5-6-2021

What are the predictors of cyber power

Carter Bowman

What Are the Predictors of Cyber Power?

An Honors College Project Presented to

the Faculty of the Undergraduate

College of Arts and Letters

James Madison University

By Carter Bowman

May 2021

Accepted by the faculty of the Department of Political Science, James Madison University, in partial fulfillment of the requirements for the Honors College.

FACULTY COMMITTEE:

Project Advisor: Jon W. Keller, Ph.D.,

James Madison University

Reader: Yi X. Yang, Ph.D.,

James Madison University

Reader: Keith A. Grant, Ph.D.,

James Madison University

HONORS COLLEGE APPROVAL:

Bradley R. Newcomer, Ph.D.,

Dean, Honors College

PUBLIC PRESENTATION

This work is accepted for presentation, in part or in full, at James Madison University's Department of Political Science Honors Presentations (Zoom) on April 21st, 2021.

Table of Contents

- Acknowledgements …… Page 4
- Abstract …… Page 5

Chapter One: Introduction …… Page 6

- Context …… Page 6
- Why Now? …… Page 7
- Justification …… Page 9
- Methodology …… Page 9
- Looking Ahead …….. Page 10

Chapter Two: Literature Review …… Page 12

- Terms and Definitions …… Page 12
- Cyber Power …….. Page 15
- Factors that Enable a Rise in Cyber Power …… Page 19
  - Factor One: Economy ……..…… Page 21
  - Factor Two: Education …… Page 21
  - Factor Three: Espionage ……..…… Page 22
  - Factor Four: Immigration ..…….…… Page 22
  - Factor Five: Regime Type ……..….. Page 22
  - Factor Six: Preexisting Military Strength ……..…… Page 23
  - Factors Now Deemed Obsolete ……..……. Page 23

Chapter Three: The United States ……... Page 26

- Background ..…….. Page 26
- Economic Strength ……..…… Page 28
- Economic System ……..…..…… Page 31
- Education ……..……..…… Page 31
- Espionage ….…..…… Page 32
- Immigration …..…….…….…… Page 33
- Regime Type ….…….…..…….…… Page 35
- Preexisting Military Strength …..…….…….…… Page 36
- Factors that Inhibit Cyber Power for the U.S. …… Page 38

Chapter Four: China ……. Page 40

- Background ..…..…….…..…….…… Page 40
- Economic Strength …..…….…….…… Page 41
- Economic System ……...…..…… Page 42
- Education …… Page 43
- Espionage …… Page 44
- Immigration …… Page 45
- Regime Type …….…….. Page 47
- Preexisting Military Strength …..…….…….…… Page 48
- Factors that Inhibit Cyber Power for China …… Page 49

Chapter Five: Comparisons ……. Page 51

- Factor One: Economy ……..…… Page 51
- Factor Two: Education ……..… Page 53

- Factor Three: Espionage …… Page 54
- Factor Four: Immigration ..…… Page 55
- Factor Five: Regime Type ……..….. Page 56
- Factor Six: Preexisting Military Strength ……..…… Page 58
- Vulnerabilities ……. Page 58

Chapter Six: Conclusions …… Page 60

- Findings……..……..…… Page 60
- Research Qualifications ……...…… Page 61
- Future Research ……..……..…… Page 62
- Concluding Remarks …… Page 63

References …… Page 64

Acknowledgements

I would like to acknowledge my James Madison University Political Science thesis committee: Drs. Jon Keller, Edward Yang, and Keith Grant for their invaluable help throughout this process. Additionally, I would like to thank Jeffrey Ding, researcher at the University of Oxford's Future of Humanity Institute for his informal advising on this project.

Abstract

This thesis identifies the predictors needed to anticipate a rise in a state's national cyber power. Historically, national power measurements provide solid starting points but are not sufficient to rely on when assessing modern cyber power. Because of various factors such as an increase in globalization and reliance upon intelligence, factors that were once of paramount importance are now obsolete, and factors that had not been considered are now extremely important. By identifying the factors that matter most in predicting a rise in cyber power, future researchers have the tools to create a sophisticated metric by which to rank anticipated cyber development, and policymakers can use the information to develop a strategy to optimize efficiency in a domain necessary for national security.

Chapter 1: Introduction

Context

In an ever more globalized world, discussions of security are becoming a quintessential part of national governance. With more occurrences, increased severity, and lingering effects, cyberattacks are now listed among the United States' top security threats. According to a survey conducted by the Pew Research Center, 70% of Americans now view a cyberattack as a serious threat to national security (Stokes, 2014).

Former United States Secretary of Defense Leon Panetta pointed out the possibility of a "cyber-Pearl Harbor attack" back in 2012 (Bumiller, 2012). A comparison to such a tragic and devastating act helps to illustrate the urgency that various actors have placed on the development of a comprehensive cybersecurity apparatus. The world has already seen catastrophic damage done by the hands of hackers, from meddling in elections to stealing the utmost classified data. Similar to conventional terrorism, cyberattacks are detrimental because they can be perpetrated by small groups and organizations or entire nations. One advantage in comparison to traditional attacks is that cyberattacks often afford attackers the advantage of anonymity, just one of several reasons that a country or non-state actor might choose such an attack. A variety of issues surrounding cyberattacks have arisen over the years, such as how to classify them, how to proportionally respond, and how to identify the perpetrator. Juggling these variables has proven difficult for countries around the world, leading to instability in a domain that is in critical need of control.

This thesis attempts to identify the primary drivers and predictors of cyber power, fully defined on page eleven, examining several variables in an attempt to determine where relative

power lies throughout the progression known as the fourth industrial revolution (4IR). This fourth revolution references the rise in digital technology (Horowitz, 2018). In this discussion will be an in-depth analysis of the factors used to measure cyber power, the reliability of data, the factors that predict or cause a rise in cyber power, and more. However, an examination of the literature surrounding cyber power and capabilities more broadly is essential to the identification of factors that lend rise to cyber power.

This is an interesting time in the world because while there have been various power transitions in the past few hundred years, there has not yet been widespread power diffusion, or the rise in power of historically less powerful states and the loss of power in historically more powerful states, resulting in a power dynamic closer to an equilibrium. Nye argues that this is what is happening with cyber power. Because it is relatively easy and inexpensive for small states and non-state actors to attain cyber power, the battle among major players is more complicated than say nuclear issues were. Nye claims that governments are still undoubtedly the strongest actors, but other groups are now in the fight as well and should not be discounted (Nye, 2010). Because no identification currently exists of which factors enable a state to rise in cyber power, this thesis focuses on just that by looking at the two states which currently hold the largest portions of cyber power.

Why Now?

Today, the debate over the severity of cyber power and cyberattacks lies not in whether they *can* inflict legitimate harm, that is widely accepted to be true; rather, scholars often diverge when analyzing the likelihood of a major attack, and the best way to classify the strikes when they do occur. The main distinction that scholars draw is between cyberattacks and cyberwar.

Those who believe that cyberattacks are relatively benign are referred to as cyber-optimists. One such cyber-optimist, Rid, contends that the world is by no means destined for cyber war, and that no matter how violent a cyber attack might be, "cyberwar" cannot occur because it will not meet the three defining elements of war according to Carl von Clausewitz: violent character, or the loss of life and/or property; instrumental character, a means to an end; and political nature, requiring two political parties and a political goal (Rid, 2012). In this view, Rid does not deny the potential for horrendous attacks against nation-states; he just would never define such attacks as war. A large reason for his hesitation is that once a state classifies an attack as an act of war, there are certain protocols that must be enacted in a retaliatory response. Still, to date, there is disagreement over whether there should be retaliation, and if so, to what extent. This dilemma is further complicated by the uncertainty in identifying the perpetrators. Another writer who agrees that cyber threats are exaggerated is Gartzke. Like Rid, he sees the threat of a cyberattack as non-trivial. However, both scholars also recognize that high-magnitude attacks are rare. (Gartzke, 2019).

Opposite of the cyber-optimists who believe either that cyberwar is not a legitimate threat, or that the severity of these attacks is something that states are worrying too much about, Nye can be described as a cyber-pessimist, or one who believes that these attacks are real, imminent, and dangerous. Nye discusses not only a way in which one can measure cyber power, both qualitatively and quantitatively, but also the reasons for measuring cyber power, which include assessment of adversary capabilities, understanding comparative strengths, and identifying areas of weakness or vulnerability (Nye, 2010).

Similarly, Kello has put forth his own definitions for distinguishing between cyberattacks and cyberwar. Kello argues that if the effects of a cyberattack produce *significant physical destruction* or *loss of life*, the action can be labeled "cyberwar." While Kello is very much concerned with the threat and severity of cyberattacks, in his view, however, it is important to maintain a limited view of the word significant. With this in mind, the vast majority of cyberattacks cannot be classified as cyberwar. On the whole, however, Kello, because he is a cyber-pessimist, is often described as a threat-believer (Kello, 2013).

Justification

In this thesis, the major two players that will be discussed are the United States and China. This is because these two countries are currently leading the cyber-race, the United States, having always been a major player, and China rising to power over the past twenty years. Multiple theories will be discussed in this thesis as this is an attempt to understand not only the current state of affairs in terms of cyber power but also to look at how we got here. Therefore, a discussion of the security dilemmas and more will be discussed.

The global consensus on cyber power as it stands today is that the United States is still a world leader; although, China is not far behind (Voo et al., 2020). Because of this, it is necessary to examine what factors could have been used to predict this rise. In doing so, hopefully, a measure will emerge allowing future political scientists to accurately predict rises and falls in cyber power.

Methodology

There are multiple ways that one can measure power, but before that discussion of measurement can even arise, it is necessary to define power upfront. While recognizing that no

one definition of power exists, for this thesis, I will use the following definition of power, as given by Joseph Nye: “the ability to affect other people to get the outcomes one wants,” (Nye, 2012). This definition encompasses the intent of an aggressor, or influencer, as well as the capabilities that they possess. Those two metrics, intent (willingness) and capability (opportunity), are what researchers at the Belfer Center used to devise the National Cyber Power Index (Voo et al., 2020). The index examines factors such as spending, research, hardware, a willingness to act, and more. I will be using the same factors to analyze the relative cyber-power possessed by both China and the United States. One concession that the Belfer Center Paper on Cyber Power does make, and that I will regrettably make in my research as well, is that there is a lack of available and accurate data for some of the metrics I will attempt to use (Voo et al., 2020). As is qualified more in the conclusions chapter, some of the data that does exist could be, and likely is, falsified, so that will be taken into account as the process continues. My thesis contributes to this understanding by parsing out specific drivers of cyber power. My goal is that in identifying these predictors, policymakers will be able to make more informed decisions and future political scientists will be able to apply knowledge of these factors in two distinct manners. First, as I expand upon in the “Conclusions” chapter of this thesis, because this thesis looks retroactively at the United States and China, future research can focus on the future of cyber power in the United States and China. Second, I hope that researchers can use these factors to inform predictions regarding states outside of the United States and China.

Looking Ahead

It is known that the United States has been a world superpower since the second world war, filling that role even more so after the fall of the Soviet Union. However, in recent years,

China has risen as well, especially in terms of their cyber capabilities. Depending on the role that cyber technology plays in the coming years, American dominance could be called into question. With the United States so economically dependent on China today, it is unlikely to see any actions as destructive as all-out war occurring in the near future (World Economic Forum, 2019). Meanwhile, the Chinese government can act with impunity as there is no another party or democracy to hold the Chinese Communist Party (CCP) accountable. On top of that, the lack of privacy laws in China allows the government to attain much more information about its people and thus about international corporations.

As the literature continues to develop, I anticipate even more of an emphasis will be placed on the necessity to fund and devote resources to national cybersecurity. 4IR is becoming the path of the future, and investment is needed. However, part of the problem over the past twenty years has been a reluctance to fund these efforts in democracies such as the United States. This is in large part due to the need for public approval and a concept known as selectorate theory. Bueno de Mesquita, Smith, and Luo write that there are three groups in any political setting: the residents, the selectorate, and the winning coalition. The argument goes that regardless of regime type, there is always a group of people that those elected need to please in order to remain in power (Bueno de Mesquita, Smith, and Luo, 2014). The problem for democracies is that oftentimes, the elected officials are more beholden to residents than are leaders in authoritarian regimes. This is one area in which China has the potential to excel. The one-party state allows the Chinese government to make investments that they view as objectively important without concern for popular appeal, a luxury that American lawmakers cannot afford.

