국제학석사학위논문

Wired For War: An Analysis of United States Cyber Security Against a Rising China

하이테크 전쟁: 중국의 부상에 대응하는 미국의 사이버 안보에 관한 연구

2017년 8월

서울대학교 국제대학원

국제학과 국제협력 전공

에멧 존슨

Wired For War: An Analysis of United States Cybersecurity Against a Rising China

하이테크 전쟁: 중국의 부상에 대응하는 미국의 사이버 안보에 관한 연구

Thesis By

Emmett Johnson

Graduate Program in International Cooperation

In Fulfillment of the Requirements

For The Degree of Master in International Studies

August 2017

Graduate School of International Studies

Seoul National University

Seoul, Republic of Korea

Wired For War: An Analysis of United States Cybersecurity Against a Rising China

하이테크 전쟁: 중국의 부상에 대응하는 미국의 사이버 안보에 관한 연구

지도교수: 송지연

이 논문을 국제학석사 학위논문으로 제출함

2017년 8월

서울대학교 국제대학원

국제학과 국제협력전공

Emmett Johnson

Emmett Johnson의 석사학위논문을 인준함

2017년 8월

위 원 장 김 태균 (인)

부위원장 Kadir AYHAN (인)

위 원 송지연 (인)

Wired For War: An Analysis of United States Cybersecurity Against a Rising China

Advisor: Professor Jiyeoun Song

Submitting a master's of International Cooperation

August 2017

Seoul National University

Graduate School of International Studies

International Cooperation

Emmett Johnson

Confirming the master's thesis written by Emmett Johnson

August 2017

Chair Taekyoon Kim **(Seal)**

Vice Chair Kadir AYHAN **(Seal)**

Examiner Jiyeoun Song **(Seal)**

Abstract

Wired For War: An Analysis of United States Cyber Security Against a Rising China

The United States hegemony is challenged by China. With China's economic and military rise, it is inevitable a power transition will take place. In this power transition from the United States to China, the use of cyberspace will be prevalent. This thesis proposes the United States' public and private sector should form a partnership that uses a multifaceted approach in protecting its interests against China. The tenets of the multifaceted approach are: 1. Dialogue between the United States government and private sector which involves inviting private sector leaders to discuss pervasive issues in cyber security; 2. Create special commission on cyber security that passes legislation to update and protect cyber security of the public and private sector; 3. Reanalyze open source and consider block chain and create a comprehensive crisis management plan; 4. Honor the U.S.-China cyber agreement and discuss the importance of cyber security with Chinese stakeholders; 5. Punish Chinese citizens who engage in espionage and push for international law for cybersecurity. This multifaceted approach is a strategy that would enhance U.S. cyber defense and protect its vital interests against a rival China.

Keywords: Cyberspace, Cyber Security, Power Transition, Cyber Attack

Student ID: 2015-25081

Table of Contents

List of Figures

1. Introduction

With the fall of the Berlin wall, and the subsequent capitulation of the Soviet Union, the seeds of pax America blossomed. Starting from the early 1990s, The United States endured a time of economic and military superiority; no challengers were present during this period. The United States became the leader in international affairs, without any significant challenges from the international community. By taking the role of the world's sole super power, many countries look towards the United States for leadership in the international arena, whether it is maintaining international order or for humanitarian reasons. It can be unanimously agreed upon that the United States became the supreme power since the end of the Cold War.

However, a new rising power presents a challenge to the United States' hegemony. China is considered a threat to U.S. dominance on the global stage. It has seen its economy grow rapidly in a matter of years and now ranks second in the world, while the United States ranks first. Furthermore, China has been increasing its military capabilities and undertaken expansionist moves. It has produced and bought state of the art military equipment to modernize its military, and expanded its reach in the South China Sea, threatening many U.S. allies. The United States, as well as its allies, now sees an aggressive power that wishes to revise the current international order. Due to this aggression, a rivalry currently ensues between the

United States and China in the pursuit of dominance on the world stage.[1] It is inevitable that these two nations will enter in some sort of conflict with each other in the near future.

Along with this potential power transition, a new creation by humanity has changed the course of international affairs. Starting from the mid 20th century, scientific-technological developments have sparked an information revolution. No other time in the history of mankind have we witnessed such a leap forward in technology. Due to these technological advancements, humanity has now created a new world, which is referred as cyberspace.[2] It is completely in its own realm, without the physicality of our own world. Many people use this world for information, communication and etc. It has now been deemed a fundamental aspect in today's society. Unfortunately, this "new world" is now being utilized by nations for national security purposes. If we look below, the history of cyberspace, as well as a progressive use of it by nations to sabotage other nations, is shown.

- Creation of Colossus: The first programmable digital machine. The Germans used "Tuny", a highly sophisticated teleprompter encryption, in World War 2. Tuny created a nuisance for the Allied powers, which

[1] Tammen, Ronald L., and Jacek Kugler. "Power Transition and U.S.-China Conflicts." Oxford Journals: Chinese Journal of International Politics 1 (2006): 35-55. Web. <http://cjip.oxfordjournals.org/content/1/1/35.short>.

[2] Tabansky, Lior. "Basic Concepts in Cyber Warfare." Military and Strategic Affairs 1st ser. Volume.3 (2011): 75-92. Web. <http://www.inss.org.il/uploadimages/Import/(FILE)1308129610.pdf>.

initially gave the Germans an upper hand. However, Colossus was made to encipher these codes by Tuny. Due to this machine, it gave the Allied powers a pivotal advantage over Axis powers, which contributed to an Allied victory.[3]

- ARPANET: First to implement TCP/IP: a basic communication language. Later on, it allowed a series of networks to join together. Thus, it was the early seed of shared networking which later spawned the Internet. [4]
- Farewell Dossier: The first cyber attack initiated by the United States. Farewell, a KGB source, informed United State officials that the USSR planned to buy computer equipment to operate a gas pipeline The United States intervened by altering the software of the computer, which caused the pipeline to explode.[5]
- Morris Worm: Robert Tappan Morris released a worm that caused 10% of 88,000 computers connected to the Internet to crash. It is considered the first worm attack that occurred on the Internet.[6]
- Creation of the Internet: APANET transformed into the Internet. When it was initially released, 2.8 million people worldwide had access to it.

