.uk/article/uk-5g-network-huawei.

[96] National Cyber Security Centre, "NCSC Advice on the Use of Equipment from High Risk Vendors in UK Telecoms Networks," last modified January 28, 2020, accessed March 21, 2020, https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks.

France struggled to reach a consensus until recently. Its cybersecurity agency, ANSSI, supplied guidance to allow for the use of Huawei telecommunications equipment on French non-core networks to minimize risk. France is following in the footsteps of Britain's recent decision regarding Huawei 5G equipment.[97]

In Belgium, the government recently made the decision to open its doors to Huawei based on E.U. guidance. Huawei opened a cybersecurity transparency center in Belgium, a similar move to its' actions in the U.K., to build trust and provide the country's cybersecurity experts the opportunity to verify the security of its equipment. The cooperation and openness of Huawei helped win over another country.[98]

New Zealand also changed direction on Huawei technologies. Initially, New Zealand, one of the Five Eyes partners, supported America's stand of banning Huawei telecommunications technology. Estimates show that New Zealand would pay 15-35 percent more for national 5G if the decision excluded Chinese equipment.[99] The government opened access to multiple vendors to supply 5G equipment. The primary winner so far in New Zealand's 5G race is Samsung, which won most contracts to expand

---

[97] Mathieu Rosemain and Gwenaelle Barzic, "Exclusive: France to Allow Some Huawei Gear in Its 5G Network - Sources," *Reuters*, March 13, 2020, accessed March 30, 2020, https://www.reuters.com/article/us-france-huawei-5g-exclusive-idUSKBN20Z3JR.

[98] Juan Pedro Tomas, "Huawei Opens Cybersecurity Center in Belgium," *RCR Wireless News*, March 6, 2019, accessed March 30, 2020, https://www.rcrwireless.com/20190306/5g/huawei-opens-cyber-security-center-belgium.

[99] Brad Glosserman, "Huawei and the Realities of the 5G World," *The Japan Times*, last modified February 3, 2020, accessed March 22, 2020, https://www.japantimes.co.jp/opinion/2020/02/03/commentary/world-commentary/huawei-realities-5g-world/.

5G capabilities across the country. Huawei is now authorized as a telecommunications vendor, but no significant purchases or actions indicate a movement to integrate the Chinese company in New Zealand.[100]

Germany is feeling the pressure to come to a decision. The German government is concerned about opening the market to Huawei and the repercussions of America limiting information sharing due to security concerns. On the other hand, China is threatening to drastically reduce German imports if Germany decides to keep Chinese telecommunications equipment out of its country.[101]

The EU revealed a set of security standards for 5G. If a telecommunications company meets these stringent standards, its equipment is authorized for use. Keeping the supply chain diversified with multiple vendors ensures a sustainable deployment of 5G that keeps up with the high demand for expansion. The E.U. created a category of high-risk suppliers whose equipment cannot be installed on core networks, although Huawei is not currently listed in this category. The E.U. commission also noted the differences in the levels of transparency of the corporate governance between Finland's Nokia, Sweden's Ericsson, and China's Huawei.[102]

---

[100] Cho Mu-Hyun, "Samsung to Supply 5G Network Solutions to Spark New Zealand," *ZDNet*, accessed March 30, 2020, https://www.zdnet.com/article/samsung-to-supply-5g-network-solutions-to-spark-new-zealand/.

[101] Katrin Bennhold and Jack Ewing, "In Huawei Battle, China Threatens Germany 'Where It Hurts': Automakers," *The New York Times*, January 16, 2020, sec. World, accessed March 30, 2020, https://www.nytimes.com/2020/01/16/world/europe/huawei-germany-china-5g-automakers.html.

[102] Elena Sanchez Nicolas, "EU Rules Leave 5G Networks Open for Huawei," *EUobserver*, last modified January 30, 2020, accessed March 21, 2020, https://euobserver.com/science/147303.

An exciting development of the E.U.'s executive body is its new proposal to build partnerships between E.U. countries to develop new 6G technologies. This proposal will allow the E.U. to certify future network technologies with direct oversight of the development. Another benefit is the assurance that sufficient vendor telecommunications equipment exists that meet E.U. security criteria for an efficient rollout of 6G.[103]

Several countries took a stance of containment with China by refusing to use Chinese telecommunication equipment on their countries' networks. These countries include America, Australia, and Japan. Concerns for national security outweighed the benefit of inexpensive telecommunications equipment.

Amongst the Five Eyes partners (America, Australia, Canada, New Zealand, and the United Kingdom), Australia stands alone with America in denying Chinese telecommunications equipment. According to authorities, Australia's stance on Chinese network products is even stricter than America's. Australian cybersecurity experts refer to China's national intelligence law that binds Chinese companies in cooperating with their government to collect intelligence. Mike Burgess directs the Australian cyber warfare and information security agency. He stresses that as 5G technology advances, the lines between core/mission-critical and non-essential network infrastructures will distort. Burgess emphasizes that the network evolution will add to the difficulty of keeping Huawei telecommunications equipment away from network segments that handle sensitive or secure data.[104]

---

[103] Sanchez Nicolas, "EU Rules Leave 5G Networks Open for Huawei."

[104] Meaghan Tobin, "Huawei Ban: Australia Isolated If UK Includes Chinese Firm in 5G," *South China Morning Post*, last modified April 26, 2019, accessed March

Huawei lodged a complaint with the WTO about Australia's ban. In the complaint, Huawei accuses Australia's decision of being blatant discrimination against their company. Australian WTO representatives defended the decision, clarifying that the decision intended to maintain strong national security. Australia's ban makes no specific mention of China or Huawei; the direction of the ban is towards any vendor that could be subject to persuasion from a foreign government.[105]

China also retaliated by delaying imported Australian coal at its ports, citing environmental hazards. Coal is Australia's second most profitable export.[106] China is willing to use punitive tactics that affect other countries' exports when opposition arises to its global expansion efforts.

In Japan, the government decided to ban all 5G equipment that could pose an elevated risk to national security. While Huawei is not directly named, most Chinese vendors are likely to fall into this category. Japan flagged fourteen different infrastructures to prioritize for protection, to include the financial sector and air travel. The Japanese government also supplies tax cuts to Japanese companies investing in the development of 5G to lessen overall costs and encourage Japanese technology advancement. Additionally, maintaining what America considers as a strong network

---

22, 2020, https://www.scmp.com/week-asia/geopolitics/article/3007810/huawei-ban-australia-becomes-increasingly-isolated-among-five.

[105] James Fernyhough, "Australia's Huawei Ban on Shaky Ground at WTO," *Australian Financial Review*, last modified April 15, 2019, accessed March 21, 2020, https://www.afr.com/policy/foreign-affairs/australia-s-huawei-ban-on-shaky-ground-at-wto-20190415-p51ebi.

[106] Tobin, "Huawei Ban."

infrastructure could go a long way in adding Japan to the Five Eyes intelligence network.[107]

In America, with the Chinese ban in place, President Trump favors America's 5G development led through the private sector. American telecommunications companies await guidance from their government on how to build high-tech networks without Chinese parts and a limited American workforce with enough training and knowhow to implement 5G. Other countries took an opposite approach by leading the development of 5G and 6G technologies with the support of their governments.[108]

A significant concern in America is the lack of qualified workers in place to deploy 5G promptly to keep up with the demand. The Department of Labor partnered with the commercial industry to develop telecommunication apprenticeships to assist with this effort. There are currently only 2000 apprenticeships in place, and this number needs to expand significantly to meet the expected expansion demand.[109]

The U.S. Government recently released its national strategy guidance for securing 5G.[110] This guidance is relatively brief and nonspecific, so additional supporting

---

[107] Glosserman, "Huawei and the Realities of the 5G World."

[108] John Hendel, "The Big Barrier to Trump's 5G America," *POLITICO*, last modified December 29, 2019, accessed March 30, 2020, https://www.politico.com/news/2019/12/29/big-barrier-trump-5g-america-089883.

[109] Ibid.

[110] US Government, "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.

information will be used to fill in the details. COA 1 will use the material derived from this research for the feasibility, acceptability, and suitability application.

Is there a solution that blends Trump's efforts with the international community's efforts to upgrade to 5G technologies securely?

Course of Action (COA) three in chapter four will attempt to answer this question by blending portions of COA 1, COA 2, and recommendations made by authors such as Bill Gertz in his book, *Deceiving the Sky: Inside Communist China's Drive for Global Supremacy,* and the Trilateral Cyber Security Commission findings.

This chapter supplied the bulk of the information that chapter 4 will use to effectively determine the Feasibility, Acceptability, and Suitability of each COA.

CHAPTER 3

RESEARCH METHODOLOGY

Proposed Methodology

The research methodology used in this thesis is a qualitative analysis using Army Design Methodology (ADM) model. According to ADP 5-0, ADM is commonly used to understand, visualize, and describe problems and approaches to solving them.[111] A graphical depiction of the framework will define the current state, the desired end state, and what changes need to occur described in the form of lines of effort (LOEs) to achieve the end state.

A qualitative content analysis methodology was used to address the secondary supporting questions throughout chapter two. These questions include:

(1) Why is Chinese technology a threat to national security?

(2) Are there any historical examples of these threats?

(3) Can we learn any lessons from other countries with their handling of Huawei, and how is America handling the 5G rollout?

Information collected throughout chapter two answered these supporting questions. This content will aid in determining the Feasibility, Acceptability, and Suitability of the three strategies in chapter four. These COAs include:

COA #1: The US policy of containment with Huawei

COA #2: The UK's policy on engagement with Huawei

[111] Headquarters, Department of the Army, Army Doctrine Publication 5-0, *The Operations Process* (Washington, DC: Government Publishing Office, July 2019), 2–16.

COA #3: A mixed policy that takes pieces from each of the previous two COAs and recommendations made in documents referenced in the literature review.

The research performed in chapter two ensured the author had a strong understanding of the intellectual and historical information regarding Huawei and the overall threat of China. Several primary sources were used to build chapter two, along with numerous supporting government publications and reliable websites, to obtain the most current status regarding the global acceptability of Huawei.

The primary justification America used to restrict Huawei was the concern of national security. All COAs presented in Chapter four must meet the minimum criteria for maintaining national security and must minimize the threat of unauthorized foreign access. The Feasibility, Acceptability, Suitability (FAS) analysis will aid in determining whether this threshold is met.

This research will scrutinize a COA using LOEs from the adaptation other countries have used in integrating Huawei equipment into their network infrastructures to address the thesis question. These countries, while not necessarily trusting Chinese companies, have taken measures to reduce the threat to their national security.

Chapter 4 will present three Courses of Action (COAs) for evaluation using FAS measures to determine the effectiveness of each as the validation criteria. FM 6-0 states

that FAS is a useful screening and measurement criteria of COAs.[112] COAs not meeting FAS requirements will not be included in the study.

COA #1, the containment COA, will detail the existing state and operational environment that President Trump constructed to keep Huawei products off US networks. Lines of Effort Trump is using to advance 5G telecommunication capabilities in America will be measured against the criteria of FAS. The goal of this thesis is to prove this COA as the most effective to help America and its allies reach their objective of establishing 5G networks across the country without impacting national security.

As mentioned in chapter two, several countries have already adapted methods to adapt and integrate some Huawei equipment into their 5G networks. The engagement COA, COA #2, will incorporate the actions of the UK's implementation of 5G into LOEs for evaluation. If this COA receives a higher overall assessment, it may disprove the general aim of this thesis.

Last, COA #3 will focus on a blended solution that takes pieces of the previous two COAs and recommendations made in documents referenced in the literature review. It will receive the same level of analysis and validation using the FAS criteria. If this COA gets a higher overall assessment, it may refute the general aim of this thesis, but also reveal alternative methodologies to handle the Chinese threat while improving 5G rollouts.

---

[112] Headquarters, Department of the Army, Field Manual 6-0, *Commander and Staff Organization and Operations* (Washington, DC: Government Publishing Office, May 2014), 9–36.

America's National Strategy to Secure 5G doctrine recommends the Prague proposal as a solid baseline for developing security principles.[113] The Prague proposals took place in 2019 with attendance from representatives from over 30 countries to include the EU, NATO representatives, America, Australia, Germany, and Japan, as seen in Figure 2.[114] The meeting allowed those in attendance to develop standardized practices, policies, and security for 5G implementation. While participants did not sign any agreements after the meeting, a strong foundation was established with many countries in agreement.[115] The document provides a solid baseline of lines of effort that are used as a standard for each COA.

[113] US Government, "National Strategy to Secure 5G of the United States of America," 3.

[114] Government of the Czech Republic, "Prague 5G Security Conference Announced Series of Recommendations: The Prague Proposals, last modified March 5, 2019, accessed April 4, 2020, https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/.