Chapter Two: Literature Review

Terms and Definitions

According to Valeriano and Maness, cyber conflict is the use of computational technologies with the intent to compromise an adversary's capabilities (Valeriano and Maness, 2015). Based on that definition, nearly any attempt to interfere with cyber capabilities could classify as cyber conflict. It is important to remember that this thesis examines cyber power, the ability and willingness to act and to deter enemies, not cyber conflict. These definitions are provided solely for context on the subject. In terms of cybersecurity, the United States federal government defines this more defensive term as "the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation," (Cybersecurity, 2020). Based on that definition, it follows that a cyberattack would be any attempt by a foreign state or non-state actor to compromise a communications system or information.

Interestingly, the severity of the attack can have a drastic impact on the way that it is classified within the literature surrounding cybersecurity. For instance, Kello argues that an attack can be labeled as "cyberwar" so long as it produces significant destruction or loss of life. However, Kello maintains a limited perception of the word "drastic," and therefore would not classify many attacks as cyberwar (Kello, 2013). For example, an attack to gather intel or steal intelligence would not classify as cyberwar whereas hacking into a nuclear energy site and exploding generators would qualify. Similar to how researchers look at militarized conflict in international relations (IR), by using the correlates of war militarized interstate disputes to

determine a state's power, a judgement of the cyber power of a state is made on the basis of the nature of historic cyberattacks.

A single definition of power does not exist amongst political scientists. Most definitions include some reference to an ability to influence others' behavior (Pevehouse, 2004). Nye analogizes power to the weather in that it is widely discussed, little understood, and next to impossible to predict (Nye, 2011). Understanding power as a malleable and complex concept is necessary for developing a comprehensive strategy with which to examine cyber dynamics.

In terms of measurement, the Composite Index of National Capability (CINC) measurement approach had historically been very well-recognized in the scholarly community as a great measurement tool to operationalize national power (Singer, Bremer, and Stuckey, 1972). However, with drastic changes in the twenty-first century such as electronic technologies and globalized trade, factors in the metric such as iron and steel production should no longer carry the same weight as military expenditure. Additionally, as mentioned earlier, military personnel is less important as the chance of large-scale war between states decreases. Various new components play into one state's ability to exert influence over another, such as economic standing and aggregate intelligence. Such factors contribute to a state's power insomuch as they allow that state to achieve desired outcomes through methods such as coercion and fear-mongering (Nye, 2012). For the purposes of this thesis, I will be examining both capabilities, or the ability to act, as well as power, the ability to influence other states. Further, if the targeted state fails to comply, then it becomes incumbent upon the aggressor to follow through with the attack to maintain their reputation in the international community (Beckley, 2018). The advantage that comes with having more power incentivizes states to desire as much of said

power as possible. For most military technologies, it is easy to discern what constitutes power in that domain. For example, the number of nuclear warheads that a state possesses is a quantifiable way to measure nuclear power (Nye, 2011). When assessing cyber power, however, the lines are not so clear. It is much easier to disguise cyber-capabilities and cyberattacks than it is a nuclear warhead (Buchanan, 2020). Many times, states are unaware that they were attacked, or even if they are, then the process of attributing that attack to another actor proves difficult due to the anonymity behind which an aggressor can hide (Rid, 2012). Additionally, it is much easier for states to disguise their cyber-capabilities than it would be to disguise conventional weaponry such as tanks or warships. It is for this reason that cyber weapons can heighten the threats between states, thus further increasing the need to advance cyber power.

This manifestation of a security dilemma, wherein one state's attempt to make themselves more secure antagonizes another state thus making the original state less secure, in a cyber domain is characterized by Buchanan as a cybersecurity dilemma (Buchanan, 2017). Ordinarily, the security dilemma indicates that an increase in capabilities that another state views as threatening can hurt the state who initially built up capabilities by encouraging the threatened state to build their own arsenal as well. Buchanan takes a different approach to the traditional dilemma: *every* advancement to a state's capabilities is defensive. While some technologies can assuredly be classified as solely defensive, Buchanan claims that no advancement can be solely offensive in cyber (Buchanan, 2017). This is interesting for the conversation on cyber power because if one accepts Buchanan's theory, then it seems as if states need not bolster spending in the way they have over the past twenty years. Yet, the need does exist for security, and while

increases in capabilities are oftentimes defensive, there are some increases, as will be examined later, that lend themselves to offensive attacks.

The security dilemma is a sort of arms race, but it is reactive to the other's change in capability. With cyber, however, that capability is not observable until used, unlike building new ships, raising troops, or assembling nuclear warheads on Cuba. Because of this inherent difference, the offense would have the advantage to strike more readily, a counter to Buchanan's argument, thus exacerbating the issue of the cybersecurity dilemma compared to the security dilemma (Jervis, 1978).

Cyber Power

As previously discussed, power needs to be thought of as a fluid and widely encompassing concept. With that in mind, cyber power, as a manifestation of power itself, also needs that same consideration. For this thesis, I will define cyber power as a combination of the two terms: the ability to both defend oneself through cybersecurity and to exert influence over others through the use of or threat of cyberattacks. This definition, similar to those provided for power more broadly, casts a wide net, allowing for many factors to influence cyber power. Of course, over the years there have been some notable attacks which do provide states with cyber power, such as the 2007 attack on Estonia's election, presumably conducted by Russia; the Office of Personnel Management attack on the United States, likely committed by the Chinese government; and the meddling in the 2016 U.S. presidential election is widely thought to have been Russia as well (Libicki, 2011). However, it is not by the number of attacks that a state's cyber power is calculated, but rather, it is based on three categories: intent, capability, and effect.

In using these three metrics to judge the cyber power of a given state, one can better understand how that power came about.

In terms of intent, there are four primary factors: goals, willingness, strategies, and legislation. First, there has to be a goal, or something that justifies the strike in the attacker's mind. More often than not cyberattacks have the goal of gathering intelligence through espionage (Valeriano and Maness, 2015). However, the goal could also be to compromise data centers, interfere in elections, or to undermine confidence in government security. Once a state has a clearly defined policy goal, a determination as to whether it will be willing to execute the necessary steps to the end of that goal is an important determination to make. Another point in need of consideration when assessing a state's intent is the rhetoric espoused by the state leaders and included in important state documents such as national strategies. At least for democracies, the legislation passed is the clearest and most consistent metric by which one can assess a state's action and direction in terms of its cyber policy (Buchanan, 2020). Meanwhile for authoritarian regimes such as China, an outcome-based examination proves more fruitful. This is because the legislation passed in a democracy is more likely reflective of the action that will follow than it is for non-democracies.

Equally as important a consideration as intent in measuring cyber power of a state is capability, or the capacity for a state to carry out strikes and to defend itself from attacks. In terms of capability, five primary factors will play a role in this assessment: spending, patents, limitations, personnel, and physical technology. These factors will all contribute to a composite measure of a state's cyber capability. Spending is an important quantitative measure because, without proper funding, advancing capabilities proves difficult unless a state resorts to espionage

as will be discussed in more detail later on. Patents are also an important consideration because they enable a state to control certain advancements and technologies, at least in a legal sense. Limitations are also critically important. For example, a democracy like the United States will be bound by privacy considerations for its citizens which authoritarian regimes such as the People's Republic of China (PRC) can largely ignore. As far as personnel is concerned, there are two factors that will be taken into account, the number of people dedicated to cybersecurity and the quality, or strength, that those individuals possess. Finally, the ability to manufacture physical, as well as digital, technologies is a necessary point to examine in any discussion of cyber power. Measurement of that physical technology is difficult to attain. Physical cyber technology can be the size of a microchip no larger than an infant's baby finger. Compared to the measurement of nuclear weapons, which were arduous to conceal, identifying physical cyber technology material is challenging to say the least (Bowman, 2020).

In both the intent and capability assessment, there are qualitative and quantitative measures to take into consideration. In examining both metrics, a holistic picture emerges that shows where the balance of power lies between the United States and China, and how that balance has changed over time. Future research might use the metrics that I have identified to establish a metric by which to judge the anticipated rise in state cyber power.

Understanding the belief that threats are real and imminent, Lindsay has recognized that the Chinese government has become a serious threat over the past couple of decades (Lindsay, 2014). While demonstrating the potential threat they may pose, Lindsay is also cautious in his claims, recognizing that the availability of reliable data is scarce. While he has focused primarily on China's rise in cyber power, Lindsay has also done work on specific case studies of various

attacks with his most well-known work being about Stuxnet, a malicious computer worm discovered in 2010 that allowed access to nearly a dozen countries (Lindsay, 2014).

While Lindsay has done a deep dive into Stuxnet and a few other specific cases, arguably the most investigative person to study cyberattacks and failed attacks is Buchanan. Having published multiple documents regarding national security; coming up with a cybersecurity dilemma theory, which is more or less a manifestation of the security dilemma in the cyber-medium; and most recently writing *The Hacker and the State*, Buchanan has proven himself to be both a committed and diverse player in the quest for understanding cyberattacks and their implications (Buchanan, 2020).

Two other researchers, Garfinkel and Dafoe write about measures of offensive and defensive capabilities as they pertain to cyber power (Garfinkel and Defoe, 2019). These political scientists distinguish between two types of technological advancement: qualitative, or the invention of some new technology, and quantitative, which as the name suggests, is the ability to produce more of the technology that already exists. According to these scholars, a cyberattack, even if not classified as cyberwar, could cripple the American economy or shut down military defense systems necessary to maintain homeland security. This damage could qualify such an attack as meeting Kelly's criteria of large-scale destruction necessary for classification as cyberwar. The interesting and unexpected finding of their research is that as cyber technology becomes more prevalent and more advanced, the balance of power will begin to shift from the current state of affairs, an obvious offensive advantage, to a defensive one (Garfinkel and Dafoe, 2019). This research is based on the idea that new technologies generally favor the offense because defenses for those attacks have yet to be developed. As the defensive capabilities catch-

up to the offensive attacks, and the attack severity reaches diminishing returns on development, the defensive advantage grows.

Despite continued disagreement as to whether cyberattacks could constitute a serious threat and thus warrant a sophisticated response, the paradigm has shifted in recent years to favor threat-believers. Articles published after the Chinese released the "AI Dream" in 2017 have overwhelmingly leaned toward cyber-pessimism. This is because in the AI Dream, the Chinese government set forth a plan to become the world leader in artificial intelligence (AI) by 2030. In response, the United States decided to bolster its own research and development (R&D) by devoting more funds and resources to cyber development. While AI and cyber are by no means synonymous, there is some overlap, and that overlap is projected to grow in the coming years as technological applicability advances. Moreover, even throughout the early 21st century, the world has already witnessed an enormous increase in the number and severity of attacks being levied primarily on states. For a spectacular graphic of the prevalence of cyber attacks, please check out the interactive Cyber Threat Map.[1] These continued attacks coupled with tactics such as compulsion, fear-mongering, coercion, and more are the reason that a discussion of how a state comes to obtain cyber power is critical (Nye, 2011).

Factors that Enable a Rise in Cyber Power

Through the use of the case studies of the United States and China, I argue that there are identifiable factors that contribute to a state's ability to increase its net cyber power. Prior to doing so, an exploration is needed into what factors have historically been known to either cause an increase in cyber power or to be correlated with an increase in cyber power. For all of these

[1] https://www.fireeye.com/cyber-map/threat-map.html

metrics, the process can be applied to power more broadly understood in terms of the ability to achieve desired outcomes. Because the instances of rises and falls in cyber power are rather limited, a large portion of the theory and analysis from which I will need to draw relates to the proliferation of other technologies and military arsenals. I will briefly introduce the factors here before diving deeper into the applications and implications of such measurements during the individual case studies. The literature surrounding a rise in technological and military power illuminates many factors that may be used to predict an increase in power, but I have chosen six that directly relate to cyber power. When examining these factors, one can classify them into two camps: direct and indirect. A direct factor is one which directly leads to more cyber power. An indirect factor, on the other hand, is one that does not necessarily impact cyber power but is directly correlated with cyber power success. Both measures are useful in the assessment of rises in cyber power because they can both be used as predictors for future rises. Using the case studies of the United States and China, I identify the means by which direct and tangential factors translate into cyber capability which can then be used to form a theory of cyber power. This thesis will enable other researchers to have the metrics by which to predict future rises and falls in state cyber power.