[3] Robert O'Harrow and David Linch, "Timeline: Key events in cyber history," The Washington Post,

[4] Ibid

[5] Ibid

[6] Ibid

Currently, there are now over 3.2 billion Internet users.[7]

- Information War Exercise: A cyber attack exercise, Eligible Receiver, initiated by the Pentagon. Specialists conducted a simulated attack on power and communication networks in numerous cities. It found that many of these attacks succeeded in ease, with little or no resistance.[8]
- Titan Rain: Hackers, supported by the Chinese government, attacked military and government systems in the United States; an estimated terabyte of information was taken.[9]
- Operation Buckshot: A Pentagon worker inserted a flash drive in a military laptop in the Middle East; this flash drive uploaded a malicious code that a foreign power used to steal important information.[10] The malicious code was undetected on classified and unclassified systems. It is considered the most significant breach in United States history.[11]
- Operation Aurora: Google and a number of other corporations experienced a cyber breach. It resulted in stolen data, and many blame China as the originator of this attack.[12]
- Stuxnet: A worm that devastated hundreds of Iranian centrifuges. It

[7] Ibid
[8] Ibid
[9] Ibid
[10] Ibid
[11] Ibid
[12] Ibid

specifically targeted Siemen systems that were used by the Iranians for its nuclear program. Its originators were the United States and Israel.[13]

- U.S.-China Cyber Agreement: An agreement between the Chinese and Americans to refrain from cyber attacks from one another. It outlines to both nations not to engage in espionage, theft of each other's information. It remains to be seen if both nations adhere to this agreement.[14]

As we can see from timeline above, cyberspace is now an outlet for nations to engage in espionage. It first began in World War 2 and is now common in the 21st century. Cyber attacks threaten not just governments, but private enterprises as well. Anyone can be a victim to cyber intrusions; it has become one of the most pressing issues of the 21st century.

The challenge to the United States hegemony by China, as well as the existence of cyberspace, has created a new outlet for these two powers to engage in conflict. Currently, both powers are using cyberspace for espionage and sabotage. Particularly in the United States, there has been preponderance in cyber attacks, especially during the Bush and Obama administrations. Intellectual property, private information of citizens, and military intelligence has been compromised numerous times. Many U.S. officials and experts blame China for these attacks.

[13] Ibid

[14] John W. Rollins et al., "U.S.–China Cyber Agreement," Congressional Research Service Reports, October 16, 2015, , https://fas.org/sgp/crs/row/IN10376.pdf.

Therefore, The United States is in a predicament in order to protect its vital assets from Chinese intrusion. It presents a question of what policy the United States can undertake to improve its cyber security structure and protect its interests.

1. 1 Research Question

The United States has endured numerous cyber attacks within the last 15 years. According to U.S. officials and experts, many of these attacks can be traced back to China. It presents certain questions: Is the United States cyber security structure sufficient enough to protect its interests? If not, what steps in cyber security can the United States take to minimize the damage of cyber attacks?

With persistent cyber attacks and compromises on certain data, United States cyber security is inefficient in preventing cyber attacks from China. The main problems of the current policy comprises of failures to hold China accountable, create a strong cyber defense network that deters or mitigate attacks, and punish China for its actions. The exponential increase and cataclysmic attacks in the past adhere to this point. Therefore, fundamental changes are needed in U.S. cyber security. Previous studies give an outline for the United States to improve its cyber defense, but it does not go far enough. Most studies on this issue give a one step approach - such as dialogue, defense or aggression - but this current issue demands a multifaceted approach. This thesis will analyze data and case studies of

Chinese cyber attacks, and give ideas that may mitigate and deter China’s campaign of cyber attacks on the United States.

2. Background

2.1 Power Transition: United States and China

The United States' decline and China's rise may cause a conflict. In Organski's *World Politics*, Organski introduces the theory of power transition. This theory entails that the world is hierarchical, not anarchical[15]. Furthermore, Organski explains there is one "dominant" power with the largest amount of resources; there are "great powers" that rival the dominant power; "middle powers" that have some resources but cannot change the international system; and "small states".[16] Power transition theory comes into play when the "dominant" power is in decline, while a "great" power is on the rise.[17] It is inevitable for a conflict to ensue because there is a "great power" that wants to change the current international order which is ruled by a "dominant" power. In this particular case, the United States maintains the current international order and is declining, while China is rising while challenging the United States.

By applying Organski's theory, we can surmise the United States is the dominant power, while China is the great power. China is now threatening the 20 years of United State hegemony. The growing Chinese economy, as well as its increase in military spending can prove this. However, in the United States, the

[15] Organski, A. F. K. World Politics. New York: Alfred A. Knopf, 1968. Print
[16] Ibid
[17] Ibid

economy has not been as strong as before. This is coupled with a decrease in military spending, compared to previous years. Therefore, we can surmise a power transition may take place because of current trends in military spending and the economy of both countries.

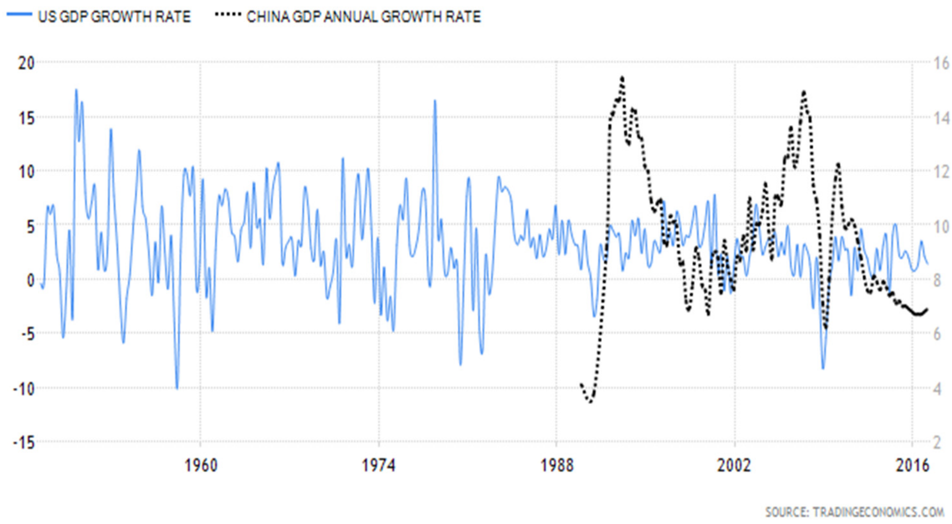


Figure 1: U.S and China GDP Annual Growth Rate
(Source: "United States and China GDP Growth Rate 1947-2015 | Data | Chart | Calendar." Trading Economics. Accessed May 03, 2017. https://tradingeconomics.com/united-states/gdp-growth-annual. Data from U.S. Bureau of Economic Analysis and National Bureau of Statistics of China)