[115] Michael Kahn and Jan Loptaka, "Western Allies Agree 5G Security Guidelines, Warn of Outside Influence," *Reuters*, May 3, 2019, accessed April 4, 2020, https://www.reuters.com/article/us-telecoms-5g-security-idUSKCN1S91D2.

Figure 2. Prague 5G Security Conference Participants

Source: Government of the Czech Republic, "Prague 5G Security Conference Announced Series of Recommendations: The Prague Proposals," last modified March 5, 2019, accessed April 4, 2020, https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/.

Defining COA Lines of Effort

Each of the three COAs laid out in chapter 4 will use standard LOEs to make FAS analysis comparable between the COAs. The Prague 5G security conference proposals aided in providing information to build these LOEs. This conference had the added benefit of being one of the few meetings regarding 5G with a global attendance that developed strong policies towards regarding future implementation with strong international concurrence. The standards for each COA can be viewed in figure 3 below.

Figure 3. COA Standard

Source: Created by author.

LOE 1: Policy. Information such as the following fall into this category:

(1) What doctrine or guidance, if any, is available to address national policy and strategy for 5G implementation?

(2) What diplomatic efforts have taken place regarding 5G?

(3) What international endeavors have occurred with the developments of 5G?

(4) Are government organizations involved with 5G?

LOE 2: Technology. The following areas define technology:

(1) Are there plans in place to perform a vendor assessment to determine whether there is any state influence or involvement?

(2) Is there a risk assessment accomplished for supplier's products to identify vulnerabilities and mitigation strategies?

(3) Are customers informed on the origin and pedigree of components verifiable and documented?

LOE 3: Economy. Information falling into this category includes:

(1) Is there a diverse supply chain?

(2) Is there an investment in Research and Development for future technological improvements?

(3) Does the government provide any incentives or tax cuts to aid companies?

(4) Is there a sufficiently trained workforce available for a timely deployment?

(5) Is there adequate freedom to choose from a wide array of vendors to maintain a strong competitive market where there is little threat from a monopoly?

LOE 4: Security. Information such as the following falls in this category:

(1) Stakeholders coordinate and share information to promote security and network resilience.

(2) Best practices and lessons learned are shared to minimize network vulnerabilities and maximize network availability.

Defining the FAS Framework

Harry Yarger, in his book, *Strategic Theory for the 21st Century*, provides clear definitions of feasibility, acceptability, and suitability. The FAS assessment will be used to validate each COA in chapter 4. The framework used for scoring each COA's LOEs are as follows:

Feasibility—Using existing resources, can the strategic concept execute within the given time, space, and resource limitations?[116] *Can I squeeze this fruit with my hands?*[117] Several questions are used to assess the feasibility of each COA.

(1) Are the financial resources available to accomplish this COA?

(2) Does the technology exist to accomplish this COA?

(3) Is there enough time available to accomplish this COA?

(4) Is there sufficient qualified staff available to accomplish this COA?

(5) Is there sufficient supply available to accomplish this COA?

Acceptability—Is the overall cost outweighed by the strategic effects of the objectives? Considerations for intangibles such as international opinion, national will, and reactions of US allies and adversaries weigh heavily into this assessment.[118] *Is the juice worth the squeeze?*[119] Several questions are used to assess the acceptability of each COA.

(1) Is this COA acceptable to the Government?

(2) Is this COA acceptable to the nation's people?

(3) Is this COA acceptable to the nation's business sector?

---

[116] Harry Yarger, "C205RA: Strategic Theory for the 21st Century: The Little Book on Big Strategy," February 2006, 70, http://www.StrategicStudiesInstitute.army.mil.

[117] US Army Command and General Staff College. "C203: Power and Strategy Slides," (presented at the C204: Power and Strategy Briefing, n.d.), slide 30.

[118] Yarger, "C205RA: Strategic Theory for the 21st Century: The Little Book on Big Strategy," 70.

[119] US Army Command and General Staff College, "C203: Power and Strategy Slides," 30.

(4) Is this COA acceptable to allies and partners?

(5) Is this COA acceptable to the WTO?

Suitability—Will using the instruments of power to achieve the objectives meet the required strategic effects?[120] In other words, does it meet the end state? *Will the squeeze produce the juice I want?*[121]

(1) Will this COA maintain national security?

(2) Does this COA advance the nation's networks to 5G?

(3) Is this COA acceptable to the nation's business sector?

(4) Is this COA able to be implemented by allies and partners?

(5) Does this COA use the nation's strengths effectively?

Once the FAS assessment of each COA is complete, an analysis of the pros and cons of each approach will aid in determining which COA is most effective.

[120] Yarger, "C205RA: Strategic Theory for the 21st Century: The Little Book on Big Strategy," 70.

[121] US Army Command and General Staff College, "C203: Power and Strategy Slides," 30.

CHAPTER 4

ANALYSIS

The end state of each COA is to implement 5G solutions across the country promptly while maintaining strong national security. Each country needs to deploy 5G to keep up with the international telecommunication standard and provide its people with improved speed and network capabilities for the future. Additionally, each country needs to maintain its national security and minimize network vulnerabilities and back doors that threaten stability. These are all standards that are universally desired for a successful deployment of 5G technologies.

COA 1: Containment

President Trump took an approach of containment when dealing with China and the rollout of 5G in the United States. He signed an executive order in 2019 which prohibits the purchase of electronics from foreign companies that threaten national security. Along with this order, the US government added several Chinese companies to the US Department of Commerce's Bureau of Industry and Security Entity list. This action impacted numerous Chinese corporations, including Huawei, by placing a ban on the purchase of products from companies on the entity list while also blocking their ability to purchase products from US companies such as Google, ARM, Intel, Qualcomm, and Microsoft. [122]

[122] Doffman, "Huawei Goes To Court To Fight 'Illegal' Ban As China Decides On Softer Approach."

The House Intelligence Committee released a report in 2012 regarding Huawei and its threat to national security. Although Huawei identifies as a privately-owned company, its representatives were unable to explain the company's relationship with the Chinese government.[123] Another concern of the committee was China's recently enacted National Intelligence laws that force companies to cooperate with the government as necessary.[124]

These actions by the US Government shut Huawei out of the American market for 5G expansion. America will have to rely on other vendors to supply the telecommunications equipment for America's 5G rollout. How does America currently stand in their efforts to roll out 5G technologies without Huawei's involvement?

COA 1 / LOE 1: Policy

Doctrine

In March of 2020, President Trump released the *National Strategy to Secure 5G* document that provides America's vision of deploying 5G technologies while maintaining reliable, secure communications to protect national interests. The doctrine offers guidance on how the accelerated domestic 5G rollout will occur, methods to assess both risks and principles of security of the 5G infrastructure, address risks to US economic and national security, and promoting the responsible deployment of 5G globally.

[123] Greene and Tibken, "Lawmakers to U.S. Companies."

[124] Ibid.

President Trump's national strategy for 5G includes details on facilitating the rollout of 5G domestically. The vision of the administration is to use government agencies to streamline commercial private sector efforts to deploy 5G. The National Economic Council is responsible for collecting updated guidance from other governmental organizations regarding 5G and supplying reports to the President. The Federal Communication Commission will develop the strategy to facilitate America's 5G deployment plan by making more of the radio spectrum available for commercial use, streamlining government processes for expeditious deployment, and modernizing domestic regulations to incorporate 5G guidance. The Secretary of Commerce is responsible for providing domestic guidance on the National Spectrum Strategy. The President also encourages the private sector to work and coordinate with government agencies to foster the evaluation of innovative technologies and architecture.[125]

Diplomatic Efforts

Diplomatically, America encouraged its allies to ban the use of Huawei telecommunications equipment due to the concern of backdoors that threaten national security. The overall message to allies was that the threat to national security and the NATO alliance far outweighs the economic advantage of utilizing Chinese telecommunications equipment. Most allies strongly considered these security concerns, then decided to allow Chinese equipment on up to 35% of non-essential networks to reduce costs due to EU 5G security guidance and a desire to maintain strong relationships

[125] US Government, "National Strategy to Secure 5G of the United States of America," 2.

with their Chinese trade partners.[126] It is unknown how America will react regarding sharing intelligence with its allies, knowing those countries have added Chinese equipment and the threat of spying and backdoors on their public networks.

The two primary countries that agree with American guidance regarding the threat of Chinese telecommunication companies are Australia and Japan. These allies also recognized the threat from the ties between Huawei and the CCP. The bonds and intelligence sharing between these countries will increase with the reduced threat of Chinese backdoors.

Poland is also likely to follow the warnings from America. Previously, Poland used Huawei equipment in the country's efforts to deploy 5G. Two spies recently arrested were involved with Huawei network deployment within the country. America is expanding its global footprint in the country. Because of this, Poland is likely to reconsider the use of Huawei equipment to minimize the threat of Chinese espionage and encourage America's deployment into the country.

International Endeavors

Internationally, America provided support to the Trilateral Cybersecurity Commission. The commission is committed to improving cybersecurity standards in the US, Japan, and Europe. Experts from each country cooperated to develop recommendations to improve network security standards. The commission published its

[126] Sanchez Nicolas, "EU Rules Leave 5G Networks Open for Huawei."

findings in its *NSS for 5G Findings and Recommendations on Meeting the 5G Challenge* in 2019.[127]

America also provided representation at several internationally attended conferences to develop universal 5G standards. In May of 2019, they participated in the Prague 5G security conference. America was one of 30 countries with representatives in attendance. The meeting allowed those in attendance to develop standardized practices, policies, and security for 5G implementation.[128]

Government Organization Involvement

President Trump still encourages the growth of 5G through the free-market, private sector development but uses government organizations to establish national standards and eliminate roadblocks that may decelerate growth. There was a strong consideration to nationalize 5G in America to protect against foreign threats properly. The decision was made to maintain an open internet run by several competing private wireless providers was in the best interest of America. Several government organizations are involved in assisting and establishing standards.

The Department of Labor developed the Telecommunications Industry Registered Apprenticeship Program that enrolled over 2000 apprentices in the program to develop skilled telecommunications professionals to deploy 5G across America. The primary issue is the sheer scale of hardware installation. Estimates state that over the next 20

[127] Trilateral Cyber Security Commission, "National Security Strategy For 5G: Findings & Recommendations on Meeting the 5G Challenge."

[128] Government of the Czech Republic, "Prague 5G Security Conference Announced Series of Recommendations: The Prague Proposals."

years, an additional 800,000 5G towers will need to deploy, along with network cabling and the switching equipment that supports the expanded network backbone requirements. There is a shortfall of approximately 20,000 technicians to complete these deployments.[129] Existing staff trained in 4G installation can install 5G with minimal training, but the demand for 5G expansion is high, and the current pool of personnel primarily maintains existing 4G equipment.

The Committee on Foreign Investment in the United States (CFIUS) is chartered to operate in the best interest of protecting valuable American IP and technology. The committee has oversight over the foreign acquisition of American companies. 5G is still a developing technology, and each company has patents that would be invaluable to other telecommunication companies. CFIUS ensures that foreign countries, such as China, cannot acquire any American company that would lead to the threat of leaking technological capabilities to its government.[130]

As previously mentioned, America's 5G national strategy document covers the involvement of additional organizations. The National Economic Council collects guidance from other governmental organizations regarding 5G and supplies reports to the President. The Federal Communication Commission develops strategy for 5G deployment by making maximum use of the radio spectrum available for commercial use. The Secretary of Commerce provides domestic guidance on the National Spectrum

---

[129] Julia Bailey, "5G Is the Next Big Thing in Mobile—But Are There Enough Service Techs to Build It?" Field Service Digital, accessed May 7, 2020, https://fsd.servicemax.com/2019/10/10/5g-is-the-next-big-thing-in-mobile-but-are-there-enough-service-techs-to-build-it/.

[130] Moran, Three Threats: An Analytical Framework for the CFIUS Process.

Strategy and securing ICTS. The Federal Acquisition Security Council develops risk management guidelines for the supply chain.

COA 1/LOE 2: Technology

Vendor Assessment – State Influence

The Department of Commerce is responsible for executing the President's Executive Order 13873, Securing the ICTS Supply Chain.[131] The executive order provides the authority to the Secretary of Commerce to determine foreign adversaries and potential risks from the purchase of ICTS from these foreign threats. The Secretary also can prohibit any transaction if deemed a risk to sabotage or subversion of ICTS.

The Secretary of Commerce also receives regular updates and guidance from other agencies regarding National Security concerns. The Director of National Intelligence and the Secretary of Homeland Security have established communications and share routine assessments concerning foreign threats. These organizations working and regularly communicating, can handle identifying the threat of any state influence.