Also included in this section are factors that once had a tremendous impact on military development, but now, for some reason, appear to be obsolete. These factors include possession of territory with natural resources and natural resources. While these factors could impact the attainment of cyber power, it looks unlikely that they would. Since 2006, the GlobalFirepower (GFP) has been a measurement of military strength based on several factors including, but not limited to, manpower, equipment, natural resources, finances, and geography (Global, 2020).

While natural resources and manpower are both present in this assessment, the cyber realm obfuscates some of these concepts. By developing technologies capable of emulating human thought and action, artificial intelligence (AI) technology can replace human capital at an exponential rate (Leung, 2019). Similarly, when dealing with coding computer language, education is far more important than a factor such as natural resources.

Factor One: Economy

The status of state power has often been measured by gross domestic product (GDP). While there are several more specific metrics by which to judge a state's economic well-being, Liu and others argue that state power correlates more strongly to a raw measure of GDP than it does any other economic measurement (Liu, 2018; Heo and Tan, 2001; Weede, 1984). For this reason, my analysis of economics as an indicator of future cyber power will focus on GDP. Beckley (2010) found that the states with the best economies tend to fare better militarily because they have the ability to develop more and better technology than their adversaries. Of course, this causal reasoning is contingent on actually using the strong economic circumstances to fund advancements in military technologies (Beckley, 2010).

Factor Two: Education

Second, education is unarguably an essential driver of state power (Kramer, et al., 2009; Nye, 2010; Buchanan, 2020; Voo et al., 2020). In terms of military technology, the largest example that can be drawn on is nuclear weapons. Some theorists, such as Nye, have drawn stark parallels between nuclear weapons and cyber power. One of those parallels is the education necessary to develop such sophisticated technologies. Nye argues that those who can develop these capabilities are advantaged tremendously because of the devastating impact of an attack

and thus the ability to influence others out of fear (Nye, 2011). An investment into science, technology, engineering, and mathematics (STEM) explains why both the United States and China have been successful in cyber power advancement, as will be examined in later chapters.

Factor Three: Espionage

The rather benign discussion of education transitions nicely into a more hostile one of espionage. There are two ways to develop new technologies: to create them or attain them through a technology transfer. The transfer can be a peaceful transaction of technologies or technological theft in the form of espionage (Hannas and Chang, 2019; Segal, 2017). The difficulty with using espionage as a primary driver for technological development is that surpassing the state from which you are stealing is next to impossible (Segal and Gerstel, 2019).

Factor Four: Immigration

More now than ever, the ability to bring in foreign talent for development purposes is becoming an important factor in power. In addition to fostering education talent at home, foreign acquisition of knowledge is a critical factor in development. Interestingly, this has been a burden for the United States over the past twenty years because, when combined with the risk of espionage, governments are wary of accepting foreign talent, especially from adversaries (Arnold et al., 2019, Cybersecurity Workforce, 2021). While the object of foreign talent acquisition is appealing due to the expertise, there is also great risk associated with the decision to recruit foreign talent for the purpose of national security (U.S. Senate, 2019).

Factor Five: Regime Type

Historically, regime type has been a factor allowing states to develop technologies at various rates. Democracies incentivize the creation of new technologies in the private sector

more than a one-party, authoritarian regime that oversees and surveils their citizens to gather much more data. These pros and cons are reported to cancel out today, leading to strength under both regimes (Stier, 2017, Slater and Fenner, 2011; Leeds and Davis, 1999; Goldsmith, Chalup, and Quinlan, 2008). It is predicted, however, that as private sector advancement of cyber technology continues, this could shift the power to one regime or the other. An authoritarian government could demand access to that technology from the private companies whereas the free-market economies might develop the technology at a faster rate. Of course, this analysis overlooks the information released by Edward Snowden in 2013 which exposed the U.S. government for tapping into citizens' private devices in the name of national security, but that discussion will be left for another paper (Coyne, 2019).

Factor Six: Preexisting Military Strength

A strong military tends to build on itself. Tillis argues that military strength is the most important factor when considering national power in a postindustrial age (Tillis, 2000). This is because with a top-tier military comes the ability to exercise offensive attacks as well as defend oneself. Additionally, an advantage in military capabilities today is a powerful predictor of future technological advancement. O'Hanlon argues that current technological advantages enable states to develop at exponentially faster rates than their less advanced counterparts (O'Hanlon, 2020).

Factors Now Deemed Obsolete

To begin this section, it is important to note that I may find in the case studies that these factors do impact the rise of cyber power on a national scale; however, this seems unlikely. To start, having territory with materials necessary to develop weapons was critical in times such as World War II when metal ore was essential to the development of arms, vehicles, and nuclear

weapons. When examining cyberattacks though, such materials are largely irrelevant. Yes, of course, to exercise an attack one needs some hardware to create and launch the code, but that is so widely available that the factor of having those natural resources will likely not play a role in the advancement of cyber power. Moreover, trade in the 21st century is essential for all world powers (Hoekstra and León, 2019). While things such as tariffs and sanctions inhibit trade, they do so minimally. Countries are forced to trade the materials they produce or have access to in an effort to maintain their economic status, and as a result, possession of territory with key resources is not essential to the development of cyber technology.

Similar to the previous need for natural resources, a state's population is no longer a consideration when looking at advancement in cyber power. In a large-scale ground war such as those seen in the twentieth century, the more bodies a country had, the more powerful they were (Global, 2020). In the modern era of cyberattacks, there are two reasons why this is not the case: cyber war is limited in nature and cyberattacks do not require ground soldiers. Based on the argument that states are interdependent agencies who rely on one another for things like trade, it seems only rational that one such state would not want to annihilate an adversary that they rely upon. It is for this reason that cyber war is largely limited in nature (Allen and Chan, 2017).

Another factor that was once largely indicative of a rise in technological capabilities is the number and quality of patents. Patents, or licenses for specific technologies, was an indicator that a state either has or will have great cyber power (Paarlberg, 2004). However, because of cyber espionage, and the ability to legally and illicitly trade or steal technologies, this factor is no longer as significant. Additionally, the patents themselves can be rather weak. For example,

China produces more patents than any other state, but their patents are often less substantive than those produced by the United States (Ding, 2018).

Chapter Three: The United States

Background

The rise of America's cyber power dominance was predicated on its rise as a world power. Coming out of the Cold War, the U.S. was undoubtedly a leader in the international community no matter which measurement was used: soft power, economic strength, military security, ability to attract immigrants, etc. (Deudney and Ikenberry, 1991). This position as a world power not only allowed the U.S. to unilaterally shape the world in its image, but the power also enabled the U.S. to develop new technologies at rates far superior to its adversaries and therefore lead the world in innovation, research, and technology (Manyika, McRaven, and Segal, 2019). An investigation into the factors that enable such a rise in cyber power can be useful to future studies and attempts at forecasts and predictions. For this reason, I have selected the United States as the first of two case studies. By serving as an ideal case, or the top of the line example, the U.S. allows this investigation a point of comparison. In an attempt to identify the driving forces behind this development, I have confirmed previous hypotheses of predictors in power increases, such as a strong economy and military, but I have also discovered additional factors that drive cyber development but did not necessarily play the same role with previous technologies.

According to the original national cyberstrategy document, entitled The National Strategy to Secure Cyber Space, put forth by the Bush Administration, there are three strategic objectives: preventing cyberattacks; reducing national vulnerability; and minimizing damage and recovery time (Strategy, 2003). The interesting fact about these objectives is they are all defensive in nature. This is profound because looking back retroactively at the United States policy, the U.S.

has invested much more research and development (R&D), time, and resources, towards what might appear to be offensive cyber capabilities, but are actually used primarily in a defensive manner. The idea behind perception in using public statements/documents to determine intentions is one inherent limitation of research into democracies. There is undoubtedly a difference between what is stated and what happens. The U.S. government gets around this by classifying such acts under counterintelligence and cyber espionage. The difficult part for an outside party is identifying where to draw the line between gathering intelligence for offensive and defensive purposes.

The United States has perpetrated dozens of high-level cyberattacks, some of which have likely yet to have been recovered. However, cyberattacks for the United States are a less valuable topic to discuss than its vulnerabilities. According to the aforementioned Belfer Center study, the United States already holds the title of the most advanced state in the world in terms of cyber power. Because of this strength, they are seldom able to use cyberattacks to gather intelligence relating to further development of capabilities, but they do exercise that power to enhance their ability to control the international stage. Nonetheless, all of this is to say that the United States, due to its colossal size and enhanced capabilities, is more susceptible to attacks than any other state, despite all of its advancements (Specops, 2020). This is why an important discussion of some major cyberattacks that have hurt the United States is critical.

One attack that the media did not report much of during the time of its occurrence, be it because of government pressure or a lack of knowledgable intel, is the. Office of Personnel Management (OPM) attack that occurred in 2015. This attack can likely be attributed to a Chinese hacking organization using spear-phishing techniques to gain personal details about

thousands of government employees, burning aliases, costing people jobs, and exposing many of our nation's secrets. People lost personal information such as social security numbers, passport details, and even answers to highly classified surveys (Buchanan, 2017). An attack such as this one, which was not widely publicized after it occurred, might have been better prevented with adequate funding ahead of time.

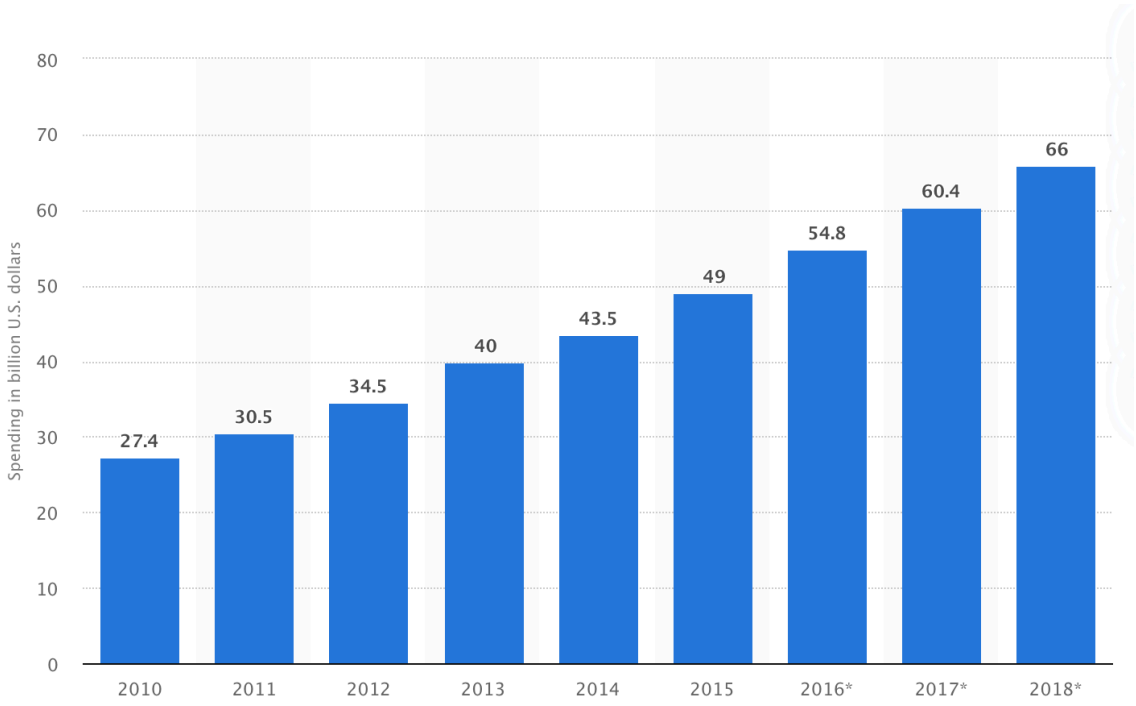
Another attack that did garner wide-spread media attention was when the Democratic National Convention (DNC) was hacked leading up to the 2016 U.S. presidential election. As Special Counsel assigned to uncover the truth behind the attack, Robert S. Mueller III uncovered that the likely attacker was a Russian group with the aim of changing the outcome of the election.

More recently, a group identified by the U.S. Justice Department as Cozy Bear (APT29), funded by Russian intelligence agencies, hacked into U.S. high-ranking government officials to steal data and information. The group has also stolen data from large corporations such as Microsoft and SolarWind.