In Figure 1 we can see the stark contrast in the amount of annual GDP growth between the United States and China. From 2004 – early 2008, the United States economy was doing fairly well. However, in 2008, the Great Recession caused its GDP to crash. President Obama's American Recovery and Reinvestment Act, which was a Keynesian economic package that consisted of an increase in public spending and tax cuts, caused the U.S. GDP to rise again.[18] Looking at Figure 1, the United States GDP is fluctuating around 2- 5% since 2010. Therefore, it has recovered, but is doing mildly well.

China's trend is quite different from the United States. Ever since it joined the World Trade Organization in 2001, its GDP has been in an upward trend, averaging 8%-15% from 2004 – 2008, according to Figure 1. This growth rate is astronomical, compared to other nations. Like the United States in 2008, its GDP did decline, but it was not as harsh as the United States. According to Baocheng Ji, China recovered because of its "unique mechanism of resource allocation, macroeconomic decision-making process functions, and the existence of state enterprises that are compatible with its economy."[19] To many people in the world during this period of time, it seemed like China would be the next leader in global trade. However, China is currently experiencing a decline, but its GDP is on the rise and does not fluctuate as much as the United States. It should not be taken as a barrier to China's rising economy.

[18] Kimberly Amadeo, "Did Obama's Stimulus Plan Work?," The Balance, , https://www.thebalance.com/what-was-obama-s-stimulus-package-3305625.

[19] Baocheng Ji, "China's economic recovery and the China model," Renmin University of China 8, no. 3.

In addition to China's strong economy, it has improved its military as well. China has rapidly increased its military spending and modernized its equipment. According to Edward Wong and Chris Buckley, China has increased its military spending over the year, mainly due to its economy, and is ranked second only to the United States.[20] Now, there is an expected increase of 7% in 2017.[21] With this increase in military spending, China is modernizing its military. New equipment, ships, aircrafts and other military related ventures have been undertaken. Its aviation technology is closing the gap with the United States, and has created a new array of weapons that challenges United States interests in the Pacific. As we can see, China's military spending and modernizing army presents a challenge to the United States.[22]

Furthermore, China has been more aggressive in East Asia. It has island disputes with neighboring countries (Philippines, Japan, Vietnam and etc.) and creates artificial islands, which is causing unease with traditional United States allies and even non-allied powers. We see examples of countless standoffs with neighboring nations by aircrafts and ships that created a highly volatile region. China even refused to obey international law on these island disputes. When the

[20] Edward Wong and Chris Buckley, "China's Military Budget Increasing 10% for 2015, Official Says," The New York Times

[21] Ben Kentish, "China announces plans to increase military spending by 7 per cent," The Independent

[22] Paul McLeary, "Pentagon: Chinese Military Modernization Enters," Foreign Policy, May 13, 2016, , http://foreignpolicy.com/2016/05/13/pentagon-chinese-military-modernization-enters-new-phase/.

Permanent Court of Arbitration ruled in favor of the Philippines, China flat out refused to obey the ruling.[23] China's increase in military spending, and its aggression in the South China Sea all points towards a revisionist country that challenges the United States.

However, unlike China, the United States' military spending has been on a downward trend. According to Dinah Walker, the United States has been on a decline in spending since 2010.[24] This is mainly due to the Budget Control Act (also known as the 2013 sequester but was passed in 2011), which cuts funding in military and domestic programs starting in 2013.[25] This deal guts the military in the most vital areas, which explains the decline in military spending, compared to previous years. Furthermore, the exhaustion of foreign intervention by the United States also plays a role in reduced military spending. The wars in Iraq and Afghanistan mentally drained a major part of the U.S. populace; many Americans feel uneasy with an increase in military interventions. Therefore, a consequence in this is reduced military spending that downplays further military ventures abroad. Since 2010, we have seen a downward trend in military spending in the United States because of the Budget Control act, as well as an exhausted populace that is still recovering from war.

[23] Panda, Ankit. "International Court Issues Unanimous Award in Philippines v. China Case on South China Sea." The Diplomat. N.p., 12 July 2016. Web.
[24] Dinah Walker, "Trends in U.S. Military Spending," Council on Foreign Relations
[25] Khimm, Suzy. "The sequester, explained." The Washington Post. September 14, 2012..

The trends in military and economic of the United States and China point towards a power transition. However, the limitation of Organski's theory in the context of the potential power transition between the United States is the use of cyberspace. Organski could have never predicted its use in a power transition. His theory only outlined economic, military and political in a power transition. Therefore, we must take in to account this new method in power transitions. In the case of China and the United States rivalry, cyberspace is new concept used by both powers.

2.2 Cyberspace and Chinese Cyber Attacks

According to the Merriam-Webster dictionary, Cyberspace is "The online world of computer networks and especially the internet".[26] It is a world where information is stored and communication is easily accessible. In Lior Tabansky's article, we see the tenets of cyberspace. First, cyberspace is composed by all the computerized networks in the world, and is controlled by commands that go through these networks.[27] Second, cyberspace has three layers to it: physical layer, software logic, and a layer of data that machines contain and disseminate

[26] "Cyberspace," Merriam-Webster Dictionary
[27] Tabansky, Lior. "Basic Concepts in Cyber Warfare." Military and Strategic Affairs 1st ser. Volume.3 (2011): 75-92.

information.[28] Third, much of cyberspace is controlled by private and cooperative organizations without geographical boundaries.[29] Fourth, cyber space is highly complex and constantly changes.[30] It is basically a new world where information is freely flown and communication can happen.