The President previously added several Chinese companies to the Department of Commerce's Security Entity List, which blocks those companies from purchasing US

[131] Executive Office of the President, "Securing the Information and Communications Technology and Services Supply Chain," *Federal Register,* last modified May 17, 2019, accessed April 7, 2020, https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain.

products. This move impacted Huawei by preventing its purchase and use of products from Google, ARM, Intel, Qualcomm, and Microsoft.[132]

In 2012, the House Intelligence Committee released a report that discouraged American companies from purchasing telecommunication equipment from Huawei due to a direct threat to national security.[133] The committee found Huawei unwilling to explain its relationship with the Chinese government adequately and a likely existing dependency on the Chinese government for support.[134]

Vulnerability Assessments

Outside of the Secretary of Commerce's involvement in identifying foreign adversaries and preventing the purchase of ICTS equipment from those countries, no government organization performs vulnerability assessments of telecommunications equipment authorized for installation. Instead, this responsibility falls on the companies utilizing the equipment to hire experts to perform these assessments.[135] Due to the ever-present threat of hacking and cybertheft, a company that doesn't adequately perform a vulnerability assessment could lead to leaked company or personal data.

---

[132] Doffman, "Huawei Goes To Court To Fight 'Illegal' Ban As China Decides On Softer Approach."

[133] Greene and Tibken, "Lawmakers to U.S. Companies."

[134] Rogers and Ruppersberger, *Investigative Report on the U.S. National Security Issues Posed by Telecommunication Companies Huawei and ZTE*, i.

[135] Trilateral Cyber Security Commission, "National Security Strategy For 5G: Findings & Recommendations on Meeting the 5G Challenge," 20.

Risk Mitigation

Outside of US Government involvement to ban HRV equipment, remaining risk mitigation strategies fall on the private sector companies running the 5G networks to accomplish.[136] There is no centralized authority to provide and share guidance to reduce risks from vulnerabilities nor to ensure telecommunication equipment vendors update the firmware to alleviate the susceptibilities. A government organization involved with sharing vulnerabilities and risk mitigation strategies would aid in reducing cyber threats.

Origin and Pedigree of Components

Other than the certification within the equipment shipping box and the documentation regarding manufacturing origin, there is no official government stamp of approval on telecommunications equipment. Having a certified agency that verifies the authenticity of equipment and a method to certify direct shipment to a customer would go a long way in reducing the threat of equipment tampering.

COA 1/LOE 3: Economy

Diverse Supply Chain

America has a diverse supply chain in place from a wide selection of trusted vendors to ensure there will not be a shortage of equipment needed for the rapid deployment of 5G. Vendors from allied countries have enough supply of telecommunications equipment to support 5G expansion across America. Companies

[136] Cybersecurity and Infrastructure Security Agency, "Overview of Risks Introduced by 5G Adoption in the United States," n.d., 12, https://www.cisa.gov/sites/default/files/publications/19_0731_cisa_5th-generation-mobile-networks-overview_0.pdf.

from Nokia, Ericsson, Samsung, LG, and Japanese Rakuten Mobile. Nokia provides a full end-to-end solution of equipment, which is a considerable advantage due to the reduction in concern regarding interoperability between different brands of gear. Rakuten Mobile is a new international player that builds software-based radio access 5G networks.[137]

Free market principles are in play here, allowing companies to work with any vendors not identified as a threat to national security. National security trumps the option to work with HRV that have a history of strong ties to its government. The WTO may disagree with this sentiment, but America is using National Security to exclude Chinese telecommunication equipment from its market.

Investment in Research and Development

In America's National Strategy document for 5G, it discusses working aggressively with the private sector to foster research and development of new technologies.[138] R&D is one area that America's free-market should handle independent of government involvement. Although, the government could provide incentives to encourage a focus of R&D in critical areas of interest for technologies that have national security implications.

---

[137] Martha DeGrasse, "Which Vendor Leads in 5G Contracts?," *FierceWireless,* last modified September 13, 2019, accessed April 8, 2020, https://www.fiercewireless.com/5g/which-vendor-leads-5g-contracts.

[138] Donald Trump, "Presidential Memorandum on Developing a Sustainable Spectrum Strategy for America's Future," The White House, 6, last modified October 25, 2018, accessed April 5, 2020, https://www.whitehouse.gov/presidential-actions/presidential-memorandum-developing-sustainable-spectrum-strategy-americas-future/.

Government Incentives and Tax Cuts

Trump's National Strategy guidance on 5G recommends working with the private sector to develop market-based incentives.[139] The President also created tax cuts and deregulations to build further incentives for the private sector to bolster their efforts towards successful rollouts of 5G technologies. His administration also eliminated regulations that prevented efficient means of deployment for companies, streamlining processes to provide companies a smoother path towards deployment.[140]

Trained Staff for Deployment

Having enough numbers of trained, qualified staff for a timely rollout of 5G across America is a concern. The Department of Labor developed the Telecommunications Apprenticeship Program, which over 2000 students have graduated. Upon completion, these apprentices move directly into the telecommunication workforce and are in very high demand. There is a vast need for 5G expansion and not enough qualified employees to keep up with the demand. There is a shortfall of 20,000 technicians to complete these deployments.[141]

[139] Trump, "Presidential Memorandum on Developing a Sustainable Spectrum Strategy for America's Future."

[140] Donald Trump, "President Donald J. Trump Is Taking Action to Ensure That America Wins the Race to 5G," The White House, last modified April 12, 2019, accessed April 8, 2020, https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-taking-action-ensure-america-wins-race-5g/.

[141] Bailey, "5G Is the Next Big Thing in Mobile—But Are There Enough Service Techs to Build It?"

Market Competitiveness

America's National Strategy document for 5G encourages working with international government partners and the private sector to foster market competition and diversity. Together, they will design a means of accountability for a diverse market through evaluations on component transparency, diversity, and competition.[142] The national strategy deals in the future. These actions have not occurred yet, as the White House released the strategy mere weeks ago.

COA 1/LOE 4: Security

Stakeholders Promote Security and Resilience

Trump recommends the government working with the private sector and international partners in fostering an environment where all stakeholders cooperate and share information to increase security.[143] Trump is relying primarily on the private sector to work together to protect networks and eliminate vulnerabilities. The President does not explicitly name a government agency that will work with the private sector. More details are necessary, as the National Strategy is an overarching strategy that does not provide ample specifics.

Best Practices

The National Strategy recommends the same means of the private sector working with governmental agencies to develop best practices. These practices could be shared

[142] Trump, "Presidential Memorandum on Developing a Sustainable Spectrum Strategy for America's Future," 6.

[143] Ibid., 6–7.

with companies responsible for securing the networks of America. The onus of responsibility for this tasking is not named.

COA 1: FAS Assessment

Feasibility

Are the financial resources available to accomplish this COA?

The American government has the funding to achieve successful deployment of 5G across the country. Numerous government agencies are in place to help streamline the rollout and establish standards. Huawei equipment averages 30-35% cheaper than competing 5G equipment. Carriers deploying 5G systems will end up spending more to complete their rollouts due to the exclusion, but the government is providing tax breaks and other means to reduce the fiscal impact. The American solution may cost more, but national security has priority over cost.

Does the technology exist to accomplish this COA?

Several vendors have the equipment necessary to make 5G deployment across America a reality. Companies ranging from Nokia, Ericsson, Samsung, LG, and Japanese Rakuten Mobile all have the means to provide the necessary equipment and know-how. These companies can work with the telecommunication carriers to deploy 5G.

Is there enough time available to accomplish this COA?

There is not a nationally prescribed timeline for 5G deployment. Very few cellular phones are currently available to take advantage of 5G. In late 2020, Apple will release the iPhone 12, which will support 5G technologies for faster communication, streaming, and downloads. Apple's iPhone is one of the most popular brands in America,

with an overall market share of 45% in the states.[144] As customers upgrade to newer phones that support 5G services, demand will grow. 5G phones all support the older, slower telecommunication networks, so even if 5G is not available in an area, phone services and data plans will still work – just at a slower speed.

Several carriers already have 5G established throughout America. AT&T expects nationwide 5G coverage within the first half of 2020. T-Mobile has 5G service in over 5000 cities and towns. Sprint expanded 5G service into several major cities. With the recent merger of T-Mobile and Sprint, the new company will combine its existing networks into a single carrier's service, thereby providing immediate expansion across the US. Verizon has 5G live in several areas across America as well.[145] The priority is to expand 5G service into major metropolitan areas to provide immediate service to the largest number of customers. Expanding service into rural areas will take longer. Considering there are many rural areas that have difficulty receiving any type of cellular service, 5G expansion may not solve this issue in the immediate future.

Is there sufficient qualified staff available to accomplish this COA?

The labor force is an area that carriers have concerns. Currently, there is not an adequate about of qualified laborers able to expedite carrier timelines. Carriers expressed a need for the Department of Labor to expand its program to expedite the needed

---

[144] S. O'Dea, "Share of People with IPhone in the US 2014-2021," Statista, last modified February 27, 2020, accessed April 8, 2020, https://www.statista.com/statistics/236550/percentage-of-us-population-that-own-a-iphone-smartphone/.

[145] Tim Fisher, "When Is 5G Coming to the US? (Updated for 2020)," *Lifewire,* last modified April 13, 2020, accessed April 8, 2020, https://www.lifewire.com/5g-availability-us-4155914.

workforce. 5G already exists in the majority of large cities, which relieves this requirement. However, as demand grows, so does the need to expand 5G across the nation. Customers have at least one carrier available, providing 5G in large cities as cellular phones are released in 2020. Worst case scenario, a customer may have to switch telephone carriers to receive 5G based on their location or use existing 4G connectivity until 5G capabilities expand into that area.

Is there sufficient supply available to accomplish this COA?

Absolutely. Several vendors have 5G equipment available and ready to deploy as necessary. Companies from Nokia, Ericsson, Samsung, LG, and Japanese Rakuten Mobile have equipment that carriers can purchase for 5G expansion right now. Eliminating HRVs from the vendor pool doesn't significantly impact the supply availability for 5G expansion.

Acceptability

Is this COA acceptable to the government?

This COA is the existing strategy of the US Government to achieve and secure national security. The President's National Strategy on 5G spells out the details provided above for COA 1. National security is the highest priority with this COA to protect its citizens' information, private sector data, and sensitive encrypted government information that rides on the same networks.

Is this COA acceptable to the nation's people?

The American people are concerned with their privacy and do not want their personal information stolen. The government's efforts to maintain national security play

into the American people's desire for network security. Overall, most US citizens do not care which vendor equipment is used on their phone networks if the networks are running smoothly and secure from hacking attempts.

Is this COA acceptable to the nation's business sector?

US Businesses have a responsibility to keep their sensitive information protected from unauthorized intrusion. This strategy makes network security its top priority. Any actions taken to reduce the threat of hacking would be welcomed by US businesses.

Is this COA acceptable to allies and partners?

America recommended to its Five Eyes partners to follow suit in banning Huawei and other high threat 5G equipment from China. Australia stood alone in following America's ban on Huawei. Japan also refused Chinese telecommunication vendors onto its networks. America's other partners accepted Huawei equipment but identified a new category of high-risk companies. These companies are only authorized for use on non-essential networks and limited to 35% on these networks.

America's allies and partners do, however, accept America's policy of containment enacted to maintain its national security. Countries that allow HRV onto their networks should not have any issues communicating with America and its uncompromised networks that exclude HRV equipment.

Is this COA acceptable to the WTO?

The WTO has not provided any response to the issue yet. Indications point to the WTO accepting America's current decision based on national security. Still, as China

contests these changes to America's stance on free-market trade, the WTO may push back and pressure America to play by the established international trade system rules.

Suitability

Will this COA maintain national security?

America identified Chinese companies as a threat due to their strong ties to the Chinese Government and the potential for backdoor access to unauthorized data. While there is no complete solution to eliminate the threat of hackers, keeping HRV off American networks improves the security of its network infrastructure.

Does this COA advance the nation's networks to 5G?

America already has 5G in place across the country. The vendors are available to provide the telecommunication equipment to spread 5G to all parts of America. A capable workforce is expanding through government apprenticeship programs but may not be able to keep up with demand. Rural areas may receive 5G last, but the capability to reach these areas in the next few years exist.

Is this COA able to be implemented by allies and partners?

Australia and Japan have followed suit with America in shutting out HRV such as Huawei based on National Security concerns. The same vendors that America is using for 5G telecommunication equipment can also supply the same capability to these allies.

Other allies throughout Europe took a different approach by allowing the same HRV into their non-core networks. This decision allows these countries the ability to expand 5G capabilities quickly and with less overall cost, but with the threat of Chinese

involvement. All allies could implement the same strategy but decided to align with WTO fair trade principles.