A logical question is: if the U.S. is really the number one leader in the world in cyber power, then why are they still hacked so frequently? This question illuminates some dynamics behind the asymmetric nature of cyberattacks and cyberwar. As I will discuss in further detail later, "winning" the battle on cyber does not necessarily mean that any one country has a monopoly on its benefits.

Economic Strength

In an examination of how a state's economic success can predict its cyber power rise, there are two figures to examine: the overall power of the economy of that state and the emphasis



Department, P. (2015, April 01). Cybersecurity spending in the U.S. 2010-2018. Retrieved January 23, 2021, from https://www.statista.com/statistics/615450/cybersecurity-spending-in-the-us/

it places on devoting funds towards cybersecurity. Without devoting any funds to the cause of cyber development, a state could have the strongest economy in the world, but still remain weak in cyberdefense. It is for this reason that to predict an increase in cyber power, a state should have a strong economy *and* it should sufficiently fund cyber-related projects and agencies.

There is no doubt that the U.S. meets the standard of having a strong economy. As the strongest economy in the world, measured by gross domestic product (GDP), the United States is well-positioned to meet the first of these two qualifications: having a strong economy. As for the second, the U.S. spends more than any other state in the world on cybersecurity. In 2021 the cyber defense budget will be $18.8 billion (U.S.). That figure represents a less than one percent decrease in spending since 2020; however, the portion of that spending that is going to the Department of Defense (DoD) will go down 2.27% (U.S.). Regardless of the year to year

changes, as seen below, the U.S. has generally increased spending from 2010 to 2018, a step that seemed necessary to maintain cyber dominance (Department, 2015).

However, research conducted by Price Waterhouse Coopers (PWC) suggests that spending on cyber does not guarantee success. A survey of high-ranking government officials from across the world who make decisions regarding cybersecurity found that 47% of said officials prefer investing in the development of new technologies as opposed to the evaluation and enhancement of current capabilities (Kolochenko, 2016). While the rationale for this desire cannot be certain, new technologies often sound more attractive than an increase in spending on a preexisting ones. This is concerning to the extent that technologies are less effective if they have not gone through a sophisticated refining process. The study also concluded that United States officials tended to follow this trend, meaning that U.S. leaders also favored acquiring new technologies over enhancing current ones.

In examining the America's position on the economy as an influencing factor, it seems like they certainly would stand to benefit from any advantage offered up by economic strength. Nonetheless, that advantage may be mitigated by an insistence on developing new technologies. A likely explanation for this behavior in the United States is a desire to please a constituency and win re-election. Because of the aforementioned 70% of Americans that believe cyber threats are real, and because developing new technologies can appear more settling to a constituency, it seems in the best interest of the legislators to make these decisions, even if they are less beneficial to the state in the long-term (Valeriano and Maness, 2015). This relates back to the selectorate theory, which postulates that those elected need to please those who elect them if they want to remain in power.

It is clear that America's strong economy and willingness to sufficiently fund cybersecurity measures definitely played a role in getting them to where they are today. Nonetheless, the U.S. has been criticized for still failing to fund these measures enough. While the U.S. Department of Defense (DoD) has more money, that money is not being allocated in favor of research and development (R&D) initiatives. In fact, it only accounted for an estimated $95 billion of the nearly $700 billion in the DoD mandatory budget. Given that cyber research specifically only accounts for a fraction of that $95 billion, Next Government argues that the U.S. needs to do more to fund cybersecurity efforts (Vincent, 2019).

Economic System

The free market economy has been long understood to drive innovation (Baumol, 2002). Because of factors like constant competition, rising companies, the need to please stockholders, and limited government intervention, the United States, the largest free market economy in the world, has been a leader in technological development (Litan, 2016). The only disadvantage in having a free-market economy for the purposes of examining a cyber benefit is that the United States government is not always privy to the information that is acquired, even if that information comes into U.S. borders. This is a dichotomy that will be explored in depth during the chapter on comparative analysis because it seems that there are both pros and cons of having either of the economic systems of the U.S. or China.

Education

The United States is currently in the middle of an education crisis. In science, technology, engineering, and mathematics (STEM) the United States is falling behind other, less advanced countries. In 2016, China had 4.7 million recent STEM graduates whereas the United States had

568,000. When controlling for population, that makes for a 1:573 ratio for the U.S. and a 1:293 ratio for China (Herman, 2018). Despite the disparity between the U.S. and China, America still ranks third in STEM graduates (Herman, 2018). This correlation could help to partially explain the rise in U.S. cyber power.

Despite this lag, the U.S. has made strides towards enhancing education standards. This movement started during the Obama Administration with the release of The Comprehensive National Cybersecurity Initiative in 2010. In initiative number eight of this memorandum, the administration recommended an expansion of cyber education (Executive, 2010). While largely symbolic, this gesture has spawned an increase in the number of cyber programs. Presidential Policy Directive 21, which was released in 2013, requires the Department of Homeland Security (DHS) to oversee cybersecurity practices and education in the United States. In light of this, the DHS created the Cybersecurity Education Training Assistance Program (CETAP) which provides K-12 teachers the resources to best instruct cybersecurity throughout grade school. While this program did teach students valuable content, the primary purpose was to inspire an interest in cybersecurity studies with the hope that students would develop an interest in cybersecurity (Cybersecurity Classroom, 2021). It seems that education is an important aspect of developing cyber power, so much so that the U.S. enhanced its already advanced education system. Because of this, I would identify education as a significant driving force of cyber development in America.

Espionage

One factor that has unquestionably led to U.S. strength in the cyber domain is espionage. The intelligence apparatus in the United States federal government is unparalleled throughout the

world. It can be assumed that the amount of espionage initiated by the United States is actually larger than anyone can be certain of today (Valeriano and Maness, 2015). Take for example American surveillance over Greece from 2004-2005. In the second Olympic Games following the September eleventh attacks, the first outside of the U.S., the United States, who was worried about insufficient counterterrorism capabilities in Athens, asked Greece if they could wiretap all communication coming into the country in the name of security. While the legality of allowing such surveillance was highly questionable under Greek law, government officials who wanted to avoid the physical harm and international embarrassment of an attack gladly accepted the help. After remaining in the Greek network for nearly two years after the games, the U.S. was caught while making an update to the software they claimed to have dismantled years prior (Buchanan, 2020). This example illustrates that the U.S. will apologize for getting caught, but not for committing the act in the first place. Buchanan argues that had it not been for the slip in a software update, the U.S. might still be monitoring Greek communications today (Buchanan, 2020). At this point, it should be noted that espionage will asymmetrically benefit countries attempting to catch up, like China, more than it will countries already atop the leaderboard, like the U. S.

Immigration

Immigration is an important driving factor in cyber power, but not for the reason that one might think. As noted at the beginning of the literature review, the sole number of people in a country, or the manpower that a country possesses, is largely insignificant in the race towards cyber power dominance. Instead, the reason that immigration is a large concern is that the ability to acquire foreign talent can serve as a tremendous benefit.

Bureaucratic barriers have plagued nearly every aspect of advancement in the United States, and cybersecurity is no different. Countries like China and Russia are creating programs to facilitate the immigration process for foreigners with cybersecurity intelligence capabilities. This is an area in which the United States has lagged behind for some time now. American adversaries offer scholarships, stipends, aid packages, and other incentives to recruit foreign talent. While the U.S. has similar programs, they are not nearly as expansive as the ones presented by other nations (Arnold et al., 2019). This is problematic to the extent that when foreign talent is choosing which developed state to live in, the U.S. wants them to come, but there are barriers here, and more incentives elsewhere, that deter them from coming. A report from the Center for Strategic and International Studies (CSIS) concludes that the problem is two-fold: first, the United States has rigorous standards for admittance to the country; and second, the U.S. needs to balance national security risks with the need for advancement (Segal, 2019).

Despite America's rigorous application process to get H-1B skilled worker status, there has been a push in recent years to get these visas secured for STEM workers. To limit barriers, the U.S. has added exemptions to caps on H-1B visas and green cards for people well-suited to work in cybersecurity (Arnold et al., 2019). Nonetheless, the annual cap on the maximum number of these visas peaked from 2001-2003 and has since leveled off at nearly one-third that level (H-1B, 2020). While this might appear counterintuitive, the government made this reduction to protect national security after 9/11 (Examining the Importance, 2003). Still, as of 2019, the United States sits at the top of the leader board with fifty-one million migrants currently residing in America (Bradley, 2020). While the United States could do more to attract foreign talent, their efforts thus far have been sufficient.

Regime Type

The final, and perhaps largest, problem posed by the emergence of AI technology is that of a foreign threat to the safety and security of the U.S. and its citizens. As other countries, and non-state actors, are surpassing the U.S. in AI research spending and development programs, this problem is growing larger. Due to relaxed regulations on worker environment and lower taxation in countries like China, multinational companies are establishing research and development centers abroad far more frequently than in the U.S. (Hannas and Chang, 2019). This is a difficult problem because while the United States *does* want to attract these companies, they also do not want to compromise moral boundaries, workplace rights, or taxation on large business. In addition to being a more attractive destination for physical facilities, China also plays dirty when it comes to technology sharing. They have a reputation for stealing foreign technology without providing anything in return. There is a widespread belief that liberal democracies possess a creative advantage when it comes to technological development; however, that claim is not well supported in the academic community (Hannas and Chang, 2019).

Additionally, the largely democratic structure in America requires leaders to only taken actions for which the people approve, that is if they care about legacy or want to seek reelection. According to a Harvard Business Review article, politicians in America are beholden to two groups, those who elect them and those who fund said reelection (Gehl, 2020). As previously mentioned, this principle of the selectorate theory cripples the ambitions of elected leaders (Bruce, Smith, and Luo, 2014). Because the American populace has been largely concerned over cyber threats, the cyber power in the U.S has been steadily increasing to match the demand. In fact, according to a Pew Research study surveying 2,000 Americans, nearly three in four people

consider cyberattacks a major threat to the U.S., with a cyberattack being ranked second among perceived national threats behind a terrorist attack from an organization such as the Islamic State of Iraq and al-Sham (ISIS) (Waddell, 2016).

One final way that the American regime type has aided their cyber development is through private innovation. While this subject blends into economics, it is a principle built into the founding documents of America and thus is worthy of being discussed as an aspect of the regime. Nearly all technological developments since the Cold War era were developed by the government prior to the private sector. For example, both global positioning systems and the internet were being used by the government for years before they became available commercially. With the rise of cyber capabilities such as hacking and artificial intelligence development, this pattern took a colossal shift (Snyder, 2019). This phenomenon has the potential to be problematic because if the U.S. government is playing catch-up on technological advances, then the country could be susceptible to attacks that the government has no way to combat. However, what the U.S. does have going for them is that the private sector world leaders in cyber technology are located in the United States. This not only means that America will benefit from the economic returns of such technology, but that the U.S. government will likely have this technology before other governments.

Preexisting Military Strength

The United States is the more vulnerable to cyberattacks that any other state, and there is not much it can do once breached (Gartzke, 2019). Reliance on technology for critical national security operations coupled with being a world leader makes the United States susceptible to attacks from both state and non-state actors. Interestingly, this threat has actually been a driving

influence in the buildup of American cyber capabilities. While the U.S. still leads development of technological advancements, other countries such as China are creating serious competition. The Chinese government announced a plan in 2017 detailing how they will become the global leader in AI by 2030 through increased funding, of up to $150 billion, and implementation of new programs. China's goal is to build the fastest, best-informed AI technology so it can develop autonomous military vehicles (Williamson, 2019). Similarly, Russia has focused a great deal of spending on cyber technologies as well (Snyder, 2019). In response, the United States has increased funding for research and development (R&D) as well as the number of personnel assigned to work on cyber development (Arnold, 2019).

In addition to the threat of the United States as a driver of cyber power, another factor associated with preexisting military strength is alliances. Perhaps the alliance from which the United States benefits most in terms of cyber power is Five Eyes. this organization is composed of five countries: the U.S., United Kingdom (UK), Canada, New Zealand, and Australia. While most of the detailed information surrounding the organization is inaccessible, it is known that there are over thirty-three countries that have at one point partnered with Five Eyes in some collaborative arrangement. One of these thirty-three is Denmark, which aided the organization by cable-tapping Russian communications that passed through Danish lines (Buchanan, 2020). While international organizations have undoubtedly contributed to America's rise in cyber power, it remains to be known whether the United States is on the right end of that deal, or whether partner countries are benefiting more than the U.S. The bottom line is that because the U.S. has more cyber power than any other state, partnerships will likely benefit other countries more than America, but that does not mean that the U.S. is unjustified in these endeavors.