Currently, many people across the globe embrace cyberspace. The free exchange of information and communication with one another is a major achievement of this cyberspace. Statistically, we see an overall increase in the usage of the internet/cyberspace in the past 10 years. In Figure 2, we see a rise from 1,000 millions users worldwide in 2005 to over 3,000 millions of users worldwide in 2015. This is mainly due to cyberspace being more accessible to the general populace. More people are using the Internet as a convenient way to share and store information. Starting as a weapon before the post-Cold War era, it is now accessible to everyone. It has become a new norm it today's global society.

[28] Ibid
[29] Ibid
[30] Ibid

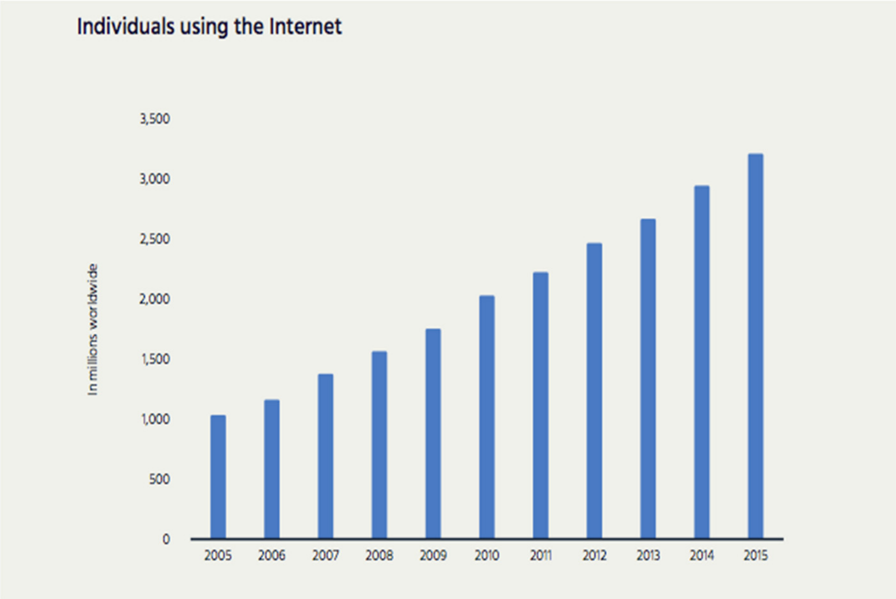


Figure 2: Individuals Using the Internet

(Source: "Global Internet Report 2016." Internet Society. Pg. 32, https://www.internetsociety.org/globalinternetreport/2016/wp-content/uploads/2016/11/ISOC_GIR_2016-v1.pdf.
Data from ITU 2016

In theory, everyone should rejoice the use of this new “world”, since it brings the world closer together. However, many nations, as well as groups and individuals, use cyberspace for espionage and sabotage. This encompasses meddling in elections, stealing intellectual property, conducting military espionage and etc. We see a preponderance of stories in the world that deal with cyber attacks. In Figure 3, we can see the amount of cyber attacks in recent years. From 2013 – 2015, we see an increase in the number of incidents, with the biggest increase occurring in 2013-2014. These breaches reveal a trend that is happening in the 21st century. Cyber attacks are now used to benefits one's own gain at the expense of another. We can surmise this will be a common occurrence for the future.

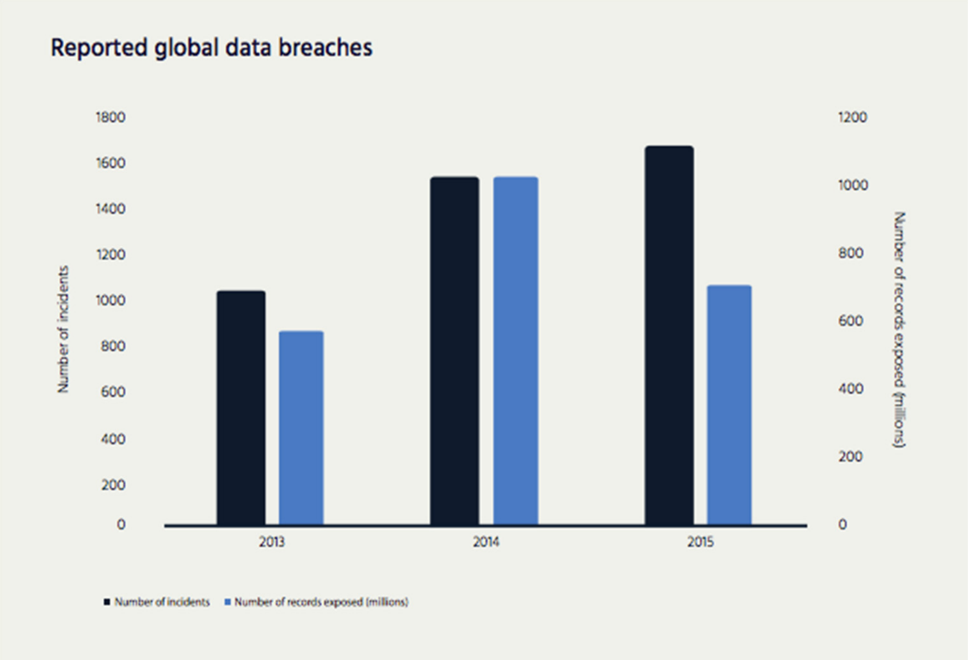


Figure 3: Reported Global Data Breaches

Source: "Global Internet Report 2016." Internet Society. Pg. 37, https://www.internetsociety.org/globalinternetreport/2016/wp-content/uploads/2016/11/ISOC_GIR_2016-v1.pdf.

There are a couple of reasons for its cyberspace's frequent use for data breaches. According to Lior Tabansky, it is cheap and efficient to undertake, compared to other methods, and is hard to trace,[31] Rather than investing in other military methods such a missiles and other weaponry, which cost an astronomical amount to use, it is cheaper to use cyber attacks. This is coupled with no evidence of the perpetrator. This can leave the cyber attacker virtually unscathed in a cyber attack. Second, it is expensive for another power and requires constant communications on all levels to prevent a cyber attack.[32] A cyber attack can cause massive amounts of damage to a nation or corporation. The amount of time and resources to recover is much higher, compared to undertaking a cyber attack. In addition, there are no international laws that dictate cyber warfare.[33] Therefore, anyone can undertake this attack without repercussions from international law. This is unlike conventional war, which the Geneva Convention dictates the laws of war. These reasons are why the use of cyber attacks has become more popularized in the 21st century.