Does this COA use the nation's strengths effectively?

President Trump still encourages the growth of 5G through the free-market, private sector development but uses several governmental organizations to establish standards and eliminate roadblocks that may decelerate growth. America's National Strategy for 5G document provides guidance for both government and the public sector to follow. America is using its strengths effectively with this COA.

FAS Conclusion

President Trump's strategy of containment meets the assessment criteria of being feasible, acceptable, and suitable to deploy 5G throughout America promptly while maintaining National Security. Throughout the analysis, a few concerns were revealed that need attention, but overall do not severely impact the effectiveness of the American strategy.

First off, no US government organization performs vulnerability assessments of new telecommunication equipment before release to the public. Government involvement at this level would help to ensure companies are installing secure equipment onto their networks. This same agency could work with and collect added vulnerabilities from private companies to share with others to ensure all owners of that hardware have a single repository for information and risk mitigation strategies.

Second, there is not a certified agency to confirm the authenticity of equipment. A centralized agency could develop a method to certify direct shipments to customers to

reduce the threat of tampering with equipment while in transport from the seller to the buyer.

Third, the most significant finding is the lack of a sufficiently trained workforce to deploy America's 5G solutions to meet consumer demand. The primary focus has been on large cities to bring 5G to the masses, but the rural areas of America suffer due to the impact on fewer consumers. The Department of Labor created an apprenticeship program, but feedback from carriers is that the program does not supply adequate numbers of trained employees to meet their ambitious expansion plans.

Last, there is potential blowback from the WTO or retaliation from China due to America's refusal to accept Chinese telecommunication equipment. China has historically refused key exports from trade partners to heighten the pressure to fall in line and play by WTO standards.

COA 2: Engagement

Against the strong warning from America to ban HRV from their 5G footprint, the United Kingdom decided to allow Huawei telecommunication equipment on their network. The government decided on a policy of engagement that would bring added gains through cooperation and open trade with China. However, there are limitations to the extent of Huawei integration as part of the UK's risk mitigation strategy. All networks in the UK have a limit of 35 percent of their network equipment coming from HRV, which includes Huawei. The UK's core Critical National Infrastructure and its sensitive military networks do not authorize Huawei equipment use. Additionally, the UK cannot purchase network analytic equipment, authentication systems, and data management systems from HRVs whatsoever. The UK's National Cyber Security Center

(NCSC) was vital in supplying information to the Prime Minister to aid in his decision.[146]

COA 2 / LOE 1: Policy

Doctrine

The UK published its National Strategy in 2017, titled "Next Generation Mobile Technologies: A 5G Strategy for the UK."[147] The document provides a vast amount of detail regarding the rollout of 5G within the country. The UK published this document three years ago, and updates were necessary. Reputable web resources were used to fill in the blanks and to obtain updates to this older document. The National Strategy details the need for 5G across the country, secure deployment of 5G, and technological standards the country will use for 5G.

Diplomatic Efforts

Diplomatically, the UK worked with China to form a solution that allowed Chinese telecommunications equipment on its networks while still maintaining adequate network security for the sake of National Security. Huawei launched the Huawei Cyber Security Evaluation Center (HCSEC) in England with the intent of cooperating with the UK government. The UK's National Cyber Security Center (NCSC) evaluates Huawei's equipment and firmware in the HCSEC. Together, the two teams strive to identify and

---

[146] Burgess, "The UK Just Approved Huawei 5G Equipment. Here's Why."

[147] Department for Digital, Culture, Media & Sport, "Next Generation Mobile Technologies: A 5G Strategy for the UK," GOV.UK, last modified March 8, 2017, accessed April 9, 2020, https://www.gov.uk/government/publications/next-generation-mobile-technologies-a-5g-strategy-for-the-uk.

patch vulnerabilities to provide the country with secure equipment for 5G expansion purposes.

The NCSC was vital in aiding the Prime Minister's decision regarding Chinese companies. The UK government did establish limitations to maintain what they determined as a high degree of security. The NCSC created a category of HRV. Non-core networks have a limit of 35% of equipment from any company on the HRV list. Core networks cannot have any HRV equipment installed.

There is a concern that America may limit intelligence sharing with countries not heeding its warnings regarding the threat of spying. The UK parliament opposed the decision, seeing it as a decision based on cost-cutting measures and less on the concern of national security.[148] The EUs guidance regarding 5G is aligned with the UK's solution.

International Endeavors

The UK government is involved in several international committees to share and collaborate their findings, and aid in making decisions regarding the outcome of 5G on an international basis. The establishment of 5G testbeds throughout the UK will facilitate international links to maximize global network speed, bandwidth, and efficient communication. These same links will also facilitate the sharing of 5G findings to improve the development of 5G internationally.[149]

---

[148] John Lee, "5G and Huawei: The UK and EU Decide," *The Diplomat*, last modified February 15, 2020, accessed April 10, 2020, https://thediplomat.com/2020/02/5g-and-huawei-the-uk-and-eu-decide/.

[149] Department for Digital, Culture, Media & Sport, "Next Generation Mobile Technologies," 56.

While the UK was still part of the EU, it provided representation at several conferences to develop international 5G standards. In May of 2019, they participated in the Prague 5G security conference. The UK was one of 30 countries with representatives in attendance. The meeting allowed those in attendance to develop standardized practices, policies, and security for 5G implementation.[150]

Government Organization Involvement

The UK's NCSC performed a thorough evaluation and published annual reports regarding their work with Huawei. Huawei launched the Huawei Cyber Security Evaluation Center (HCSEC) in England with the intent of cooperating with the UK government. HCSEC supplied a lab for the NCSC to evaluate the security of Huawei equipment. The NCSC performs annual inspections and publishes reports of security risks for vendors to assess and fix. On top of security checks for vendors, the NCSC also works with customer needs to develop new security architectures and builds 5G testbeds.

The Department for Digital, Culture, Media, and Sport (DCMS) is responsible for establishing rules and policies for digital infrastructures in England, including 5G.[151] The department established a new branch responsible for building and sharing 5G expertise across the UK to increase 5G capabilities that benefit the entirety of the country. The team will ensure proper coordination of 5G development while capturing best practices and disseminating its knowledge with industry and the private sector. DCMS will also

[150] Government of the Czech Republic, "Prague 5G Security Conference Announced Series of Recommendations: The Prague Proposals."

[151] Department for Digital, Culture, Media & Sport, "Next Generation Mobile Technologies," 8.

work with other subject-matter experts from other countries to share lessons-learned and aid in assisting the global 5G standards.

The National Infrastructure Commission developed recommendations to aid the UK in becoming a world leader for the deployment of 5G across the globe. This strategy defines steps for the government to accelerate 5G deployment, maximize benefits for the UK, and create new opportunities for businesses.[152]

Parliament assigned the duties of spectrum management to Ofcom, which is an independent organization responsible for ensuring the available radio spectrum meets the future technological needs of the country, including 5G. The World Radio Communications Conference of 2015 analyzed the existing radio spectrum and determined it could meet the future demands of the faster technologies. The strategy developed from that conference stressed a need for spectrum sharing between government, private citizens, and industry. This strategy will be reassessed as 5G technologies expand throughout the region.[153]

The UK government created legislation in 2018 based on its Enterprise Act of 2002, which allows the Secretary of State more control and visibility of market acquisitions. This act gives the government the ability to block mergers and acquisitions deemed a threat to national security. Another benefit is that crucial IP developed within

[152] Department for Digital, Culture, Media & Sport, "Next Generation Mobile Technologies," 8.

[153] Ibid., 47.

the UK does not change hands with a foreign entity. This measure provides long term protection for the UK's technical sector's valuable IP.[154]

The UK's 5G strategy document does discuss the potential concern for a shortage of qualified workers to deploy the new 5G architecture. There are many existing civil engineers and technical specialists already in the field that focuses on 4G, but a full deployment for 5G requires far more staff. The document states that the government will investigate the skill requirements and determine whether any government involvement needs to take place.[155] No further updates regarding worker shortages could be found.

COA 2/LOE 2: Technology

Vendor Assessment – State Influence

The United Kingdom's National Cyber Security Center (NCSC) developed a category of vendors that pose an added threat due to questionable relationships between companies and their governments, known as HRV. The danger of government pressure and influence to provide sensitive information riding on the company's equipment was a top concern. The ruling of the NCSC enforces all networks in the UK to have a limit of 35 percent of their network equipment coming from HRV, which includes Huawei. The UK's core Critical National Infrastructure and its sensitive military networks do not authorize Huawei equipment use. Additionally, the UK cannot purchase network analytic

[154] Robert Bell, "BCLP EU & Competition Law," EU Competition Law, last modified May 17, 2018, accessed April 10, 2020, http://eu-competitionlaw.com/greater-national-security-scrutiny-at-the-heart-of-new-uk-merger-control-reforms/.

[155] Department for Digital, Culture, Media & Sport, "Next Generation Mobile Technologies," 34.

equipment, authentication systems, and data management systems from HRVs whatsoever.

Vulnerability Assessments

The UK's NCSC performs thorough evaluations and publishes annual reports regarding its work with Huawei. Huawei launched the Huawei Cyber Security Evaluation Center (HCSEC) in England with the intent of cooperating with the UK government. HCSEC supplied a lab for the NCSC to evaluate the security of Huawei equipment. The NCSC assesses new equipment and firmware from Huawei to identify and eliminate vulnerabilities that hackers could exploit.

Risk Mitigation

The NCSC placed Huawei on their HRV list. This move limits Huawei equipment to a maximum of 35% of its equipment on non-core networks. Core networks cannot use any equipment from a vendor on the HRV list.

The Department for DCMS is responsible for building and sharing 5G expertise across the UK to increase 5G capabilities that benefit the entirety of the country. The team will ensure proper coordination of 5G development while capturing best practices, risk mitigation strategies, and disseminating its knowledge with industry and the private sector. DCMS will also work with other subject-matter experts from other countries to share lessons-learned and aid in assisting the global 5G standards.[156]

[156] Department for Digital, Culture, Media & Sport, "Next Generation Mobile Technologies," 8.

Origin and Pedigree of Components

Like America, the UK does not have an agency that verifies the authenticity of equipment. Other than the certification within the equipment shipping box and the documentation regarding manufacturing origin, there is no official government stamp of approval on independently purchased telecommunications equipment to reduce the risk of tampering.

COA 2/LOE 3: Economy

Diverse Supply Chain

The supply chain options in the UK do not rule out a single vendor. With every vendor being an option, it creates a very robust supply chain that does not rely on a single vendor, which minimizes the risk of dependency while maximizing competition. The three primary players in the country are Huawei, Ericsson, and Nokia. Free market principles are in play.

Investment in Research and Development

The UK Telecoms Supply Chain Report discussed the government's strategy regarding research and development in the 5G market. Companies investing in R&D for 5G technologies are eligible for tax credits to lower the burden of bringing new technologies to the market.[157] Additionally, the government makes public funds available for innovations, such as the National Security Strategic Investment Fund and the

[157] Jeremy Wright, "UK Telecoms Supply Chain Review Report," Department for Digital, Culture, Media & Sport, July 2019, 43, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819469/CCS001_CCS0719559014-001_Telecoms_Security_and_Resilience_Accessible.pdf.

Industrial Strategy Challenge Fund.[158] Tax cuts, tax credits, and public funding options are great enablers to encourage more players in the 5G market.

Government Incentives and Tax Cuts

The UK government stimulated growth in the 5G market by establishing tax incentives for businesses to attract vendors to the market. The government also improves costs overall for carriers by using its collective purchasing power to buy massive quantities at a discount. Additionally, the government provides tax credits to companies investing in research and development in 5G and future technologies.[159]

Trained Staff for Deployment

The UK's 5G strategy document discusses the potential concern for a shortage of qualified workers to deploy the new 5G architecture. The existing 4G workforce can transition to 5G, but a full deployment requires far more staff. The document states that the government will investigate the skill requirements and determine whether any government involvement needs to take place.[160]

Market Competitiveness

According to the UK Telecoms Supply Chain Review Report release by the DCMS, the organization will build a diversification strategy that allows for the growth of

[158] Wright, "UK Telecoms Supply Chain Review Report," 41.

[159] Ibid., 43.