In 1979, the first U.S.-China Agreement on Cooperation in Science and Technology was signed by Presidents Jimmy Carter and Deng Xiaoping. Despite attempts to encourage open sharing of technology, it quickly became apparent the Chinese were not willing to comply. Through backdoor dealings with other countries, enhanced surveillance, and withholding of information, the Chinese proved to be unreliable. As tensions escalated, the U.S. needed to better manage the flow of science, technology, and engineering information. In 1985, the National Security Decision Directive (NSDD)-189 was issued. This directive codified the previous language from other, less comprehensive initiatives and would better protect the United States from foreign attacks (Segal and Gerstel, 2019). Efforts like this to force foreign compliance allows the U.S. to make sure it is on the winning side of these agreements.

Factors that Inhibit Cyber Power for the U.S.

While the primary focus of this research is to identify which factors are strong predictors and causes of a rise in state cyber power, it is also important to identify factors or elements of a state that hinder cyber power development. Research into the United States has revealed two such factors: privacy requirements and technological reliance.

There are benefits that come with being a leading democracy in the world, such as the private sector development mentioned earlier. However, those same democratic ideals that enable cyber power rise in certain capacities may work against development in others. For example, because the United States elects officials to protect their interests, there are concerns that American legislators need to address that lawmakers in non-democratic societies can largely ignore (Shahbaz, 2018). This is problematic to the extent that citizens in the U.S. often have little regard for issues until they occur, and then, they want to do something about it (Ding, 2018).

While authoritarian regimes can forecast problems such as cyber and plan for that defense, the U.S. can only anticipate the issues as much as the public perceives them to be threatening. Understanding this position, the United States government is in a difficult situation, stuck between an international disadvantage in the cyber race and the need to align with citizen preferences.

Another factor that restrains America's cyber power is its reliance on technology. Earlier, I stated that the United States, being the largest target in the world, is actually aided in its cyber power because of the need to develop a sophisticated cybersecurity apparatus (Specops, 2020). Nonetheless, that same point can be taken in the opposite regard. By relying on technology for key military operations such as communications, ground operations, and even nuclear weapons, the U.S. leaves itself susceptible to hacking (Bryant, 2011). These types of operations that were once done without electronic technology are now much more efficient, but at what cost? The analysis put forth by Bryant a decade ago is true now more than ever. The United States has only increased reliance, or even dependence, on technology, which makes operations more efficient but hampers national security.

Chapter Four: China

Background

Chinese cyber development has ramped up in the past couple of decades. One of the more landmark initiatives occurred in December 2013 when the main communist party policy-making group, the Politburo, created the Central Leading Group for Cyberspace Affairs, known better as the Cyberspace Administration of China (CAC). This was the first time the Chinese government created a separate agency to oversee cyber operations (Yuen, 2015). This agency was tasked with creating national strategies and policies for the Chinese government relating to cyber operations. After such a monumental agency was created, the Chinese government needed a plan to move forward with its cyber operations. In 2017, it launched China's AI Dream, an initiative targeted at becoming a global leader in artificial intelligence. This movement focused in large part on the implementation of AI into cybersecurity and attacks (Ding, 2018). China's development since this launch three years ago has been difficult to track and will likely be better understood decades from now, but because of China's progress, goals, and potential it is a country worthy of examination.

As measured by the National Cyber Power Index (NCPI) 2020, China ranks second across all seven of their measured indicators (Voo et al., 2020). However, this is not something to be largely concerned with because as was discussed in the introduction, large-scale war between countries is likely behind us (Fukyama, 1992). In fact, Chinese possession of advanced cyber capabilities have even been posited to mitigate the effects of cyber attacks in a similar way to how Soviet acquisition of a nuclear arsenal deterred the use of such weapons by the United States (Inkster, 2016). The difference with cyber is that the ability to exercise mutually assured

destruction (MAD) is unknown in the cyber realm in the same way that it was known in nuclear disputes.

In addition to Chinese advancement, Chinese world leadership more broadly has increased tremendously throughout the twenty-first century. Chinese expansion is a legitimate and significant threat to the United States (Brands and Sullivan, 2020). China's increasing control over manufacturing in recent years has placed them in a position of international power. Because other states have a reliance on China for manufacturing needs, China is well-positioned to negotiate against adversaries and to resist compliance with international treaties and agreements. Because the imposition of tariffs hurts the country exercising the tariffs on China almost as much as China itself, it is oftentimes not in the best interest of a state to impose tariffs on China (Tulley, 2019).

Economic Strength

Since the aftermath of the cultural revolution, stabilizing and exciting the Chinese economy has proven difficult. Starting with leader Deng Xiaoping in 1978 the Four Modernizations plan re-emerged. With a focus on agriculture, industry, STEM, and defense, China had a plan to rise as a world power once again (Inkster, 2016). As the five-year plans aimed at achieving this lofty ambition were implemented, it became apparent that STEM and industry were going to become far more lucrative than agriculture and defense. This is why Jiang Zemin, president of the Chinese Communist Party (CCP) decided in 1983 to make the electronics industry a primary focus, increasing the output goal for that five-year plan by eight times the previous amount. Such a bold action encouraged the private sector to focus on making information technology (IT) accessible to the Chinese people (Austin, 2014).

The rise in manufacturing throughout the twenty-first century coupled with the focus on IT services put the Chinese economy on an upward path. In fact, the total economic output in China passed Japan in 2010, making China the world's second-largest economy (Overview). This transition from extreme poverty in 1970 to the second-largest economy in the world forty years later happened because of China's willingness to open its borders. With a series of changes in the '70s and '80s China became a hotspot for companies looking to manufacture goods at cheap labor prices. Because of China's lack of concern regarding worker rights, manufacturing costs were much lower than in more developed countries, and meanwhile, the resources and ability to manufacture were the same. This foreign investment was also aided by China's creation of four special economic zones, which essentially allowed foreign investors to invest in certain blocks of the Chinese market with mitigated risk (Special, 2020). The Chinese economic story parallels the United States in that a rise in economic conditions appears to at least be correlated with cyber power, if not a direct cause of the rise.

The reason that a strong economy in China has been able to facilitate strong cyber power is because of the government's willingness to invest necessary funds to the field (Ding, 2018). While this may appear obvious on the surface, it does need to be noted that simply possessing a strong economy does not guarantee cyber power success.

Economic System

In addition to economic strength, the restructuring of the Chinese economic system also played a critical role in China's rise in cyber power and power more broadly. This transition was not only instrumental in the development of Chinese strength but perhaps essential to remaining relevant as a world power (How China, 2020). If China had not opened their markets to the

international community and allowed businesses to operate independent of the state, their economy would likely have stalled compared to other trade heavy countries such as the U.S. Today, China sits as the largest trade partner in the world, which is a stark shift from the previously consumer-heavy economy that China had been used to. Since China became the manufacturing capital of the world, the economy has done well as shown by a declining, but steady, rise in GDP since 1979 (China's Economic, 2019). Looking at the Chinese economic system holistically, it becomes apparent that the transition from isolationism to a global trade leader facilitated economic growth (Inkster, 2016).

Education

Education in China has long been a weak point in their development, but that has been changing throughout the 21st century when a shift towards a focus on STEM education began to foster talent in cyber operations. In 2018, the Education Ministry created the "AI Innovation Action Plan for Institutes of Higher Education." This plan, implemented at the same time as China's AI Dream, meant that the government would not only provide universities with the necessary tools to foster educational development, but they would also incentivize students to participate in these programs (Hannas and Chang, 2019). This program, and others like it, encourages educational development in the area of artificial intelligence, which to a large extent overlaps with national cybersecurity needs. Despite this push towards education enhancement, China still struggles to educate a large portion of its citizenry. While the Chinese government reports that it educates over 95% of its population, many sources remain skeptical of those figures (Education in China, 2020).

Part of what might have contributed to the overall increase in Chinese intelligence is their Military Personnel (Talent) Cultivation System which strives to educate citizens interested in serving in the Chinese military. This, again, incentivizes the citizenry by providing educational services in exchange for military service (DOD Releases, 2020).

These educational efforts have proven beneficial as they foster talent for the development and maintenance of advanced cybersecurity as well as attacks. One such instance that required advanced education was a series of attacks launched by the Chinese government at the United States in 2003 known as Titan Rain. These attacks were aimed at securing classified Department of Defense information. The attackers were able to infiltrate DoD networks because of malware they had uploaded into the computers (The Lesson, 2005). Attacks such as these prove that an educational background within China is beneficial towards its cyber ends. The attackers would not have been able to steal the code used to exercise the Titan Rain attacks from other governments because if the United States, or one of its allies, had been aware of the deficiency, it would have been patched before the Chinese government could exploit it. If a state such as China wants to attack another state such as the U.S., then developing an attacking mechanism for which the other state has no defense is essential. In terms of cybersecurity, a state's top priority is usually to mend any weaknesses it is aware of, so China in this case needs to develop code independent of the U.S. (Nye, 2010).

Espionage

China is the largest *known* perpetrator of international espionage campaigns (Karatzogianni, 2010). Such a bold statement does, however, come with a qualification (hence my use of italics for the word *known*). Because of the nature of espionage, the best attacks

remain undetected to this day, and so while the Chinese government has been caught in the act of stealing information and technologies from other countries more than anyone else, it is unknown whether another country actually commits more of these acts. Regardless, China has gained much of its technological edge by stealing technologies from other countries. For example, China has been known to have hacked and stolen from the United States, India, and Japan, all global leaders in cyber capabilities (Valeriano and Maness, 2015).

The reason that espionage has been so beneficial to the Chinese is because of their technological lag for years. Wang Yukai, a State Council expert in the Chinese government stated that "[s]ecurity is actually a technological competition in which China, lacking core technology, has lagged behind due to excessive dependence on overseas equipment and information systems," (China Eyes, 2014).

Espionage has been a successful strategy for China throughout its rise in cyber power since the turn of the century, but that could change. Because of cyber espionage, the need for conventional spying operations, such as planting field operatives, is diminished (Meserve, 2007). However, once a state is able to catch up to its greatest competitors, as China has largely done in relation to the U.S., espionage starts to yield diminishing returns. At that point in time, a return to the discussion of education and self-produced intelligence comes back into focus. As China advances in cyber power, their reliance on espionage as a primary tool for acquiring knowledge will become obsolete.

Immigration

In much the same way as the Chinese government has fostered STEM education at home, it has also made China an appealing destination for foreign talent. By requiring fewer documents

and less red tape than other powerful countries such as the United States, China becomes a viable option for immigration (Hannas and Chang, 2019).

Even more telling perhaps is not an issue of immigration so much as the lack thereof. The number of Chinese students who study higher education in the United States has increased from 2009 to 2019 from 98,235 students to 369,548 students (Number, 2019). This nearly quadrupling of students is indicative of lingering educational deficiencies in China, but what is more telling is where these students go once they have completed their education. Since 2008, when data on this matter first was recorded, the annual rate of students who return to China after receiving education in the United States has continued to rise. The rate at which that increase continues to climb has gone down but still exists (China: Rise, 2020). As more Chinese students return to China, the logical question is: why?

A likely explanation is to look at the aforementioned H-1B Visa program which largely restricts foreign talent from remaining in the United States, so, by this logic, the Chinese government is benefiting from immigration policies that they never even set into action.

In addition to benefiting from the strict United States immigration stance, China itself has taken steps towards opening its borders for people with talent in STEM. By relaxing the necessary criteria for continued residence in China, the government has enabled far more people to remain working in China, specifically those with “in-demand” talent and skills (China Implements, 2019). This legislation, which took effect August 1st, 2019, expanded coverage and accessibility to students, permanent residents, part-time residents, visa workers, and more.

Legislative action such as the relaxed criteria mentioned above undoubtedly contributes to China’s rise in cyber power. By enabling the people with technological skills to remain or

easily come to China, the government removed a barrier that largely plagues other states. This type of action, again, at least correlates with the Chinese rise in cyber power throughout the 21st century and can likely be identified as a factor that has caused the rise.