In the case of China, the use of cyber attacks has become very common. Gabi Siboni and Y.R. argue China uses cyber attacks to access military information,

[31] Tabansky, 88
[32] Ibid
[33] Tabansky. 82

cutting-edge technology and other assets.[34] This would allow China to steal vital information and conduct industrial espionage against nations and commercial competitors.[35] It would boosts its domestic firms against international competition by taking information from foreign firms, and benefit its own government by gaining insight from other nations. The duality of these two benefits greatly magnifies the preponderance of cyber attacks by China. This can explains why the United States has experienced a massive amount of attacks by China within the last 15 years.

Furthermore, another reason China uses cyber attacks is to justify its government. According to Amy Chang and Joseph Nye, China's main foreign policy objective is to ensure the longevity of the communist party.[36] This is gained by domestic stability, territorial integrity, modernization, and economic growth, while at the same time preparing for a cyber conflict.[37] Beijing's main cyber strategy consists of three main component drivers: economic, political and military.[38] It uses cyberspace to protect its interests, and sabotage those who are a threat to the communist party. By looking through the lens of the Chinese government, we can understand why China's acts the way it does. It sees the

[34] Gabi Siboni and Y. R., "What lies behind Chinese Cyber Warfare," Military and Strategic Affairs 4, no. 2 (September 2012)

[35] Gabi Siboni and Y. R, Pg. 50

[36] Chang, Amy, and Joseph Nye. "Warring State China's Cybersecurity Strategy." Center for a New American Security (2014): pg. 7

[37] Ibid, pg.8

[38] Ibid

United States as a danger to its regime. Therefore, using cyberspace against the United States is a way for China to insure its longevity.

Once created as a place of information and communication, cyberspace is now being exploited as an offensive weapon. Individuals, group, and nations are using it to steal and attack the private and public sector. In the case of China and the United States, we see China using cyber attacks against the United States. Its main reason is to steal vital information and cutting-edge technology for its own purposes, and strengthen the communist party in China. The duality of these two things would give China an upper hand in this potential power transition.

3. Previous Studies

Previous studies outline the steps the United States can take to mitigate such attacks and protect its interests, while maintaining its hegemony. Kenneth Lieberthal and Peter Singer give us 6 points that the United States can do. Most of their arguments stem from a cooperation stance with China. These two authors believe dialogue and mutual agreements with China is possible. First, is to "expand engagement to match the growth of the problem".[39] This entails a bigger approach than the traditional two-track approach. Lieberthal and Singer argue that all experts in this field should come and discuss the issues at hand. Second, "Focus initially on building shared aims and identifying activities that both sides deem harmful".[40] China and the United States should come to terms to mutually identify things that are deemed criminal. Third, "make explicit the norms that are currently built into the global Internet system"[41] Lieberthal and Singer express that common values in cyberspace must be accepted on both sides. Fourth, "Examine Models of cooperation":[42] The United States and China should look at agreements on the environment, terrorism, financial sectors and etc. as a basis for cyber agreements.

[39] Kenneth Lieberthal and Peter W. Singer, "Cybersecurity and U.S.-China Relations," Brookings, February 2012.
[40] Ibid
[41] Ibid
[42] Ibid

Fifth, “address the attribution problem”.[43] The United States and China must find a common ground between positives of freedom of using cyberspace, and the negatives of remaining anonymous in cyberspace. Finally, “Discuss the red lines that could provoke major conflict if crossed”.[44] Both sides should discuss the scale of escalation that can be used if provoked by a cyber attack. By doing this, it can reduce the risks of a major conflict. Basically, Liberthal and Singer’s study is based on mutual understanding and cooperation between the United States and China. Both authors see dialogue as a way to protect U.S. interests, not aggression.

A limitation to Lieberthal and Singer’s recommendation is the assumption that China believes cyber issues is important. However, that is not the case. According to Scott Warren Harold, Martin C. Libicki and Astrid Stuth Cevallos, China has a differing view on cyber security, compared to the United States. In their interview with multiple Chinese officials and experts, many of them did not see cyber security has a major issue.[45] This is strikingly different from U.S. officials and experts who see cyber security as one of the most important issues in the 21st century. Advocating dialogue is necessary, but it should be taken with precaution. Furthermore, their study lacks a domestic plan. It solely focuses on

[43] Ibid

[44] Ibid

[45] Scott Warren Harold, Martin C. Libicki, and Astrid Stuth Cevallos, "Getting to Yes with China in Cyberspace," RAND, 2016, , http://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1335/RAND_RR1335.pdf.

dialogue with China, not improving U.S. cyber security. These are the limitations in Lieberthal and Singer’s study.

Jeffrey Bader is in line on the concept of mutual dialogue and understanding, but he has an aggressive approach as well, unlike Lieberthal and Singer. In his argument, he claims China and the United States can attempt to cooperate, but both have a vastly different outlook on cyber issues.[46] Judging from this, it would be hard to compromise concrete plans on cyberspace. Therefore, Jeffrey Bader argues that the United States should take a slightly hardline approach. His recommendation is to punish Chinese firms in the United States that benefit from Chinese cyber attacks.[47] He supports this logic because Chinese firms are beneficiaries from cyber attacks, at the expense of interests of the United States. In summary, Jeffrey Bader argues that the United States should undertake in dialogue, but it should also punish Chinese firms in the United States that benefit from China’s cyber espionage campaigns.