[160] Department for Digital, Culture, Media & Sport, "Next Generation Mobile Technologies," 34.

all vendors in the market. This strategy includes international partners, such as Huawei, to ensure fair competition within the market. From an international perspective,

Additionally, the UK government is investing in the country's future by launching a national program of 5G testbeds. The research and developmental findings from this program will allow for innovative, customizable network frameworks that ensure interoperability between different network equipment for the government and private sectors.[161] Furthermore, discoveries made in the testing environment could lead to the development of patent pool portfolios for long term market competitiveness for UK companies.[162]

COA 2/LOE 4: Security

Stakeholders Promote Security and Resilience

The Department for DCMS is responsible for building and sharing 5G expertise across the UK to increase 5G capabilities that benefit the entirety of the country. The team will ensure proper coordination of 5G development while capturing best practices, risk mitigation strategies, and disseminating its knowledge with industry and the private sector. DCMS will also work with other subject-matter experts from other countries to share lessons-learned and aid in assisting the global 5G standards.[163]

[161] Department for Digital, Culture, Media & Sport, "Next Generation Mobile Technologies," 11.

[162] Ibid., 61.

[163] Ibid., 8.

Best Practices

The DCMS is responsible for capturing best practices while working with the private sector and other governmental agencies. Having a centralized organization that companies can contact for assistance or guidance is beneficial to maximize security practices and network efficiencies.

COA 2: FAS Assessment

Feasibility

Are the financial resources available to accomplish this COA?

The UK government has the financial resources available to support 5G deployment across the country. Several government organizations are involved with ensuring the success of 5G expansion within the country. Commercial carriers will accomplish most of the deployment and have the added benefit of relying on Huawei equipment that, on average, offers savings of 30-35% over other vendor's equipment. The government also offers tax cuts and credits to encourage commercial R&D and overall growth.

Does the technology exist to accomplish this COA?

The country's strategy of engagement with China allows commercial carriers to choose from any 5G vendor. Primary companies holding contracts for 5G in the UK range from Huawei, ZTE (both blocked from sales in America), Nokia, and Ericsson. The market is open to allow other vendors as well, such as Samsung, LG, and Rakuten

Mobile. These vendors have the equipment to work with existing carriers within the country to deploy 5G effectively.

Is there enough time available to accomplish this COA?

The UK National Strategy document sets a suspense of no later than 2025. Currently, there are few cellular phones available to take advantage of 5G. As customers upgrade to newer phones that support 5G services, demand will grow. 5G phones all support the older, slower telecommunication networks, so even if 5G is not available in an area, phone services and data plans will still work – just at a slower speed.

Several carriers already have 5G established throughout the UK. EE launched 5G in May 2019 and expect to have 5G connectivity in over 70 towns and cities by the spring of 2020. Vodafone is already live in several large cities and towns. The carrier Three UK deployed to 65 towns and cities, going live with 5G services in February of 2020. The carrier O2 has 5G services already available in several major cities. Several other smaller players also offer services that aren't included here for the sake of brevity.[164] The overall strategy of most carriers is to expand 5G service into major metropolitan areas to provide immediate service to the largest number of customers. Expanding service into rural areas will take longer.

[164] John McCann, "5G in the UK: Everything You Need to Know," *TechRadar,* last modified February 14, 2020, accessed April 11, 2020, https://www.techradar.com/news/5g-uk.

Is there sufficient qualified staff available to accomplish this COA?

The UK's 5G strategy document discusses the potential concern for a shortage of qualified workers to deploy the new 5G architecture. The existing 4G workforce can transition to 5G, but a full deployment requires far more staff. The document states that the government will investigate the skill requirements and determine whether any government involvement needs to take place.[165] Considering 5G is already available throughout the country, with rural pockets lacking 5G, the strategy of providing 5G everywhere in the country by 2025 appears obtainable with the existing workforce.

Is there sufficient supply available to accomplish this COA?

Several vendors have 5G equipment available and ready to deploy, as necessary. Companies from Huawei, ZTE, Nokia, Ericsson, Samsung, and LG have equipment that carriers can purchase for 5G expansion right now. With no ban of vendors, the availability at a maximum.

Acceptability

Is this COA acceptable to the Government?

The UK's National Cyber Security Center (NCSC) was vital in supplying information to the Prime Minister to aid in his decision.[166] The NCSC is confident that the vulnerabilities and potential backdoors are minor concerns that could be handled effectively. The UK Parliament, however, is concerned about the sacrifice to security

[165] Department for Digital, Culture, Media & Sport, "Next Generation Mobile Technologies," 34.

[166] Burgess, "The UK Just Approved Huawei 5G Equipment. Here's Why."

made to eliminate potential retaliation from China. Considering the Prime Minister already approved the use of Huawei in the country, this COA is acceptable, but with strong contention.

Is this COA acceptable to the nation's People?

Citizens of the UK are concerned about the security of their confidential information. The use of Huawei equipment does allow for the integration of the company's expertise. The company is a world leader in 5G technologies. 5G has the potential for a faster rollout but at the sacrifice of security from the use of HRV equipment. The use of Huawei provides the benefit of lower cost to carriers, which may also be passed onto the customer. If there are no instances of the Chinese government intrusion to citizen's data, there should be minimal objections from people.

Is this COA acceptable to the nation's business sector?

Businesses have two primary concerns with 5G: speed and security. The use of Huawei equipment provides the benefit of the speed and extra bandwidth of 5G. At the same time, there is concern about the backdoors that Huawei may provide to the Chinese government. As demonstrated throughout chapter 2, China benefitted immensely from the illegal embezzlement of IP. UK businesses should have a strong concern of Chinese attempts to gain access to their sensitive information. The NCSC is confident that the vulnerabilities and potential backdoors are minor and can be handled effectively.

Is this COA acceptable to allies and partners?

The EU revealed a set of security standards for 5G. If a telecommunications company meets these stringent standards, its equipment is authorized for use. The EU

created a category of high-risk suppliers whose equipment cannot be installed on core networks, although Huawei is not currently listed in this category. The EU commission also noted the differences in the levels of transparency of the corporate governance between Finland's Nokia, Sweden's Ericsson, and China's Huawei.[167] The commission's policy is similar to the UK's 5G strategy.

America warned its FIVE EYES allies regarding the threat of backdoors to Chinese equipment and the close relationship between these companies and the government. There is a concern that America may limit intelligence sharing with countries not heeding its warnings regarding the threat of spying. At this time, it is unknown what reaction, if any, America will have in dealing with allies that allowed what it considered compromised equipment onto its networks.

Is this COA acceptable to the WTO?

The WTO is an international organization that establishes and enforces international trade rules.[168] The organization strives for lowering trade barriers, including customs and tariffs, and eliminating unfair, discriminatory methods to reduce the importation of foreign products. UK's agreement to use Chinese HRV's equipment supports a policy of international cooperation, engagement, and free trade, which aligns with WTO policy and guidelines.

---

[167] Sanchez Nicolas, "EU Rules Leave 5G Networks Open for Huawei."

[168] World Trade Organization, "What Is the WTO?"

Suitability

Will this COA maintain national security?

The UK's National Cyber Security Center (NCSC) evaluates Huawei's equipment and firmware in the HCSEC. Huawei launched the Huawei Cyber Security Evaluation Center (HCSEC) in England with the intent of cooperating with the UK government. Together, the two teams strive to identify and patch vulnerabilities to provide the country with secure equipment for 5G expansion purposes. Considering the NCSC limited Chinese equipment to 35% on non-core networks, they have not entirely ruled out the potential threat, but keeping the threat isolated on non-core networks reduces that threat. Until proven otherwise, the cybersecurity experts of the UK believe the threat is under control.

Does this COA advance the nation's networks to 5G?

The UK already has 5G in place in many parts of the country. The government is involved to ensure there are minimal speedbumps to slow progress. 5G still needs to expand in many places, and having Huawei equipment available, along with all the other vendors, allows carriers to grow.

Is this COA able to be implemented by allies and partners?

Many countries within the EU are using a similar strategy in the implementation of 5G and identifying HRVs on segmented portions of networks. The EUs 5G commission's policy has many similarities with the UK's 5G strategy. These countries are willing to accept an extra level of risk to reduce overall costs – sacrificing security for cost.

Other allies, such as America, Australia, and Japan, will not accept this strategy due to the high risk of backdoors and the relationship between Huawei and its government. These countries already established successful strategies that have partially deployed 5G already, and the primary concern is a potential lack of qualified technicians to install the equipment, which appears in the UK's strategy as well. Keeping Huawei and other HRVs out of the equation in these countries has not affected the deployment of 5G.

Does this COA use the nation's strengths effectively?

The Prime Minister's decision allows for free-market, private sector development. Additionally, the government uses many of its organizations and agencies to encourage growth while streamlining standards. Both the private sector and government are heavily involved and cooperating for the future of the UK's 5G.

FAS Conclusion

Overall, the UK's strategy of engagement, which allows the purchase of Chinese equipment, passes the feasibility, acceptability, and suitability assessment. There are a few concerns which did not have conclusive answers but have the potential to cause issues moving forward. Ideally, the experts in charge of 5G growth within the country make these concerns address these issues. The primary issues focus on suitability and acceptability.

One primary concern regarding this COA is how allied nations will share intelligence moving forward. It is presumed that America and other allies are unwilling to accept the UK's use of potentially compromised equipment. America warned its allies regarding the threats of backdoors, the requirement for Chinese private companies to

create a CCP branch with direct ties and communication back to the party, and the National Intelligence Law passed in 2017 that forces companies to cooperate with Chinese national authorities for intelligence gathering. The appeal of Huawei is its established 5G program and overall lower costs. It is unknown what effect the UK's decision to allow the use of Chinese equipment will have on sensitive communications between allied partners. Allies that banned Huawei equipment find this decision by the UK unacceptable and are unwilling to implement the same strategy due to security concerns.

The UK Parliament has concerns about the sacrifice of security made to eliminate potential retaliation from China. The Prime Minister approved the use of Huawei and other HRVs in the country, so overall, the government finds this strategy acceptable. But it is a controversial decision with much disagreement.

Last, there is a concern regarding the suitability of the UK's 5G strategy. While from the standpoint of security, there is no direct proof of intentional backdoors in Huawei equipment, but historical evidence leads to a reasonable likelihood. Evidence such as the previous successful attempts of Chinese cyber intrusions to steal billions of dollars' worth of IP, the stealth of millions of government and military personal data and fingerprints in the cyberattack on OPM, and Huawei's previous encouragement for employees to steal IP from other leading technology companies.

The NCSC's technical director contends the feasibility of secure 5G by keeping HRV equipment away from core networks that transmit sensitive data. He believes keeping the networks separate with improved security measures will maintain the required security, but it may also limit network performance due to design restrictions.

The NCSC's risk assessment of the malicious functionality, such as backdoors, in HRV equipment, is manageable by limiting the number of HRV products on non-core network segments.[169]

The decision comes down to their Cyber Security experts to determine if the threat is manageable. It is unknown what information America shared with its allies and partners in the classified realm, so a proverbial smoking gun is not observable from public data. The public data does, however, provide recurring evidence of ties between the CCP and its private companies. Additionally, the Chinese government demonstrated successful cyber-hacking that led to the theft of billions of dollars of American IP and government employee personal data, and Huawei's efforts to steal American IP to advance its technologies.

COA 3: Blended Solution

The first two COAs are existing strategies of two countries that have already been put into motion to move their respectful countries forward in their efforts to deploy 5G efficiently with a strong consideration of national security. Through the feasibility, acceptability, and suitability assessment of each of the COAs, both passed the assessments, but concerns were identified that could lead to potential problems moving forward. The next COA has the potential to alleviate these issues.

The third COA, the blended solution, uses the American COA as its baseline but integrates portions from COA 2 and additional findings from the Trilateral Cyber Security Commission's NSS for 5G document. Internationally, America provided support

[169] Lee, "5G and Huawei."

to this commission to develop and improve global 5G standards. The commission is committed to improving cybersecurity standards in the US, Japan, and Europe. Experts from each country cooperated to develop recommendations to improve network security standards. Ideally, these standards could become accepted by the worldwide community rather than each country developing a different strategy.

COA 3 / LOE 1: Policy

Doctrine

President Trump's *National Strategy to Secure 5G* is the doctrine used in this COA. The document requires an update to integrate changes of some of the recommendations made in the Trilateral Cyber Security Commission's NSS for 5G documents. Changes required for America's National Strategy for 5G include:

(1) The addition of a new NCSC-type agency to perform vulnerability assessments and establish strict security standards for all telecommunication vendors to meet.

(2) The establishment of a 5G International Security Council to increase international 5G coordination and development of international security standards.[170]

(3) The Department of Labor's apprenticeship program is shifted into high gear to provide the needed workforce to deploy 5G.

[170] Trilateral Cyber Security Commission, "National Security Strategy For 5G: Findings & Recommendations on Meeting the 5G Challenge," 25–26.

(4) Open-source software to standardize interfaces, improve interoperability, and provide the added value of hobbyists continuously assessing software for vulnerabilities and enhancements.

(5) An open door for all vendors, if they can meet strict security criteria and meet all of the concerns of the House Intelligence Committee.