Regime Type

The Communist Party of China (CPC), as the sole party in the Chinese government, has near autonomy over the decisions made in China. Because of the single-party state in this authoritarian regime, the Chinese government makes decisions that often resist popular opinion. In a democracy such as the United States, political parties are beholden to the wishes of the constituencies because if they are not then they will be voted out of office. Meanwhile, in China, things such as individual security and privacy are given little consideration compared to the pursuit of national power (Jacobs, 2018). Paradoxically, while a lack of privacy may appear to hinder cyber advancement in China, it actually allows them to succeed. The Chinese government, with access to an abundance of personal information, is able to better develop its cyber capabilities, tailoring its code to the need of its own government. This tactic does little to aid China in its national security, but it enhances cyber power by bolstering attacking mechanisms. If one assumes that the personal data patterns of Chinese citizens are largely similar to that of other countries, then it is easy to see how access to that information would help the Chinese government in their quest for cyber power (Ding, 2018).

In addition to their domestic surveillance, the authoritarian regime type in China has enabled them to acquire more manufacturing business. As previously mentioned, China is an appealing location for industrial business because of low taxation and limited worker safety regulations. This would not inherently serve as a benefit for the Chinese except that other power

cyber players *do* have concern for these conditions. While democracies such as the United States want to attract these companies, they also *do not* want to compromise moral boundaries, workplace rights, or taxation on large businesses, again for fear of losing political power. This idea gets at the heart of cyber power, the fact that it is a zero-sum game. Because of the nature of cyberwarfare wherein a deficiency compared to another nation makes a state vulnerable, any gain by an adversary only serves to harm the other state. This means that something such as regime type can hurt a democracy like the United States and simultaneously aid authoritarian regimes such as China.

Further, it cannot be said that China hurts from their economic structure like they once would have when they could truly be defined as a communist country. China has been more of a free-market economy than a communist state since the early 1990s (How China, 2020). By opening up its market and joining organizations such as the World Trade Organization (WTO) in 2001, China has proven to be a global player in the world economy. This, on top of the fact that the authoritarian Chinese government gathers information from the top corporations in China, allows the government to enhance their cyber power.

Preexisting Military Strength

Chinese military capabilities have increased tenfold in the past couple of decades; however, because the Chinese government cannot remotely be compared to the United States in terms of its military capabilities, I have chosen to discuss the restructuring of the Chinese military as a potential factor influencing cyber development. In 2015, Chinese President Xi Jinping introduced the most comprehensive PLA reform in over thirty years. This reform involved a restructuring of the Chinese military so that it would better streamline certain

divisions of operations such as a Space Force, Strategic Support Force, and Cyber Division (China Military, 2019). This restructuring enabled the cyber division of the military to work at their own rate. This independence led to the creation of China's AI Dream, a document released in 2017 that outlined a plan to make China the world leader in AI in only 13 years. Such a lofty goal indicated that the government would need to enhance cyber capabilities. Just as it is very important to examine the military capabilities that exist, it is equally important to look at the need for such advancement. Because of the timeline that the Chinese government issued, a need for the advancement of cyber functions became apparent for two reasons. First, because AI and cybersecurity overlap a great deal, strength in one translates to strength in another. AI enables a country to better anticipate attacks and to develop offensive capabilities quicker. Both of these benefits lend themselves toward a translatable influence on cyber power (Allen and Chan, 2017). Second, every time a state wants to become a leader in some military domain, security is one of the top priorities. As mentioned before, the Chinese government has a reputation for stealing foreign technologies. Because they are so familiar with this practice, this highlighted the need to make operations surrounding this AI dream secure.

Factors that Inhibit Cyber Power for China

While the Chinese government has shown the most improvement in cyber power over the past couple of decades, there are some weak spots that have mitigated the power gain in China. First, while the Chinese have made strides toward becoming more of a free-market economy, some of the authoritarian structures serve to mitigate innovation. Until China begins to rely more on the development of technologies than on stealing technologies, it will find it difficult to advance cyber capabilities beyond that of its adversaries (Libicki, 2011). This is why China has

started programs to facilitate independent research and development. The difficulty so far is that these programs are relatively young and so their success has yet to be fully realized.

Another vulnerability for Chinese cyber power enhancement is government oversight. While before, I noted that the Chinese government's ability to surveil its citizens without repercussions could serve as a benefit towards learning about patterns, it can also hinder development. With the government so closely connected with private companies around China, the opportunity for growth, independent of the government is diminished. This is problematic to the extent that, as mentioned in the literature review, the development of cyber technology has been atypical in that advancements have appeared in the private sector *before* the government has developed them. This temporal anomaly calls for less government control over private corporations, a more laissez-faire approach (Stier, 2017). Private companies' research into cyber capabilities is usually focused on cybersecurity because the corporations are more often interested in protecting their infrastructure than they are about launching an attack (Spade, 2012). For this reason, the Chinese government could be vulnerable to cyberattacks more frequently than a country like the United States which works more diplomatically with private companies within its borders.

Chapter Five: Comparisons

To best compare the United States and China in terms of their cyber power and capabilities, the question at the heart of the discussion needs to be, "why?" Not why should we focus on cyber power predictors nor why should we examine the United States and China, those questions were addressed early on, but rather the question needs to be why did the factors highlighted above place the United States and China in the upper echelon of states in terms of their cyber power? Why did factors such as raw materials or sheer human capital not make the list as factors that influenced a rise in cyber power? The answer to these questions can be found through an examination of the differences between the United States and China. This chapter will be used to compare the two states using each of the aforementioned predictors. By looking at the similarities and differences between the top two states in cyber power, conclusions can be drawn about which factors matter most, which matter less, which of these factors is helpful but not necessary, and more. This type of comparative analysis is useful in a discussion such as this one because it breaks down the differences and similarities, not only highlighting how China and the U.S. are similar and dissimilar but allowing a view into the factors that can be used to measure other states or to predict future trends for the states currently under examination.

Factor One: Economy

Economic Strength Table

	United States	China
Economic strength	Number One	Number Two
Cyber power	Number One	Number Two

The chart above demonstrates the correlation between economic strength and cyber power. While difficult to make a causal conclusion without examining dozens of extraneous factors, there is certainly evidence to argue for a correlation between economic strength and cyber power. Because the United States and China boast the two most powerful economies in the world, it should not come as a surprise that they also hold the title of numbers one and two in terms of cyber power. Strong economies generally lead to a strong military when funds are allocated in a proportional way (Lobont et al, 2019). Because this phenomenon has been proven to be true, when a state, which is willing to appropriately fund the military, gains economic strength, one can expect that state to gain an advantage militarily. In the case of the U.S. and China, that meant devoting funding to the advancement of cyber power. If nothing else, what one can take away from the discussion of economic strength is that it is a necessary, though not sufficient, condition for becoming a world leader in cyber power.

Economic System Table

	United States	China
Economic system	Free market	Socialist market
Cyber power	Strong	Steady increase

The above table tells a different story from the one examining economic strength. This graph explains that having a full-fledged market economy is not necessary for advancement in cyber power. In fact, the socialist market economy has benefits that can drive innovation at rates similar to that of a market economy (Alaskalink). The Chinese government controls a large

portion of the enterprise in China while allowing for some competition between non-threatening companies so long as the Chinese government remains in charge. This economic system allows the Chinese government to get its hands on any new developments that might emerge. This is important because as mentioned before, the private industry is leading the race in terms of cyber advancement. However, any gain that China sees as a result of government oversight has thus far been offset by the restriction of big, free business that the United States affords its companies.

Factor Two: Education

Education is an essential component of attaining and maintaining cyber power. For both the United States and China, an increased focus on STEM education facilitated the rise in cyber capabilities, culminating in the rise of cyber power. As China continues to fund STEM education, it will continue to rise exponentially in cyber power. One interesting point to note when comparing the education system of the U.S. versus China is the availability of educational services. While China does have a period of "compulsory" education lasting nine years, in the U.S. students are guaranteed twelve years of education (Overview, 2019). This difference is accounted for by the sheer quantity of students in China who attend post-secondary school. Valid data on the rate at which students in China continue their education at the university level is difficult to obtain as the Chinese government only releases numbers that portray a healthy continuing education perception. One reliable statistic for our measurement examines the total quantity of graduates from Chinese institutions of higher education. The World Education News and Reviews reports that as of 2017, around eight million people graduate from Chinese higher education institutions (HEIs) every year. Regardless of the percentage that this number represents, that number exceeds the United States and India combined (Education, 2019).

As for the quality of education, it is difficult to say whether one country is more advanced than the other. The U.S. and China have different goals when it comes to educational output. More specifically, the U.S. focuses on cultivating student creativity whereas China focuses on understanding knowledge and structure. The difference in approach towards education has clear ramifications: Chinese students more often take first prize in math and science competitions whereas U.S. students win more Nobel Peace Prizes (Affairs, 2015). As for which approach better serves national cyber power interests, the answer has yet to be determined. There is a clear need in cyber for developing new ideas and thinking outside of the box, but there is what appears to be an equal need to perform STEM skills at the highest function to allow those ideas to translate into reality. When combining this idea of U.S. ideas with Chinese practicality, the issue of security becomes heightened. If the Chinese government were able to steal, through espionage, U.S. ideas and blueprints and then turn them into material products, then they could see a tremendous advantage in terms of cyber power.

Factor Three: Espionage

As was discussed in the chapter, espionage disproportionately benefits states that are behind as they have more to gain from stealing technologies from those that are more advanced. According to the Verizon 2020 Cyber Espionage Report, over 90% of cyber espionage is conducted by nation-states or state-affiliated actors (Grim et al, 2020).

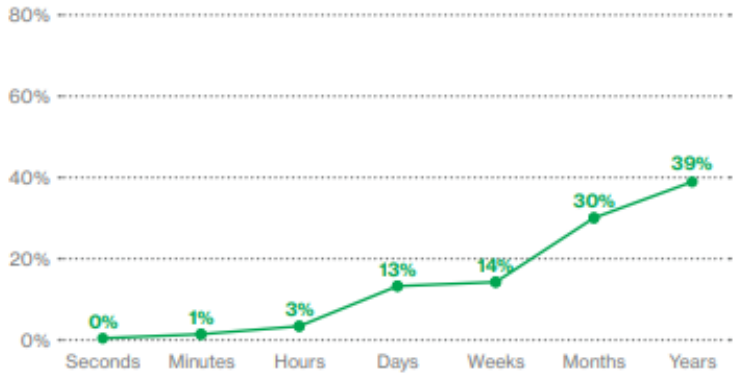


Figure #2: Time to Discovery within Cyber-Espionage breaches (2014–2020 DBIR; n=125)

Given the frequency at which states perpetrate these attacks, coupled with the knowledge that states with something to gain have a distinct, asymmetric advantage, China clearly is more powerful in the damage they can cause through espionage than is the United States.

What's more is that those attacks often remain undetected for years. As noted in the espionage section of the United States case study, once the attack is detected, there is little incentive for a state to retaliate or to even admit they discovered it (Grim et al, 2020).

Factor Four: Immigration

Immigration plays a critical role in fostering cyber talent. As noted above, in recent years China has been facilitating the smooth transition towards a more open border that recruits talent from all over the world. The United States, on the other hand, has reservations about the security risks of allowing foreign talent to represent American national security interests. This is why barriers to immigration into the U.S. for national security are in place. These barriers have served as an impediment towards U.S. talent acquisition, diminishing the extent to which the U.S. can advance its cyber power. Arguably, America may have been more handicapped by the admission of foreign operatives who turn out to betray the U.S. The requirements for obtaining a security

clearance, necessary documentation for most national security roles, are extensive and have by and large done a sufficient job of keeping threats out of the U.S. security apparatus (Go Government, 2020).

Meanwhile, the Chinese government has capitalized on American reluctance to accept foreign talent. By offering additional incentives, the Chinese government has acquired great foreign cyber talent. Additionally, as mentioned above, by incentivizing students who study outside of China, the Chinese government has established a system by which the citizenry can grow up in China, leave for higher education, often coming to the United States, and then return to China to work in national intelligence. This structure is extremely powerful because it enables the Chinese government to learn what the United States is teaching to its STEM majors and then the Chinese government can apply that knowledge themselves.