The limitation with Bader’s study is that punishing Chinese firms will ultimately lead to retaliation by China on U.S. firms. Many U.S firms, such as Google, Apple and etc., have interests in China. These firms would be the first targets of retaliation by the Chinese government. Furthermore, many Chinese firms that operate in the United States now provide manufacturing jobs; American jobs

[46] Jeffrey Badar, "A Framework for U.S. Policy Towards China," Brookings, pg. 10
[47] Ibid, pg. 11

that were lost due to globalization and technology. According to Kevin Lui, Fuyao Glass is using old General Motor assemblies, which now employ Americans, to manufacture their goods.[48] This is a growing trend in the U.S., which has seen Chinese firms invest around $200 billion in the United States.[49] It would be bad for the blue-collar American worker, as well as the U.S. economy as a whole if retaliatory steps were taken. Harsh retaliation would be detrimental for the United States, as well as China, to engage in such measures. Therefore, taking retaliatory measures on Chinese firms that operate in the United States are unwise.

Robert D. Blackwill and Ashley J. Tellis take a hardline approach, compared to the previous two studies. Black and Tellis argue that the United States has been far too lenient in cyber attacks by China. Their argument of an aggressive stance has 4 points. First, like Jeffrey Bader's argument, The United States should impose costs on Chinese firms that benefit at the expense of American firms. Blackwill and Tellis claim that tariffs on Chinese goods are a good starting point for this initiative.[50] Second, is to increase the offensive capabilities of cyber attacks by the United States.[51] This would deter China from using cyber attacks

[48] Kevin Lui, "Meet the Chinese Billionaire Who's Moving Manufacturing to the U.S. to Cut Costs," This Chinese Billionaire Is Moving Production to the U.S. to Cut Costs | Fortune.com, December 22, 2016, , accessed May 08, 2017, http://fortune.com/2016/12/22/us-china-manufacturing-costs-investment/.

[49] Ibid

[50] Robert D. Blackwell and Ashley J. Tellis, "Revising U.S. Grand Strategy Towards China," Council on Foreign Relations, no. 72, Pg. 26

[51] Blackwell and Tellis, pg.27

because of the deep repercussions that would come from it. Third, is to increase United States cyber defenses. The only way this is possible is through congressional law, which Blackwill and Tellis advocate.[52] Fourth, is to implement laws that would protect private sectors sharing intelligence with each other and even the government.[53] This act would diminish the fear of lawsuits and cause greater security. These four points advocated by Tellis and Blackwill.

The limitation with Blackwill and Tellis' argument is that it does not include dialogue and agreements with China. Black and Tellis fully commit to offensive capabilities, U.S. cyber defense and laws to protect U.S. interests. However, dialogue and engagement with China is necessary to reduce the amount of cyber intrusion. Without dialogue, it will only lead to brinksmanship and even greater cyber attacks. The mission is to reduce and prevent cyber warfare, not promulgate it. Furthermore, tariffs can possible cause a trade war with China, which would hurt United States consumers. The strategy should be preventing Chinese attacks, while having the best interests of the United States economy. Therefore, Blackwill and Tellis' study could add a dialogue element, and remove the idea of tariffs.

In a Task Force Report by Orville Schell and Susan L. Shirk, there are numerous arguments for the United States administration to take. First, The United

[52] Ibid
[53] Ibid

States should assess the risks and costs of cyber intrusion, and gather data if China reduced the scope of its hacking efforts.[54] This would give a crisis management plan for an attack, and track the tendencies of China's cyber attack. Second, improve security and crisis communications across the United States, as well as create a stronger partnership with the private sector to respond to hacking crises accordingly.[55] According to this idea, U.S. companies can quickly inform one another and the government of a possible attack. It can also represent solidarity against cyber intrusions by China. Third, the United States can engage with Chinese stakeholders to reduce the amount of attacks.[56] There can be common ground between the United States and Chinese stakeholders about the risks of cyber intrusions. Using the argument of cyber attacks being detrimental to all can be a strong argument. Fourth, the United States can use multilateral norms and institutions to pressure China in its behavior.[57] The United States can call upon its allies to create a united stand against China, use international venues - G20 and G7-, and multilateral organizations –WTO- to pressure China. These are the main arguments given by Schell and Shirk.

[54] Orville Schell and Susan L. Shirk, "U.S. Policy Toward China: Recommendations For a New Administration," Asia Society , February 2017. Pg. 33
[55] Schell and Shirk, Pg. 34
[56] Ibid
[57] Ibid

Of all the previous studies, I agree with most of the ideas discussed by Schell and Shirk. I would add on a strong push by the United States to create international law discussing the use of cyber attacks. This would implicate China even more if they engaged in these acts. It would show the world that China defied international law. Furthermore, a discussion about the flow of information in cyberspace may be required. Perhaps a tracking of history is required, in the case of national security. These are the few limitations I found in Schell and Shirks study, but most of the arguments I concur with Schell and Shirks.

Overall, most of these previous studies do give a positive step forward for the United States to protect itself. Some of the previous studies need elements from one other. If some sections of each literature were parsed together, it would give a robust policy that would give the United States a stronger way forward in its cyber security.

Author(s)	Argument	Limitations
Lieberthal and Singer	6 points of dialogue and mutual agreements	Lacks a domestic plan and China, and the United States do not agree on cyber issues
Jeffrey Bader	Dialogue but punish Chinese Firms	Retaliation on U.S. Firms
Blackwill and Tellis	4 Aggressive Points	No dialogue and it may cause more friction
Schell and Shirk	Robust Defense, Dialogue, International Institutions, and partnership between the private and public sector	International Law not discussed as a choice for the international level

Figure 4: Previous Literature on U.S. Cybersecurity

4. Analysis

4.1 Statistics of Chinese cyber attacks

The amount of cyber attacks by China is astronomical, compared to other countries. The data provided by Akamai gives the number of attacks by country, which is traced by an IP source. It clearly ranks China as number 1 for numerous quarters in 2013-2014. Therefore, China's campaign of cyber espionage can be empirically proven by the data given by Akamai.

By looking at Figure 5, we can see China has the number 1 country that perpetrates cyber attacks via percentage. In 2013 Quarter 3, it accounted for 43% of worldwide hacks; 35% in 2013 Quarter 4; 41% in 2014 Quarter 1; and 43% in 2014 Quarter 2. During this period, the United States is far lower than China, and even the rest of the world is nearly equal to China. It is by far the biggest perpetrator of cyber intrusions during these first 4 quarters in Figure 5, accounting nearly 40% worldwide.