Diplomatic Efforts

COA 3 encourages further coordination with other countries comparable to what America accomplished so far. Continue maintaining communication with NATO and FIVE EYES partners discussing the best way ahead to ensure safe communications. The US needs to reengage with China to discuss ways to progress beyond the stalemate**.** American requirements would need to be clearly defined. If Chinese vendors could not meet all the requirements, their equipment is not accepted until security conditions are met.

America needs to build the equivalent of the UK's NCSC agency to work with China. This agency would have the responsibility of ensuring all telecommunication equipment available for purchase in America meets an established minimum threshold for security requirements. Having an agency such as the NCSC available keeps the door open to work with Chinese telecommunications vendors, while also ensuring that all released equipment meet American security standards (not just Chinese vendors).

International Endeavors

Internationally, America provided support to the Trilateral Cybersecurity Commission. The commission is committed to improving cybersecurity standards in the

US, Japan, and Europe. Experts from each country cooperated to develop recommendations to improve network security standards. The commission published its findings in its *NSS for 5G Findings and Recommendations on Meeting the 5G Challenge* in 2019.[171]

America also provided representation at several internationally attended conferences to develop universal 5G standards. In May of 2019, they participated in the Prague 5G security conference. America was one of 30 countries with representatives in attendance. The meeting allowed those in attendance to develop standardized practices, policies, and security for 5G implementation.[172]

The Trilateral Cyber Security Commission's NSS for 5G report recommends establishing an International Security Council to increase international 5G coordination. This council's responsibilities include coordinating security baselines to review risks of foreign 5G vendors, sharing technical standards to assess security risks of vendors and the risk assessments of each, and developing consensus on vendors not meeting international security standards.[173] A commission involving international participation would provide a smooth way to develop international standards and ensure vendor equipment considered high-risk isn't allowed in networks on a global basis to increase international security.

---

[171] Trilateral Cyber Security Commission, "National Security Strategy For 5G: Findings & Recommendations on Meeting the 5G Challenge."

[172] Government of the Czech Republic, "Prague 5G Security Conference Announced Series of Recommendations: The Prague Proposals."

[173] Trilateral Cyber Security Commission, "National Security Strategy For 5G: Findings & Recommendations on Meeting the 5G Challenge," 25–26.

Government Organization Involvement

Identical to COA 1, but with the following changes. The Department of Labor developed the Telecommunications Industry Registered Apprenticeship Program is running in high gear to keep up with the demands for 5G expansion. The Trilateral Cyber Security Commission's National Strategy for 5G recommends that CFIUS take on the added task of screening all foreign 5G equipment providers.[174]

One observation made between the first two COAs is America's lack of a governmental body in charge of ensuring all telecommunication equipment available for purchase in America meets an established baseline of security requirements. The Trilateral Cyber Security Commission's National Strategy for 5G recommends building a cybersecurity evaluation agency similar to the UK's NCSC agency to work with China and other telecommunications vendors to ensure products meet stringent American security standards.[175] Private companies and networks carriers have little chance of protecting themselves against the might of a willing nation that heavily funds cyber-attacks. This agency could also coordinate with key representatives from the private sector to aid in ensuring their networks are properly secured and have the latest guidance on vulnerabilities and risk mitigation strategies.

This new agency would push for standardization to ensure there is interoperability between vendor equipment. Open Networking Automation Platform (ONAP) would be one strong recommendation. This capability enables a single foundational open-source

[174] Trilateral Cyber Security Commission, "National Security Strategy For 5G: Findings & Recommendations on Meeting the 5G Challenge," 21.

[175] Ibid.

platform that can work across all differing vendor equipment. This open-source capability allows for improved automation and resource allocation.[176]

Open source is essential. It allows a massive community of people to look at the software to identify problems and validate issues. An existing model of open source is the Solaris UNIX community. There is a massive community of system engineers that spend their free time analyzing code for improvements, and this community performs these tasks as a hobby.[177] The NCSC would get free analysis and assessment on the code, allowing them to release products that had far more analysis accomplished than a small team of professionals could hope to accomplish.

COA 3/LOE 2: Technology

Vendor Assessment – State Influence

Identical to COA 1, with the following changes. The creation of a new NCSC-type agency in this COA provides a liaison to work with all telecommunication vendors. Chinese companies would have to meet all American requirements. Not only would every company need to answer the questions of the House Intelligence Committee to no longer be considered a national security threat, but each vendor would also have to meet all the NCSC security requirements. If these standards are not met, the vendor equipment is not authorized. This strategy at least keeps the door open for companies currently

[176] US Department of State, "Deep Dive: How the U.S. Is Addressing 5G and Security," n.d., accessed April 7, 2020, https://www.state.gov/deep-dive-how-the-u-s-is-addressing-5g-and-security/.

[177] Ibid.

banned under COA 1 to become an option for use in America. This strategy puts the onus on companies to meet American security requirements instead of an outright ban.

Additionally, strong domestic policies would be developed to penalize foreign vendors that are found violating security requirements, or allowing backdoor access to content will immediately be removed from the authorized list. The burden of proof falls on the vendor to provide proof of no wrongdoing.[178] This policy helps keep companies honest when its future relies on maintaining American standards.

Vulnerability Assessments

In this COA, America developed the equivalent of the UK's NCSC. This agency develops security standards for vendors to meet. If a vendor's products do not meet the security criteria established by the agency, its products are prohibited. The NCSC equivalent also works with other government and private companies to identify existing vulnerabilities and share their findings with other organizations.

Risk Mitigation

Again, having an agency such as the NCSC created would go a long way in alleviating concerns regarding vulnerabilities and risk mitigation strategies. This agency would be responsible for sharing risk mitigation strategies. On top of vendor approval, vulnerability assessments, and risk mitigation, the agency would also build and share its 5G expertise and developed best practices with the public, private. Government sectors to increase 5G capabilities and awareness that benefits the entirety of the country.

[178] Trilateral Cyber Security Commission, "National Security Strategy For 5G: Findings & Recommendations on Meeting the 5G Challenge," 22.

Origin and Pedigree of Components

In this COA, America developed the equivalent of the UK's NCSC. This agency develops security standards for vendors to meet. Vendor equipment meeting these criteria receives the agency's stamp of approval for pedigree. One part of the vulnerability assessment is developing supply chain security to minimize the threat of component tampering. The agency would identify approved sellers and develop means of point-to-point delivery to ensure equipment avoids man-in-the-middle attacks after components leave production factories.

COA 3/LOE 3: Economy

Diverse Supply Chain

COA 3 still uses America's methodology from COA 1 of ensuring a diverse supply chain. One minor difference in this COA is that America is willing to keep the door open to work with Chinese vendors if they meet all American security requirements. Free market principles are in play here, allowing companies to work with any vendors not identified as a threat to national security. The WTO has no objections to this policy, as there is a willingness to allow Chinese vendors that meet all American security requirements.

Investment in Research and Development

America's existing methodology from COA 1 is effective and applied to this COA. Minimized government involvement allows the private sector to do what it does best with research and development. Providing tax cuts and other incentives to companies to focus on critical interests for technological growth of 5G and beyond with a strong

focus on future international standards and strong security could help to shape future growth with interest in both the national security requirements of the government and public sector growth.

Government Incentives and Tax Cuts

Trump's National Strategy guidance on 5G recommends working with the private sector to develop market-based incentives.[179] The President also created tax cuts and deregulations to build further incentives for the private sector to bolster their efforts towards successful rollouts of 5G technologies. His administration also eliminated regulations that prevented efficient means of deployment for companies, streamlining processes to provide companies a smoother path towards deployment.[180]

Trained Staff for Deployment

This COA takes the Department of Labor's program and multiplies its efforts to provide further qualified apprentices to reduce the demand on the workforce to deploy 5G across the country promptly.

Market Competitiveness

The previous two COAs have plans to develop strategies that allow for the growth of all vendors in the market but with nothing established. Having a multitude of existing vendors to choose from keeps competition relevant and costs down. Free market

[179] Trump, "Presidential Memorandum on Developing a Sustainable Spectrum Strategy for America's Future," 6.

[180] Trump, "President Donald J. Trump Is Taking Action to Ensure That America Wins the Race to 5G."

principles are in play here, allowing companies to work with any vendors not identified as a threat to national security.

COA 3/LOE 4: Security

Stakeholders Promote Security and Resilience

The aforementioned agency built with a similar scope of responsibilities to the UK's NCSC would ensure proper coordination of 5G development while capturing and developing best practices with partners while sharing findings to increase security improves America's national security. Sharing of information is vital to spread awareness and help mitigate vulnerabilities across the country. The agency could provide a public website to offer assistance and provide a centralized repository of information and guidance to assist network engineers expediently.

Best Practices

The NCSC-type agency would have the responsibility of sharing best practices. This effort would be accomplished through cooperation and information sharing between the private, public, and government sectors. Communication is key. If companies are not sharing their findings, it leads to stove-piped solutions instead of nationally accepted standards.

COA 3: FAS Assessment

Feasibility

Are the financial resources available to accomplish this COA?

The American government has the funding to achieve successful deployment of 5G across the country. Numerous government agencies are in place to help streamline the

rollout and establish standards. This COA allows the option for Chinese vendors such as Huawei to provide equipment, pending they meet stringent security requirements. These companies average 30-35% cheaper than competing 5G equipment. Carriers deploying 5G systems will end up spending the same amount or less due to the possible inclusion of Huawei. Still, the government is providing tax breaks and other means to reduce the impact.

Does the technology exist to accomplish this COA?

Vendors from allied countries have enough supply of telecommunications equipment to support 5G expansion across America. Companies from Nokia, Ericsson, Samsung, LG, and Japanese Rakuten Mobile. Nokia provides a full end-to-end solution of equipment, which is a considerable advantage due to the reduction in concern regarding interoperability between various brands of gear. Rakuten Mobile is a new international player that builds software-based radio access 5G networks.[181] This COA also allows for Chinese vendors if they meet all American security requirements.

Is there enough time available to accomplish this COA?

There is not a nationally prescribed timeline for 5G deployment. Very few cellular phones are currently available to take advantage of 5G. As customers upgrade to newer phones that support 5G services, demand will grow. 5G phones all support the older, slower telecommunication networks, so even if 5G is not available in an area, phone services and data plans will still work – just at a slower speed.

[181] DeGrasse, "Which Vendor Leads in 5G Contracts?"

Several carriers already have 5G established throughout America. AT&T expects nationwide 5G coverage within the first half of 2020. T-Mobile has 5G service in over 5000 cities and towns. Sprint expanded 5G service into several major cities. With the recent merger of T-Mobile and Sprint, the new company will combine its existing networks into a single carrier's service, thereby providing immediate expansion across the US. Verizon has 5G live in several areas across America as well.[182] The priority is to expand 5G service into major metropolitan areas to provide immediate service to the largest number of customers. Expanding service into rural areas will take longer. Considering there are many rural areas that have difficulty receiving any type of cellular service, 5G expansion may not solve this issue in the immediate future.

Is there sufficient qualified staff available to accomplish this COA?

Having a sufficient trained workforce is an area that carriers have concerns. Currently, there is not an adequate amount of qualified laborers able to expedite carrier timelines. The Department of Labor developed the Telecommunications Apprenticeship Program to aid carriers with meeting their requirements. This COA takes the Department of Labor apprenticeship program and increases its capability to provide more qualified apprentices to carriers deploying 5G.

Is there sufficient supply available to accomplish this COA?

Several vendors have 5G equipment available and ready to deploy as necessary. Companies from Nokia, Ericsson, Samsung, LG, and Japanese Rakuten Mobile have

[182] Fisher, "When Is 5G Coming to the US?"

equipment that carriers can purchase for 5G expansion right now. This COA also allows for Chinese vendors to provide equipment if they can meet stringent US security requirements.

Acceptability

Is this COA acceptable to the Government?

This COA is the existing strategy of the US Government to achieve and secure national security. The President's National Strategy on 5G spells out the details provided in COA 3, with the added exception to allow Chinese vendors that meet US security requirements. This caveat opens the door for Chinese vendors but keeps America in control of deciding whether the equipment meets its requirements to maintain national security. National security is the highest priority with this COA to protect its citizens' information, private sector data, and sensitive encrypted government information that rides on the same networks.

Is this COA acceptable to the nation's people?

The American people are concerned with their privacy and do not want their personal information stolen. An opposing view of this is that American citizens may contest the slow rollout of 5G across the country, which may have been alleviated by the integration of Huawei technologies. Overall, most US citizens do not care which vendor equipment is used on their phone networks, as long as the networks are running smoothly and secure from hacking attempts.

Is this COA acceptable to US Business?