Factor Five: Regime Type

As noted in the chart above, both the Chinese and American regime types have aspects that facilitate cyber power progression and aspects that hinder that development. For the U.S., and democracies more broadly, the benefit of a laissez-faire economic system helps drive innovation. As noted explicitly in the U.S. case study (page 36), the structure of American economics is tied directly to that of the regime type. The U.S. Constitution lays out the principles of economics that the government must abide by. Perhaps most important to consider in the discussion of cyber power advancement is allowing private companies to drive innovation. The rise of cyber developments marks the first time in history that private corporations have outpaced the government in technological advancements (Merritt, 2017). Because the United States allows corporations to thrive independent of the government, they remove restrictions that otherwise

would impede development. The clear downside to this is that the government is not always privy to the most up-to-date technology.

The main disadvantage, however, for democracies when it comes to cyber power advancement is the onus placed on reflecting the will of the people while in office. As mentioned before, because cybersecurity does not readily impact the lives of most Americans daily, legislators who want to be reelected often have to bend national interests to best meet the people's desires. Interestingly, while most Americans do view a cyberattack as a colossal threat to the United States, a far lower percentage want lawmakers to act on that threat at the cost of daily benefits that they receive from programs like education (Waddell, 2016).

Another disadvantage for democracies when it comes to the U.S. and cyber power development is the maintenance of company headquarters. While the U.S. does not admit to stealing information from companies directly, different agreements allow the U.S. to access some developments made by companies within its borders. The problem is that because the United States prohibits workplace violations and has higher tax rates than other countries, it struggles to acquire and maintain companies within its borders.

As for authoritarian regimes, they have the benefit of surveilling their citizenry which allows them to apply that knowledge to other states (Ding, 2018). Additionally, because of their surveillance, the Chinese government does not have the same restraints when it comes to accessing the technologies developed by companies within its borders. Speaking of the companies in China, the country has become a very attractive alternative to the United States for companies who care little about labor standards and want to pay lower taxes. For this reason, China has been able to house some huge tech companies such as Hua Wei. Authoritarian regimes

have the benefit of acting unilaterally without the worry of how their actions will be perceived. This is a powerful notion because it allows these regimes to take the necessary, despite being unpopular, actions that democratic countries struggle to take.

The downside for authoritarian regimes in the quest for cyber power is their insistence on surveillance. The very element of their regime structure that benefits authoritarian regimes also works to their detriment. Because of the constant government surveillance, innovation is hindered and progress delayed in the race towards technological innovation. Again, this can be compensated for through continued espionage, but developing new technologies that no other country possesses is more beneficial than attempting to steal them.

Factor Six: Preexisting Military Strength

A well-established military existed in both the United States and China before each of their increases in national cyber power. This correlation makes sense when one thinks of cyber power as an asset towards national security. With the number one and two defense budgets as of 2019, the United States and China have proven themselves to be committed to national defense, security, and overall power (Ranking, 2020). Given that concern over national power, it makes sense that the countries with the most resources to spend on defense would allocate a decent portion of those funds to the development and advancement of cyber power. The national interest of every nation is at least partially contingent on security, and right now, cybersecurity is as important as any other form.

Vulnerabilities

Both the U.S. and China have limitations and hinderances that have prevented, or at least stunted, optimal cyber power advancement. For the U.S., being the worlds largest target means

that they need to invest heavily into cyberdefense (Specops, 2020). This is problematic for the U.S. to the extent that China is investing in more offensive capabilities, and as was demonstrated earlier, offensive capabilities appear to have the advantage in cyberwar, at least for now (Garfinkel and Dafoe, 2020).

Additionally, the U.S. is hindered by its inability to freely surveil its citizens. While the Snowden leaks do appear to shed some light of the fact that the U.S. is conducting these routine searches of its citizens, it is much more difficult for the government to hack the private companies within its borders. Because the private sector is currently winning the cyber race, they often have more advanced capabilities than the government. Thus, authoritarian governments, like China, can overtly require the companies within its borders to hand over its latest technology without repercussion or resistance. This has been a struggle in the United States where privacy is a core principle for private citizens and businesses.

Chapter Six: Conclusions

Cyber power, as discussed throughout this thesis, is important to measure because of the impact that it has on national power more broadly. By examining the factors associated with the cyber power success of the U.S. and China, this thesis identified factors that can be used to predict the future rise in state cyber power. Below is a characterization of the findings from this research.

Findings

For both the United States and China, a strong economy appears critical to the advancement of cyber power regardless of economic structure. As far as economic systems are concerned, the two countries represented in the case studies had drastically different elements in their economies. For each of them, there are benefits and consequences. For example, the U.S. benefits from an open market when it comes to technological developments whereas the lack of regulations in China attract business headquarters. Espionage, as expected, benefits the state with more knowledge to gain, in this case, China. The H-1B visa program in the United States is an unexpected discovery that fits under the category of immigration but not in the way I had hypothesized. Originally, it appeared that strict immigration restrictions prevented the U.S. from acquiring foreign talent altogether, but after conducting research on education in both the U.S. and China, I found that the U.S. still allows people to come to the U.S. for educational purposes before being forced to return home. This has actually come at America's expense with Chinese students receiving world class education and bringing those tools back to China. Differences in regime type appear to have an insignificant effect on the ability to advance cyber power as there are pros and cons to both authoritarian regimes and democracies. Finally, as hypothesized,

preexisting military strength remains a strong predictor of technological advances, and cyber is no exception. Although one thing that I will note is that this is not as strong of a correlating factor as it once was because of the advantage in the private sector regarding cyber that did not exist for other technologies.

Research Qualifications

As was mentioned at various points throughout the thesis, this research is arduous and incomplete for two reasons. First, the country with the most advanced cyber power could yet to have been identified or the country that we know to be the best could be far better than we know. This is all because of the veil of anonymity that cyberattacks and defense systems afford those exercising them. Unlike other technologies such as the frequently compared nuclear warheads, cyberattacks are a series of ones and zeros that have very little physical tangibility. Second, China's data is extremely unreliable, but America's might be too. Because the effects of a cyberattack can be devastating, but those effects are oftentimes unnoticeable to the average person, governments have great incentive to hide the fact that they have been attacked and even less incentive to advertise their own attacks. The Chinese government has been known to fabricate data to make the country look more powerful, so it would be naive to think that cyber is an anomaly.

In addition to being forced to rely on incomplete, and sometimes blatantly inaccurate data, when looking at Chinese numbers, another limitation of the research is the speculative nature of correlative analysis. For instance, yes it is true that both the U.S. and China had an economic strength that correlated well with the rises in cyber power respectively, but it is difficult to tell whether that economic strength played a role in that rise. Because the field of

cyber politics is so young and there are only a handful of states who can be said to have any significant degree of cyber power, the data to pull from is limited. So while it is likely that a strong economy facilitates cyber power, the necessity of a strong economy, or even the impact that one has cannot yet be fully understood.

Future Research

Now that classifications have been established for predicting future rises in cyber power by looking retroactively at how the current world leaders have gotten to where they are, there are two paths forward. First, researchers could use these predictors to predict cyber power trends for other countries. Second, research examining the current abilities of the United States and China could help to show who will gain an edge in the future. Both of these ideas for future research would serve the academic community and policymakers alike. By predicting future rises in cyber power using the factors that I have identified as significant in this thesis, the academic community will have a better grasp on general trends in cyber power. That information can then be extrapolated to predict even larger trends in terms of national power more broadly.

In terms of the policymaker interest in future research of this sort, lawmakers can use data predicting future rises and falls in cyber power to influence the legislation they pass. If, for instance, the predictors indicate that a given state will lag behind should they continue on its current trajectory, that information would be useful to lawmakers who could enact policy to increase the state's chance of growing its cyber power.

While the research in this thesis can certainly inform such policy decisions on its own, it does not examine each factor in terms of its expected growth or decay. My research only looks retroactively at the factors that enabled, or inhibited, growth in cyber power for the U.S. and

China. In order to develop the ideas around which factors hold significant weight when analyzing cyber power, a look back at correlating factors that enabled two states to rise was necessary.

Concluding Remarks

Cyber power has the potential to unleash tremendous damage, and cyberdefense is becoming a critical component of national security. On the cusp of a new era of warfare, it is more important now than ever to show interest in cyber power. The states that will prosper in the future are the ones who recognize the factors above and take action to those ends. Cyber power as a concept should be taken seriously because we no longer live in a world of science fiction where entire countries can have their power grid knocked out… that is our reality.

References

Admin. (2019). Cyber-defense Strategies for Contending with Non-state Actors: A Review and Assessment of Existing Proposals. Retrieved November 05, 2020, from http://yris.yira.org/comments/2214

Affairs, O. (2015). Differences between Chinese & American education. from https://internationalnewsroom.com/cn-us-education/

Asialink Business. (n.d.). China's Economy. from https://asialinkbusiness.com.au/china/getting-started-in-china/chinas-economy?donothing=1

Allen, G., & Chan, T. (2017). Artificial Intelligence and National Security. Retrieved from https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf

Arnold, Zachary et al. (2019). "Immigration Policy and the U.S. AI Sector." CSET Georgetown, Center for Security and Emerging Technology,

Austin, G. (2014). Cyber policy in China. Cambridge: Polity Press. page 28.

Baumol, W. (2002). The Free-Market Innovation Machine: Analyzing the Growth Miracle of Capitalism. Princeton, New Jersey: Princeton University Press. doi:10.2307/j.ctt6wpz8j

Beckley, M. (2010). Economic Development and Military Effectiveness. Journal of Strategic Studies, 33 (1), 43-79. doi:10.1080/01402391003603581

Beckley, M. (2018). The Power of Nations: Measuring What Matters. International Security, 43 (2), 7-44. doi:10.1162/isec_a_00328

Bowman, Carter (2020). Could AI-Proliferation Be The Next Nuclear Crisis?, Broad Street Humanities Review, 2.

Bradley, M. (2020). The UN Migration Agency? IOM–UN Relations. The International Organization for Migration, 99-125. doi:10.4324/9781315744896-5

Brands, Hal and Sullivan, Jake (2020). China has two paths to global domination. from https://foreignpolicy.com/2020/05/22/china-superpower-two-paths-global-domination-cold-war/

Bruce, B. D., Smith, A., & Luo, W. (2014). *The dictator's handbook*. Nanjing: Jiangsu wen yi c chu ban she.

Bryant, Steven. (2011). *The Dangers of An Over-Reliance on Technology*. [Master's Thesis, Joint Advanced Warfighting School] JFSC-NDU. https://apps.dtic.mil/dtic/tr/fulltext/u2/a545545.pdf

Buchanan, Ben. (2017). The Cybersecurity Dilemma : Hacking, Trust and Fear Between Nations, Oxford University Press, Incorporated. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/oxford/detail.action?docID=4806712.

Buchanan, B. (2020). The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics. Cambridge, MA: Harvard University Press.

Bumiller, Elisabeth and Shanker, Thom. "Panetta Wars of Dire Threat of Cyberattack." (2012). New York Times.

"China Eyes Internet Power." *Xinhua* (2014). From http://news.xinhuanet.com/english/special/2014-03/08/c_133171308.htm

China: Growth rate of students returning from abroad 2008-2018. (2020). from https://www.statista.com/statistics/1029571/china-growth-rate-of-students-returning-from-abroad/

China implements new immigration policy. (2019). from https://america.cgtn.com/2019/08/22/china-implements-new-immigration-policy

China military power: Modernizing a force to fight and win. (2019). Washington, D.C: Defense Intelligence Agency.

China's Economic Rise: History, Trends, Challenges, and Implications for the United States. (2019). Congressional Research Service.

Coyne, H. (2019). The Untold Story of Edward Snowden's Impact on the GDPR. *The Cyber Defense Review, 4*(2), 65-80. doi:10.2307/26843893

Cybersecurity Glossary. (2020). From https://niccs.us-cert.gov/about-niccs/cybersecurity-glossary

Cybersecurity in the Classroom. (n.d.). from https://niccs.cisa.gov/formal-education/integrating-cybersecurity-classroom

Cybersecurity workforce programs: Sans cybertalent. (n.d.). from https://www.sans.org/cybertalent

Cyber Threat Map. (n.d.). from https://www.fireeye.com/cyber-map/threat-map.html

Ding, Jeffrey. "Deciphering China's AI Dream," Future of Humanity Institute, University of Oxford, (2018). https://www.fhi.ox.ac.uk/wp-content/uploads/Deciphering_Chinas_AI-Dream.pdf

Deudney, Daniel, and G. John Ikenberry. "The International Sources of Soviet Change." International Security 16, no. 3 (1991): 74-118. doi:10.2307/2539089.