We can also see a decrease in cyber attacks by China in Figure 5, but it still remains the top perpetrator of cyber intrusions. In 2014 Quarter 3, China attributed to 49% of cyber intrusions; 41% in 2014 in Quarter 4; 18 % in 2015 Quarter 1; and 23% in 2015 Quarter 2. China still accounts around 1/3 of total attacks during these 4 quarters. Furthermore, there is a trend of other countries increasing their attacks, however, it is not as substantial as a single country like China.

In the case of the United States, it did commit these attacks as well, but it is still far lower, except in 2015. In 2015, we can surmise that tensions between the two nations were at an all time high, in regards to cyber warfare. It was in 2015 when the U.S.- China Cyber agreement was created. Therefore, the United States was tired to China's continuous campaign and retaliated until the agreement was made. After the agreement was made, we see an overall decrease of the United States that points towards normal levels.

By looking at Figure 5, we can infer that China is the largest perpetrator of cyber attacks. It outshines every other country, and even the United States is not on par. It may be slightly decreasing overall, but it still ranks as the top initiator of cyber intrusions. The trend shows China's operations in cyberspace will be strong and continuous in the coming years.

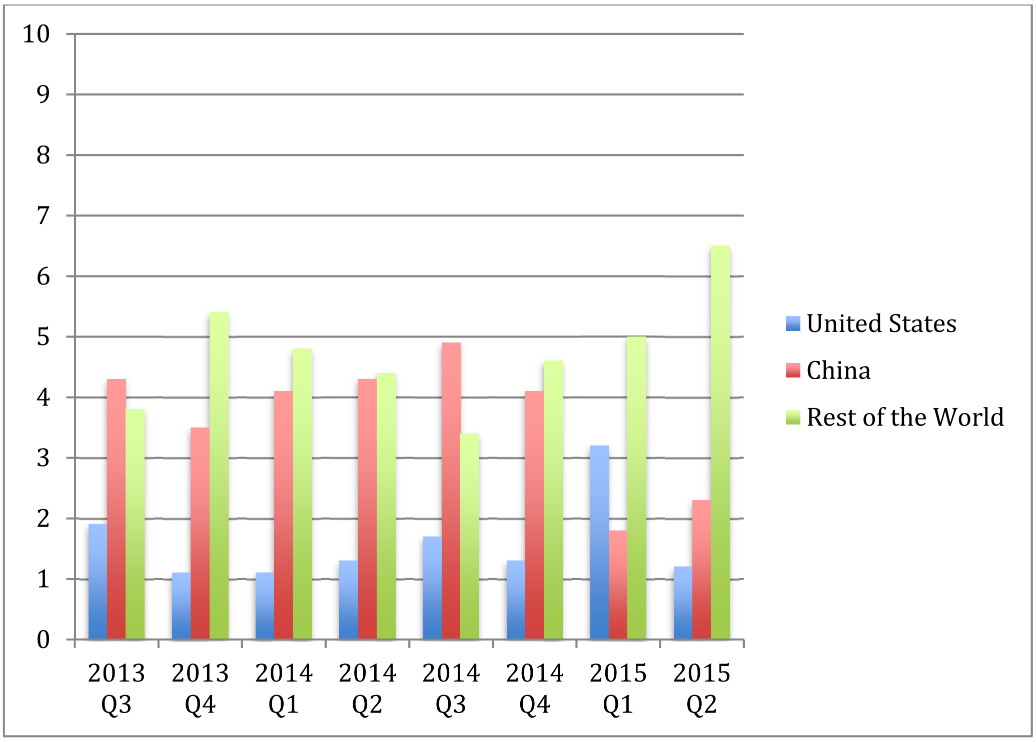


Figure 5: Source Countries of Distributed Denial of Service (DDoS) Attacks; IP Source Count

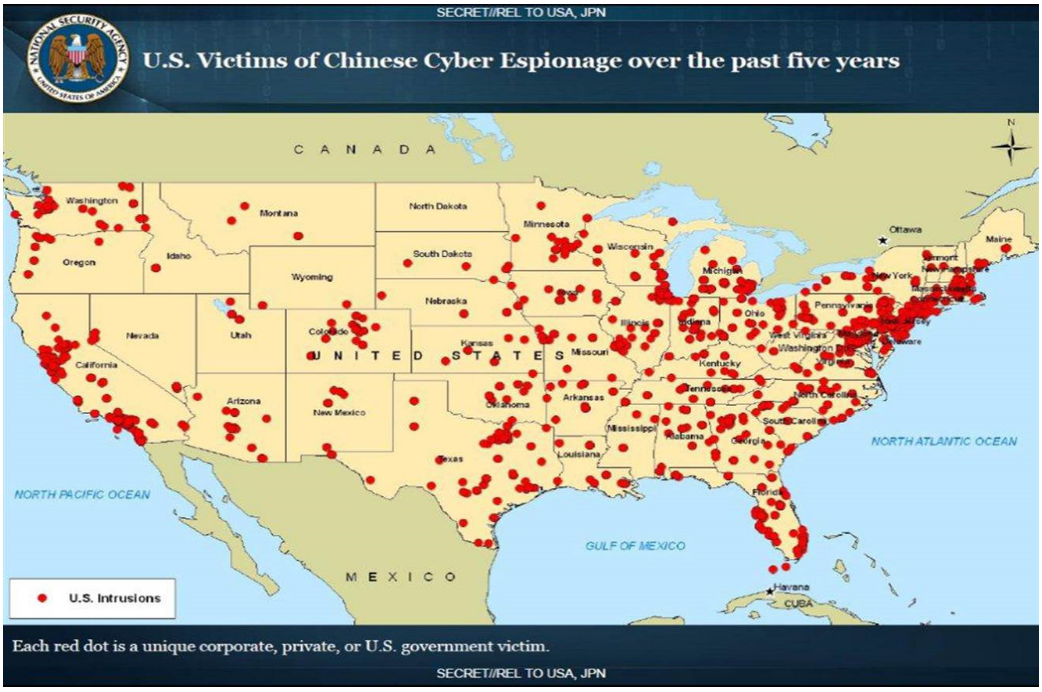
Data from Akamai: State of the Internet Report, 2013-2015
Note: 0=0%, 10 = 100%