US Businesses have a responsibility to keep their sensitive information protected from unauthorized intrusion. This COA makes network security its top priority with an option for Chinese vendors meeting strict security requirements. Any actions taken to minimize the threat of hacking is welcome by US businesses. The use of Chinese vendors has the potential to lower overall costs to customers from carrier installation savings.

Is this COA acceptable to allies and partners?

This COA maintains the same level of security as COA 1 but allows for Chinese vendors that meet strict security requirements. America still maintains the same level of national security as with COA 1, as few Chinese vendors would meet or exceed the established security criteria. Countries that allow HRV onto their networks should not have any issues communicating with America and its increased network security.

Is this COA acceptable to the WTO?

The WTO is an international organization that establishes and enforces international trade rules.[183] The organization strives for lowering trade barriers, including customs and tariffs, and eliminating unfair, discriminatory methods to reduce the importation of foreign products. This COA's willingness to engage and allow Chinese vendors supports a policy of international cooperation, engagement, and free trade, which aligns with WTO policy and guidelines.

[183] World Trade Organization, "What Is the WTO?"

Suitability

Will this COA maintain national security?

In this COA, America developed the equivalent of the UK's NCSC. This agency develops security standards for vendors to meet. If a vendor's products do not meet the security criteria established by the agency, its products are prohibited. The NCSC equivalent also works with other government and private companies to identify existing vulnerabilities and share their findings with other organizations.

Does this COA advance the nation's networks to 5G?

America already has 5G in place across the country. The vendors are available to provide the telecommunication equipment to spread 5G to all parts of America. Capable, qualified staff is expanding through government apprenticeship programs. Rural areas may receive 5G last, but the capability to reach these areas in the next few years exists.

Is this COA able to be implemented by allies and partners?

This COA is similar to the strategy used in the UK, but with a more stringent level of security criteria that must meet every requirement to be allowed for use on American networks. America still maintains the same level of national security as with COA 1, as few Chinese vendors would meet or exceed the established security criteria. Apart from Australia, which is even more strict when it comes to accepting HRV, allies, and partners would find this acceptable. Countries that allow HRV onto their networks should not have any issues communicating with America and its increased network security.

Does this COA use the nation's strengths effectively?

President Trump still encourages the growth of 5G through the free-market, private sector development but uses several governmental organizations to establish standards and eliminate roadblocks that may decelerate growth. America's National Strategy for 5G document provides guidance for both government and the public sector to follow. America is using its strengths effectively with this COA.

With the establishment of a cybersecurity agency and 5G International Security Council, this would increase the overall effectiveness of the COA and the ability to establish shared security practices and standards globally. These two new agencies would go far in establishing security standards in America and internationally. The cybersecurity agency would also help public and private companies in ensuring their networks are correctly configured to minimize vulnerabilities to cyber-attacks.

FAS Conclusion

COA 3's blended solution took the baseline strategy of COA 1 and blended in some aspects of COA 2 and adding recommendations from the Trilateral Cyber Security Commission's NSS for 5G report. Through the analysis of the previous 2 COAs and the concerns identified by the author, the focus of COA 3 was to develop a strategy that alleviated some of these concerns. Ideally, the COA addresses the concerns of the previous two COAs and minimizes negative findings.

This COA built a new NCSC-type agency to alleviate the concerns found in COA 1. This agency performs vulnerability assessments and establishes strict security standards. Any vendor desiring to sell its equipment in America must meet these strict security criteria. This agency would also work with private, public, and governmental

agencies to build, collect, and share findings and best practices help eliminate vulnerabilities. Last, the agency could provide a public website that supports and provides a centralized repository of information and guidance to assist network engineers expediently.

Internationally, the establishment of a 5G International Security Council would increase international 5G coordination. This council would hold responsibilities such as coordinating security baselines for participating members to review risks of foreign 5G vendors, sharing technical standards to assess security risks of vendors and the risk assessments of each, and developing consensus on vendors not meeting international security standards.[184] A commission involving international participation would provide a smooth way to develop international standards and ensure vendor equipment considered high-risk isn't allowed in networks on a global basis to increase international security.

Last, workforce availability is an area that carriers have concerns. This COA increases the capability of the Department of Labor developed the Telecommunications Apprenticeship Program to aid carriers with meeting their requirements. This program will provide more qualified apprentices to carriers deploying 5G. Ultimately, the rollout of 5G would occur on a faster timeframe with the elimination of the limited qualified workforce bottleneck.

[184] Trilateral Cyber Security Commission, "National Security Strategy For 5G: Findings & Recommendations on Meeting the 5G Challenge," 25–26.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

Conclusion

COA 3, the blended solution, provides the most effective solution to move forward with 5G deployment. The baseline of this strategy is pulled from the U.S. COA 1 strategy, with improvements extracted from the UK's solution. National Security is still maintained in this solution, while also appointing government bodies to take up national responsibilities for network security and 5G improvements. Additionally, an option to do business with Chinese vendors is a possibility in this solution.

President Trump's containment strategy that banned Chinese telecommunication equipment does provide the best national security for the nation. By keeping its equipment limited to trusted vendors from low-risk countries, it minimizes the risk of illegal intrusions. There is an adequate number of trusted vendors to deploy 5G across the nation while maximizing national security effectively.

Internationally, there is pressure to play fairly with the WTO guidelines and allow all Chinese products into America. Other countries bent to this pressure and the potential for Chinese trade retaliation by allowing Huawei products onto their networks. The UK feels confident in its ability to offset the threat of backdoors by limiting HRV equipment to non-core networks.

There is historical evidence of Huawei and other Chinese vendors having ties to the CCP. The Chinese government demonstrated successful cyber-hacking that led to the theft of billions of dollars of American IP and government employee personal data. Huawei regularly resorted to efforts illegal activities by stealing American IP to advance

its technologies. The book *Unrestricted Warfare*, published in China in 1999 and written by two senior officers of the PLA, calls for using unrestricted warfare against America because strong countries make the rules while China breaks them to exploit loopholes.[185] The mindset and historic occurrences show the government of China and its companies will do whatever is necessary to gain an advantage, including resorting to illegal activities. Based on the existing evidence, Huawei's promise to never share a country's information with the PLA means nothing.

Through the assessments accomplished in chapter 4, where America's strategy to deploy 5G (COA 1), and the UK's strategy for 5G deployment (COA 2), the analysis did find some shortcomings to each country's strategy. COA 3 attempted to blend actions from the previous two COAs to build an acceptable strategy that used the strengths of each country's implementation while bridging improvements over the concerns found from the analysis. Harry Yarger's book *Strategic Theory for the 21st Century*, provided a structured methodology to assess the FAS of each COA. To provide commonality between all of the COAs before the FAS assessment, the Prague Proposals supplied common LOEs for 5G rollouts. These two codifications were essential to present the information in an organized manner and effectively apply the assessment to determine where issues lay in each of the COAs.

America's existing 5G strategy provided a superior solution to ensure its national security. After collecting data from the literature review and America's National Strategy

[185] Liang Qiao and Ziangsui Wang, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, February 1999), 2, http://www.terrorism.com/documents/unrestricted.pdf.

on 5G publication, the building of LOEs and the FAS analysis identified concerns. While the COA passed the FAS analysis, it helped to identify issues that need addressing to improve the overall rollout of 5G. The US strategy lacks an established agency to perform vulnerability assessments and ensure vendor equipment passes security criteria. Additionally, there is no agency to confirm the authenticity of equipment to minimize the risk of tampering. Carriers are worried they lack sufficient trained staff to keep up with the quick deployment of 5G. Last, it is unknown how much pressure the WTO will apply to America for citing national security in its ban of Huawei and other Chinese vendors.

The UK's national strategy for 5G rollout addresses some of the concerns found in America's strategy. Still, there are concerns regarding the effectiveness of allowing HRVs onto its network and minimizing Chinese cyber-attacks. America stressed the need for allies not to allow HRV equipment onto their networks. Only Australia and Japan took heed, while others allowed HRVs onto non-core segments of the network, such as the UK. There is a concern that intelligence sharing between allies could be reduced if countries banning HRVs have apprehensions regarding sensitive data capture from HRV equipment on allied networks. The UK's NCSC believed it could effectively control the threats from HRV telecommunication equipment. Still, the UK Parliament objected to the perceived sacrifice of security to reduce pressure or retaliation from China.

COA 3 attempted to build a strategy that used America's solution as the baseline while integrating portions of the UK 5G strategy and additional findings from the Trilateral Cyber Security Commission's NSS for 5G document. Taken from the UK's strategy, a new NCSC-type agency performs vulnerability assessments and established strict security standards for all telecommunication vendors to meet. The establishment of

a 5G International Security Council would increase international 5G coordination and development of international security standards.[186] These international security standards would allow vendors to develop hardware and software solutions that meet this international criterion, thus simplifying equipment availability to countries that recognize this global measure. The Department of Labor's apprenticeship program is shifted into high gear in this COA to provide the needed staff to deploy. Open-source software is recommended to standardize interfaces, improve interoperability, and provide the added value of hobbyists continuously assessing software for vulnerabilities and enhancements. Last, this COA allows an open door for Chinese vendors if they can meet strict security criteria and meet all the concerns of the House Intelligence Committee. America controls the criteria for vendor acceptance, so national security is still maintained. This move also reduces the pressure from the WTO in America's ban on Chinese vendors.

In closing, America's national strategy for 5G assessment had minor concerns identified during the analysis. COA 3 does provide improvements to America's overall 5G strategy to improve on communication and the ability to expedite rollout with the increased staff provided via the Department of Labor's plan, maintaining national security, while also considering Chinese vendors that meet strict US criteria.

Recommendations

There was tremendous difficulty by the author in developing an accurate picture of America and the UK's rollout of 5G. The major issue encountered was that these

[186] Trilateral Cyber Security Commission, "National Security Strategy For 5G: Findings & Recommendations on Meeting the 5G Challenge," 25–26.

strategies are in a state of continuous flux. America's National Strategy on 5G was released 30 days before the completion of this thesis. A great follow-up to this thesis would be to gauge its accuracy in a few years after national strategies solidify, and each country is in the last stages of 5G rollouts.

BIBLIOGRAPHY

Adamowski, Jaroslaw. "US, Polish Presidents Sign Pact to Boost American Military Presence in Poland." *DefenseNews*. Last modified September 24, 2019. https://www.defensenews.com/global/europe/2019/09/24/us-polish-presidents-sign-pact-to-boost-american-military-presence-in-poland.

Allison, Graham. *Destined for War: Can America and China Escape Thucydides's Trap?* Boston, MA: Houghton Mifflin Harcourt, 2017. Accessed February 15, 2020. https://www.amazon.com/Destined-War-America-Escape-Thucydidess/dp/1328915387/ref=sr_1_1?keywords=destined+for+war&qid=1581800692&sr=8-1.

Bailey, Julia. "5G Is the Next Big Thing in Mobile—But Are There Enough Service Techs to Build It?" Field Service Digital. Accessed May 7, 2020. https://fsd.servicemax.com/2019/10/10/5g-is-the-next-big-thing-in-mobile-but-are-there-enough-service-techs-to-build-it/.

Bainbridge. "From 1G to 5G: A Brief History of the Evolution of Mobile Standards." Last modified December 1, 2018. Accessed March 1, 2020. https://www.brainbridge.be/news/from-1g-to-5g-a-brief-history-of-the-evolution-of-mobile-standards.

Bell, Robert. "BCLP EU & Competition Law." EU Competition Law. Last modified May 17, 2018. Accessed April 10, 2020. http://eu-competitionlaw.com/greater-national-security-scrutiny-at-the-heart-of-new-uk-merger-control-reforms/.

Bennhold, Katrin, and Jack Ewing. "In Huawei Battle, China Threatens Germany 'Where It Hurts': Automakers." *The New York Times*, January 16, 2020, sec. World. Accessed March 30, 2020. https://www.nytimes.com/2020/01/16/world/europe/huawei-germany-china-5g-automakers.html.

Borghard, Erica, and Shawn Lonergan. "The Overlooked Military Implications of the 5G Debate." Council on Foreign Relations. Last modified April 25, 2019. Accessed March 11, 2020. https://www.cfr.org/blog/overlooked-military-implications-5g-debate.

Burgess, Matt. "The UK Just Approved Huawei 5G Equipment. Here's Why." *Wired UK*, January 28, 2020. Accessed March 21, 2020. https://www.wired.co.uk/article/uk-5g-network-huawei.

Carlin, John, and Garrett Graff. *Dawn of the Code: America's Battle Against Russia, China, and the Rising Global Cyber Threat*. New York, NY: Hachette Book Group, 2018.