Department, P. (2015). Cybersecurity spending in the U.S. 2010-2018. Retrieved January 23, 2021, from https://www.statista.com/statistics/615450/cybersecurity-spending-in-the-us/

DOD Releases 2020 Report on Military and Security Developments Involving the People's Repu. (n.d.). from https://www.defense.gov/Newsroom/Releases/Release/Article/2332126/dod-releases-2020-report-on-military-and-security-developments-involving-the-pe/

Education in China: Key Facts & Statistics by China Mike. (2020). from https://www.china-mike.com/facts-about-china/facts-chinese-education/

Education in China. (2019). from https://wenr.wes.org/2019/12/education-in-china-3.

Examining the Importance of the H-1B Visa to the American Economy: *Hearing Before the Committee on the Judiciary.* Serial No. J-108-41. 108th Congress. (2003).

Executive Office of the President of The U.S., The Comprehensive National Cybersecurity Initiative (2010).

Fukuyama, F. (1992). The end of history and the last man. New York: Free Press.

Gartzke, Erik. (2019). The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. International Security, Vol. 38, No. 2, pp. 41-73 Published by: The MIT Press Stable URL: https://www.jstor.org/stable/24480930 Accessed: 27-02-2020 15:59 UTC

Garfinkel, Ben and Dafoe, Allan. (2019). How does the offense-defense balance scale?, Journal of Strategic Studies, 42:6, 736-763, DOI: 10.1080/01402390.2019.1631810

Gehl, Katherine and Porter, Michael. (2020). Fixing U.S. Politics. from https://hbr.org/2020/07/fixing-u-s-politics

Global Firepower 2020. (n.d.).from https://www.globalfirepower.com

Go Government. (2020). Background checks and security clearances for federal jobs. from https://gogovernment.org/background-checks-and-security-clearances-for-federal-jobs/

The H-1B Visa Program. (2020). from https://www.americanimmigrationcouncil.org/research/h1b-visa-program-fact-sheet

Goldsmith, B., Chalup, S., & Quinlan, M. (2008). Regime Type and International Conflict: Towards a General Model. *Journal of Peace Research, 45*(6), 743-763. Retrieved January 23, 2021, from http://www.jstor.org/stable/27640767.

Grim, J., Thapar, A., Ayers, A., Sharma, A., & Villatte, N., Wertz D., Alvarez-Fernandez D. (n.d.). 2020 cyber-espionage Report (CER). Retrieved February 10, 2021, from https://www.verizon.com/business/resources/reports/cyber-espionage-report/

Hannas, Wm. C, and Huey-meei Chang. (2019). “China's Access to Foreign AI Technology.” CSET Georgetown, Center for Security and Emerging Technology.

Heo, U., and Tan, A. (2001). Democracy and Economic Growth: A Causal Analysis. ` *Comparative Politics, 33*(4), 463-473. doi:10.2307/422444.

Herman, A. (2018). America's High-Tech STEM Crisis. from https://www.forbes.com/sites/arthurherman/2018/09/10/americas-high-tech-stem-crisis/?sh=357cfbfaf0a2

Hoekstra, B. M., and León, E. Z. (2019). Trade in the 21st century: Back to the past? Place of publication not identified: Brookings Institution Pr.

Horowitz, Michael C. (2018). Artificial Intelligence, International Competition, and the Balance of Power. Texas National Security Review, 1 (3).

How China Became Capitalist. (2020). Retrieved December 02, 2020, from https://www.cato.org/policy-report/januaryfebruary-2013/how-china-became-capitalist

Inkster, N. (2016). China's cyber power. Oxon, UK: Routledge. doi:10.4324/9780429031625

Jacobs, H. (2018). Chinese people don't care about privacy on the internet - here's why, according to a top professor in China. from https://www.businessinsider.com/why-china-chinese-people-dont-care-about-privacy-2018-6.

Jervis, Robert. (1978). Cooperation Under the Security Dilemma. *World Politics, 30*(2), 167-214. Retrieved January 23, 2021, from http://www.jstor.org/stable/2009958.

Karatzogianni, Athena. (2010). The Thorny Triangle: Cyber Conflict, Business, and the Sino-American Relationship in the Global System." Selected Works Online Academic Forum, March 2010. From http://works.bepress.com/athina_karatzogianni/11.

Kello, Lucas. (2013). The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. International Security, 38 (2), 7-40. doi:10.1162/isec_a_00138.

Kramer, F., Starr, S., & Wentz, L. (Eds.). (2009). *Cyberpower and National Security*. University of Nebraska Press. Retrieved January 23, 2021, from http://www.jstor.org/stable/j.ctt1djmhj1.

Leeds, B., & Davis, D. (1999). Beneath the Surface: Regime Type and International Interaction, 1953-78. *Journal of Peace Research, 36*(1), 5-21. Retrieved January 23, 2021, from http://www.jstor.org/stable/451101.

Leung, J. (2019). Who will govern artificial intelligence? Department of Politics and International Relations: Oxford University.

Libicki, Martin C. (2011). "Cyberwar as a Confidence Game," Strategic Studies Quarterly 5, no. 1, pp. 136-146.

Lindsay, Jon R. (2014). “The Impact of China on Cybersecurity: Fiction and Friction.” Quarterly Journal: International Security, vol. 39. no. 3: 7-47.

Litan, R. (2016). The "Globalization" Challenge: The U.S. Role in Shaping World Trade and Investment. from https://www.brookings.edu/articles/the-globalization-challenge-the-u-s-role-in-shaping-world-trade-and-investment/

Liu, Wei. "GDP and the New Concept of Development: Understanding China’s Changing Concept of Development in Regards to GDP after the Reform and Opening-up." In China’s 40 Years of Reform and Development: 1978–2018, edited by Garnaut Ross, Song Ligang, and Fang Cai, 67-74. Acton ACT, Australia: ANU Press, 2018. http://www.jstor.org/stable/j.ctv5cgbnk.12.

Lobont, O.R., Glont, O.R., Badea, L. *et al.* (2019).Correlation of military expenditures and economic growth: lessons for Romania. *Qual Quant* **53,** 2957–2968. https://doi.org/10.1007/s11135-019-00910-9

A major war between leading military powers is now impossible. here's why. (n.d.), from https://www.weforum.org/agenda/2019/07/a-major-war-between-leading-military-powers-is-now-impossible-here-s-why/

Manyika, J., McRaven, W. H., and Segal, A. (2019). Innovation and national security: Keeping our edge. S.l.: Council on Foreign Relations.

Merritt, K. (2017). Can government outpace the private sector in innovation? from https://www.nextgov.com/ideas/2016/01/can-government-outpace-private-sector-when-it-comes-innovation/125295/

Meserve, Jeanne. (2007). “Official: International Hackers Going after U.S. Networks.” from http://www.cnn.com/2007/US/10/19/cyber.threats/index. html

The National Strategy to Secure Cyberspace of the United States of America. Washington: President of the U.S, 2003. Print.

Number of Chinese students in the U.S. 2019. (2020). from https://www.statista.com/statistics/372900/number-of-chinese-students-that-study-in-the-us/

Nye, Joseph. “Cyber Power.” (2010). Cambridge, Mass.: Belfer Center for Science and International Affairs, Harvard Kennedy School.

Nye, “The Changing Nature of World Power.” (1990). p. 178.

Nye, Jr., Joseph S. (2011). Nuclear Lessons for Cyber Security? Strategic Studies Quarterly 5(4): 18-38.

O’Hanlon, M.E. (2020). Forecasting change in military technology 2020-2040. https://www.brookings.edu/research/forecasting-change-in-military-technology-2020- 2040/.

Overview. (n.d.). from https://www.worldbank.org/en/country/china/overview

"Overview of educational achievements in China in 2018". *Ministry of Education - The People's Republic of China*. 22 October 2019.

Paarlberg, R. L. (2004). Knowledge as Power: Science, Military Dominance, and U.S. Security. International Security, 29(1), 122-151.

Pevehouse, Jon C. and Goldstein, Joshua S. (2016). International Relations, Brief Edition (7th edition). Pearson Longman. ISBN 0134406354.

Ranking: Military spending by Country 2019. (2020, December 01). from https://www.statista.com/statistics/262742/countries-with-the-highest-military-spending/

Rid, Thomas. (2012). Cyber War Will Not Take Place. Journal of Strategic Studies, 35(1), 5-32. doi:10.1080/01402390.2011.608939

Segal, A. (2017). The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age. New York: PublicAffairs.

Segal, Stephanie, and Dylan Gerstel. (2019). “Research Collaboration in an Era of Strategic Competition.” CSIS Political Economy, Center for Strategic & International Studies.

Shahbaz, A. (2018). The Rise of Digital Authoritarianism. from https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism

Slater, D., & Fenner, S. (2011). STATE POWER AND STAYING POWER: INFRASTRUCTURAL MECHANISMS AND AUTHORITARIAN DURABILITY. *Journal of International Affairs, 65*(1), 15-29. Retrieved January 23, 2021, from http://www.jstor.org/stable/24388179

Snyder, Kelley M. (2019). “Artificial Intelligence and National Security.” Congressional Research Service.

Spade, J. M. (2012). Information as Power: China’s Cyber Power and America’s National Security. U.S. Army War College, 1-66.

Special economic zone. (n.d.). from https://www.britannica.com/topic/special-economic-zon

Specops. 2020. The countries experiencing the most 'significant' cyber-attacks. from https://specopssoft.com/blog/countries-experiencing-significant-cyber-attacks/

Stier, S. (2017). Internet diffusion and regime type: Temporal patterns in technology adoption. Telecommunications Policy, 41(1), 25-34. doi:10.1016/j.telpol.2016.10.005

Stokes, Bruce. (2014). “Extremists, Cyber- Attacks Top Americans’ Security Threat List.” Pew Research Center. Available at http://www.pewresearch.org/fact-tank/2014/01/02/americans-see-extremists-cyber-attacks-as-major-threats-to-the-u-s/.

Tellis, A. J. (2000). Measuring Military Capability. In *Measuring National Power in the Postindustrial Age* (pp. 133-176). Santa Monica, CA: RAND.

Tully, S. (2019). Trump's tariffs were supposed to ding china, but the u.s. economy is getting hit 2.5x harder. from https://fortune.com/2019/10/08/trump-china-tariffs-trade-war-us-economy-impact/

U.S. Government to Spend Over $18 Billion on Cybersecurity. (2020). from https:www.hstoday.us/subject-matter-areas/cybersecurity/u-s-government-to-spend-over-18-billion-on-cybersecurity/

U.S. Senate, Committee on Homeland Security and Governmental Affairs. (n.d.). *Threats to the U.S. research enterprise: China's talent recruitment plans: Staff report* (pp. 1-105) (1192000700 891099476 R. Portman & 1192000701 891099476 T. Carper, Authors) [S. Doc.]. PERMANENT SUBCOMMITTEE ON INVESTIGATIONS.

Valeriano, Brandon and Maness, Ryan C. (2015). The Contours of the Cyber Conflict World. Cyber War versus Cyber Realities, 1-19. doi:10.1093/acprof:oso/9780190204792.003.0001

Vincent, Brandi. (2019). “Energy Unveils Artificial Intelligence and Technology Office.” nextgov.com, Nextgov, https://www.nextgov.com/emerging-tech/2019/09/energy-unveils-artificial-intelligence-and-technology-office/159744/.

Voo, J., Hemani, I., Jones, S., DeSombre, W., Cassidy, D., & Schwarzenbach, A. (2020). National Cyber Power Index 2020. *China Cyber Policy Initiative - Belfer Center*.

Waddell, K. (2016). After ISIS, Americans Fear Cyberattacks Most. Retrieved January 23, 2021, from https://www.theatlantic.com/technology/archive/2016/05/after-isis-americans-fear-cyberattacks-most/481467/.

Weede, E. (1984). Political Democracy, State Strength and Economic Growth in LDCs: A Cross-National Analysis. *Review of International Studies, 10*(4), 297-312. Retrieved January 23, 2021, from http://www.jstor.org/stable/20097022.

Williamson, Murray. (2019). "Artificial Intelligence and National Security." *FAS.org*, Congressional Research Service.

World Population Review. (2020). GDP Ranked by Country 2020. https://worldpopulationreview.com/countries/countries-by-gdp

Yuen, Samson. (2015). Becoming a Cyber Power: China's cybersecurity upgrade and its consequences. French Centre for Research on Contemporary China. 2 (102), 53-58.