Cheng, Roger. “Huawei’s Legal Troubles Take a Twist with T-Mobile’s Torture-Test Robot.” *CNET.* Last modified January 29, 2019. Accessed March 21, 2020. https://www.cnet.com/news/how-a-torture-test-robot-figures-into-the-legal-assault-on-huawei/.

Cricks, James. Review of *Destined for War: Can America and China Escape Thucydides’s Trap?*, by Graham Allison. Washington, DC: National Defense University Press, 2017. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-87/jfq-87_101-102_Cricks.pdf.

Cybersecurity and Infrastructure Security Agency. “Overview of Risks Introduced by 5G Adoption in the United States,” n.d. https://www.cisa.gov/sites/default/files/publications/19_0731_cisa_5th-generation-mobile-networks-overview_0.pdf.

DeGrasse, Martha. “Which Vendor Leads in 5G Contracts?” FierceWireless. Last modified September 13, 2019. Accessed April 8, 2020. https://www.fiercewireless.com/5g/which-vendor-leads-5g-contracts.

Demchak, Chris, and Yuval Shavitt. “China’s Maxim - Leave No Access Point Unexploited: The Hidden Story of China Telecom’s BGP Hijacking.” Scholar Commons, 2018. https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1050&context=mca.

Department for Digital, Culture, Media & Sport. “Next Generation Mobile Technologies: A 5G Strategy for the UK.” GOV.UK. Last modified March 8, 2017. Accessed April 9, 2020. https://www.gov.uk/government/publications/next-generation-mobile-technologies-a-5g-strategy-for-the-uk.

Doffman, Zak. “Huawei Goes To Court To Fight ‘Illegal’ Ban As China Decides On Softer Approach.” *Forbes*. Last modified May 29, 2019. Accessed March 8, 2020. https://www.forbes.com/sites/zakdoffman/2019/05/29/huawei-goes-legal-again-as-china-tells-its-officials-and-media-back-off-the-u-s/#38e81d7f6b3b.

The Economist. “Security Alert - CFIUS Intervenes in Broadcom’s Attempt to Buy Qualcomm.” Last modified March 8, 2018. Accessed March 11, 2020. https://www.economist.com/business/2018/03/08/cfius-intervenes-in-broadcoms-attempt-to-buy-qualcomm.

Executive Office of the President. “Securing the Information and Communications Technology and Services Supply Chain.” *Federal Register*. Last modified May 17, 2019. Accessed April 7, 2020. https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain.

Fernyhough, James. “Australia’s Huawei Ban on Shaky Ground at WTO.” *Australian Financial Review*. Last modified April 15, 2019. Accessed March 21, 2020. https://www.afr.com/policy/foreign-affairs/australia-s-huawei-ban-on-shaky-ground-at-wto-20190415-p51ebi.

Fingas, Jon. “China, Huawei Propose Internet Protocol with a Built-in Killswitch.” *Engadget*. Accessed March 30, 2020. https://www.engadget.com/2020-03-30-china-huawei-new-ip-proposal.html.

Fisher, Tim. “When Is 5G Coming to the US? (Updated for 2020).” *Lifewire*. Last modified April 13, 2020. Accessed April 8, 2020. https://www.lifewire.com/5g-availability-us-4155914.

Freedberg Jr., Sydney J. “Elon Musk: ‘Radical Innovation’ Needed To Beat China Militarily.” *Breaking Defense*. Last modified February 28, 2020. Accessed March 11, 2020. https://breakingdefense.com/2020/02/elon-musk-radical-innovation-needed-to-beat-china-militarily/.

Gertz, Bill. “Chinese Telecoms Spy for Beijing through Computer Equipment, House Intelligence Committee Leaders Say.” *Washington Free Beacon*. Last modified September 14, 2012. Accessed March 2, 2020. https://freebeacon.com/national-security/beijings-backdoors-2/.

———. *Deceiving the Sky: Inside Communist China’s Drive for Global Supremacy*. New York, NY: Encounter Books, 2019.

Glosserman, Brad. “Huawei and the Realities of the 5G World.” *The Japan Times*. Last modified February 3, 2020. Accessed March 22, 2020. https://www.japantimes.co.jp/opinion/2020/02/03/commentary/world-commentary/huawei-realities-5g-world/.

Government of the Czech Republic. “Prague 5G Security Conference Announced Series of Recommendations: The Prague Proposals.” Last modified March 5, 2019. Accessed April 4, 2020. https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/.

Greene, Jay, and Shara Tibken. “Lawmakers to U.S. Companies: Don’t Buy Huawei, ZTE.” *CNET*. Last modified October 8, 2012. Accessed March 2, 2020. https://www.cnet.com/news/lawmakers-to-u-s-companies-dont-buy-huawei-zte/.

Headquarters, Department of the Army. Army Doctrine Publication 5-0, *The Operations Process*. Washington, DC: Government Printing Office, July 2019.

———. Field Manual 6-0, *Commander and Staff Organization and Operations.* Washington, DC: Government Printing Office, May 2014.

Hendel, John. “The Big Barrier to Trump’s 5G America.” *POLITICO*. Last modified December 29, 2019. Accessed March 30, 2020. https://www.politico.com/news/2019/12/29/big-barrier-trump-5g-america-089883.

Kahn, Michael, and Jan Loptaka. “Western Allies Agree 5G Security Guidelines, Warn of Outside Influence.” *Reuters*, May 3, 2019. Accessed April 4, 2020. https://www.reuters.com/article/us-telecoms-5g-security-idUSKCN1S91D2.

Lee, John. “5G and Huawei: The UK and EU Decide.” *The Diplomat.* Last modified February 15, 2020. Accessed April 10, 2020. https://thediplomat.com/2020/02/5g-and-huawei-the-uk-and-eu-decide/.

Maizland, Lindsay, and Andrew Chatzky. “Huawei: China’s Controversial Tech Giant.” Council on Foreign Relations. Last modified February 12, 2020. Accessed March 3, 2020. https://www.cfr.org/backgrounder/huawei-chinas-controversial-tech-giant.

Maloof, Michael. “China: ‘Pervasive Access’ to 80% of Telecoms.” *WND*. Last modified July 1, 2012. https://www.wnd.com/2012/07/chinese-have-pervasive-access-to-80-of-worlds-telecoms/.

McCann, John. “5G in the UK: Everything You Need to Know.” *TechRadar*. Last modified February 14, 2020. Accessed April 11, 2020. https://www.techradar.com/news/5g-uk.

Moran, Theodore. *Three Threats: An Analytical Framework for the CFIUS Process*. Washington, DC: Peterson Institute for International Economics, 2009.

Mu-Hyun, Cho. “Samsung to Supply 5G Network Solutions to Spark New Zealand.” *ZDNet*. Accessed March 30, 2020. https://www.zdnet.com/article/samsung-to-supply-5g-network-solutions-to-spark-new-zealand/.

National Cyber Security Centre. “NCSC Advice on the Use of Equipment from High Risk Vendors in UK Telecoms Networks.” Last modified January 28, 2020. Accessed March 21, 2020. https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks.

O’Dea, S. “Share of People with iPhone in the US 2014-2021.” Statista. Last modified February 27, 2020. Accessed April 8, 2020. https://www.statista.com/statistics/236550/percentage-of-us-population-that-own-a-iphone-smartphone/.

Office of the Secretary of Defense. *Annual Report to Congress: Military and Security Developments involving the People’s Republic of China 2019*. U.S. Department of Defense. Accessed October 19, 2019. https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf.

Orinx, Kimberly, and Tanguy Struye de Swielande. “A Chinese Fox against an American Hedgehog in Cyberspace?” *Military Review* 100, no. 5 (2019): 10.

Pillsbury, Michael. “Michael Pillsbury.” michaelpillsbury.net.

———. *The Hundred-Year Marathon: China’s Secret Strategy to Replace America as the Global Superpower*. New York, NY: Henry Holt and Company, LLC, 2015.

Plucinska, Joanna, Karol Witenberg, and Jack Stubbs. “Poland Arrest Huawei Employee, Polish Man on Spying Allegations.” *Reuters*. Last modified January 11, 2020. Accessed March 12, 2020. https://www.reuters.com/article/us-poland-security/poland-arrests-huawei-employoee-polish-man-on-spying-allegations-idUSKCN1P50RN.

Porter, Jon. “‘Hidden Backdoors’ Were Found in Huawei Equipment, Reports Bloomberg.” *The Verge*. Last modified April 30, 2019. Accessed March 2, 2020. https://www.theverge.com/2019/4/30/18523701/huawei-vodafone-italy-security-backdoors-vulnerabilities-routers-core-network-wide-area-local.

Qiao, Liang, and Ziangsui Wang. *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House, February 1999. http://www.terrorism.com/documents/unrestricted.pdf.

Robertson, Jordan, and Michael Riley. “China Used a Tiny Chip in a Hack That Infiltrated U.S. Companies.” *Bloomberg*, October 4, 2018. Accessed March 1, 2020. https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.

Rogers, Mike, and Dutch Ruppersberger. *Investigative Report on the U.S. National Security Issues Posed by Telecommunication Companies Huawei and ZTE.* U.S. House of Representatives, Permanent Select Committee on Intelligence, October 8, 2012. https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=96.

Roper, Carl. *Trade Secret Theft, Industrial Espionage, and the China Threat*. Boca Raton, FL: CRC Press, 2014.

Rosemain, Mathieu, and Gwenaelle Barzic. “Exclusive: France to Allow Some Huawei Gear in Its 5G Network - Sources.” *Reuters*, March 13, 2020. Accessed March 30, 2020. https://www.reuters.com/article/us-france-huawei-5g-exclusive-idUSKBN20Z3JR.

Sanchez Nicolas, Elena. “EU Rules Leave 5G Networks Open for Huawei.” *EUobserver*. Last modified January 30, 2020. Accessed March 21, 2020. https://euobserver.com/science/147303.

Stern, Corey. “Goldman Sachs Says a Digital Healthcare Revolution Is Coming — and It Could Save America $300 Billion.” *Business Insider*. Last modified June 29, 2015. Accessed March 20, 2020. https://www.businessinsider.com/goldman-digital-healthcare-is-coming-2015-6.

Tobin, Meaghan. “Huawei Ban: Australia Isolated If UK Includes Chinese Firm in 5G.” *South China Morning Post*. Last modified April 26, 2019. Accessed March 22, 2020. https://www.scmp.com/week-asia/geopolitics/article/3007810/huawei-ban-australia-becomes-increasingly-isolated-among-five.

Tomas, Juan Pedro. “Huawei Opens Cybersecurity Center in Belgium.” *RCR Wireless News*, March 6, 2019. Accessed March 30, 2020. https://www.rcrwireless.com/20190306/5g/huawei-opens-cyber-security-center-belgium.

Trilateral Cyber Security Commission. “National Security Strategy For 5G: Findings & Recommendations on Meeting the 5G Challenge.” Trilateral Cyber Security Mission, December 2019. https://spfusa.org/wp-content/uploads/2019/12/TCSC-National-Security-Strategy-for-5G-Dec-2019.pdf.

Trump, Donald. “President Donald J. Trump Is Taking Action to Ensure That America Wins the Race to 5G.” The White House. Last modified April 12, 2019. Accessed April 8, 2020. https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-taking-action-ensure-america-wins-race-5g/.

———. “Presidential Memorandum on Developing a Sustainable Spectrum Strategy for America’s Future.” The White House. Last modified October 25, 2018. Accessed April 5, 2020. https://www.whitehouse.gov/presidential-actions/presidential-memorandum-developing-sustainable-spectrum-strategy-americas-future/.

US Army Command and General Staff College. “C203: Power and Strategy Slides” Presented at the C204: Power and Strategy Briefing, n.d.

US Department of State. “Deep Dive: How the U.S. Is Addressing 5G and Security,” n.d. Accessed April 7, 2020. https://www.state.gov/deep-dive-how-the-u-s-is-addressing-5g-and-security/.

US Government. “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.

Wittes, Benjamin. “John Carlin on ‘Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats’.” *Lawfare*. Last modified June 21, 2016. Accessed May 10, 2020. https://www.lawfareblog.com/john-carlin-detect-disrupt-deter-whole-government-approach-national-security-cyber-threats.

World Trade Organization. “What Is the WTO?” Accessed February 15, 2020. https://www.wto.org/english/thewto_e/thewto_e.htm.

Wright, Jeremy. “UK Telecoms Supply Chain Review Report.” Department for Digital, Culture, Media & Sport, July 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819469/CCS001_CCS0719559014-001_Telecoms_Security_and_Resilience_Accessible.pdf.

Yarger, Harry. “C205RA: Strategic Theory for the 21st Century: The Little Book on Big Strategy,” February 2006. http://www.StrategicStudiesInstitute.army.mil.