Furthermore, according to Robert Windrem, there have been hundreds of attacks on U.S firms and United States government and military. In a secret NSA map, obtained by NBC and Robert Windrem, we see the amount of attacks in the United States. According to this report, over 600 private companies, ranging from major firms (Google and Lockheed Martin) and the US. Government and military were attacked over a 5-year period.[58] In Figure 6, each red dot on the NSA map represents a successful Chinese cyber intrusion. These attacks were on the east coast, where many military and financial centers are, as well as the west coast, where many tech firms are located. This attack pilfered “everything from specifications for hybrid cars to formulas for pharmaceutical products to details about U.S. military and civilian air traffic controls systems”.[59] The hackers from China wanted to obtain critical information and technology for China’s benefit. On a positive note, the NSA did track down the IP address of these attacks, which goes to show the NSA can trace the perpetrators.[60] It goes to show China’s campaign of cyber espionage has been persistent and successful in the United States, but still can be tracked.

The data from Akamai proves China as the world leader in cyber attacks. As a repeated offender, The United States and the international community must pressure China to curtail its campaign. It threatens the interests of international commerce and even the national security of many nations. It is not a United States problem, but a worldwide problem. Furthermore, China’s hundreds of attacks on United States government, military, and U.S firms indicate it’s been a consistent widespread problem for the United States. China and its hackers have

[58] Robert Windrem, "Exclusive: Secret NSA Map Shows China Cyber Attacks on U.S. Targets," NBCNews.com, July 30, 2015,
[59] Ibid
[60] Ibid

compromised important intelligence and technology in the United States. According to these statistics from Akaimai and NSA's map of compromised targets in the United States, it does not seem like China will lose its place as the leading perpetrator of cyber intrusion. Therefore, the United States must look towards a plan that may deter and mitigate damages from Chinese cyber intrusion.



SECRET//REL TO USA, JPN

U.S. Victims of Chinese Cyber Espionage over the past five years

Each red dot is a unique corporate, private, or U.S. government victim.

SECRET//REL TO USA, JPN

Figure 6: U.S Victims of Chinese Cyber Espionage Over the Past Five Years

Source: Windrem, Robert. "Exclusive: Secret NSA Map Shows China Cyber Attacks on U.S. Targets." NBCNews.com. July 30, 2015. Accessed May 09, 2017. http://www.nbcnews.com/news/us-news/exclusive-secret-nsa-map-shows-china-cyber-attacks-us-targets-n401211.

Note: Map from NSA

4.2 Titan Rain

In 2003, a group of Chinese hackers started a process of cyber intrusion against important government targets in the United States. Many United States officials and experts argue the Chinese government sponsored these hackers, but Beijing vehemently denies it. In their operations, these hacks would try every day to access sensitive material in the United States. The main goal was to steal vital intelligence, mainly from the public sector, that can be used for China's own benefit. This would range from military equipment, logistics and technological advances in the armed forces. These operations were dubbed as "Titan Rain" in the United States.

In 2004, these hackers made their biggest breakthrough. China's Titan Rain operation infiltrated the public sector in 2004 and compromised a vast amount of military and government intelligence. This cyber attack is considered one of the most significant breaches in U.S. history. According to Nathan Thornburgh:

"They hit hundreds of computers that night and morning alone..At 10:23pm, Pacific Standard Time (PST), they found vulnerabilities at the U.S. Army Information Systems Engineering Command at Fort Huachuca, Arizona. At 1:19

am PST, they found the same hole in computers at the military's Defense Information Systems Agency in Arlington, Virginia. At 3:25am, they hit the Naval Ocean System Center, a defense department installation in San Diego, California. At 4:46 am PST, they struck the United States Army Space and Strategic Defense installation in Huntsville, Alabama"[61]

This group of hackers made their biggest breakthrough, mainly due its new weapon: The scanner program. This program would scan vulnerabilities in military networks to find a single computer that these Chinese hackers can attack later. [62] After the scan is undertaken, the attackers would exploit the computer a couple of days later.[63] The Chinese hackers found dozens of computers that were found to be vulnerable. They soon attacked days later, which prompted the massive scale of stolen data. The worst part of this attack was the lack of trails by the hackers; none of the hacks were detected until it was too late.[64] This made it easy for the Chinese government to deny it had a role. According to James Andrew Lewis, "The Chinese intelligence services are generally not so clumsy as to leave a trail of foot prints leading from the scene of the crime back to China. The goal in an intelligence activity like this is to have 'plausible deniability, the ability to have

[61] Nathan Thornburgh, "Inside the Chinese Hack Attack," Time
[62] Ibid
[63] Ibid
[64] Ibid

your foreign ministry issue a sniffy statement that credibly proclaims innocence."[65] The hackers gained critical information about U.S. military and government intelligence in a matter of days. With the power of the scanner program, this mission of data espionage was achieved. Initially, there was no traceable evidence and the Chinese government vehemently denied any involvement. Only as time passed did we finally see a connection. It is considered one of the worst hacks in American history.

Titan Rain showed the United States' cyber security in its military and government was insufficient. Within days, many key U.S. military and government departments were hit. Most surprisingly was the confusion each department was in when the intrusion happened. There was no communication from each department during the attack. Only after the incident did each department realize they were simultaneously intruded. Looking at Titan Rain, the lack of communication proved to be a significant problem in this intrusion. It proves the deficiency in a plan to respond to cyber attacks. In such a crisis, there should be a plan to respond to such circumstances. According to Lee Chung Min, crisis communication is one of the fundamental aspects in managing a crisis.[66] Since the United States was unaware of such cyber attacks occurring, it showed its novice response to cyber espionage.

[65] James Andrew Lewis, "Computer Espionage, Titan Rain and China," Center for Strategic and International Studies,

[66] Lee, Chungmin. "Escalation and De-escalation." Crisis Management. Yonsei Gsis, Seoul. Lecture.

Furthermore, this operation proved the technology was outdated to prevent the scanner program from succeeding and even the United States government from detecting it. The scanner program entered undetected and surveyed the field for potential computer to hack. As a fairly new creation, it succeeded without any hesitation. Only after a few days it surveyed the field, the attacks in China sprung their offensive, without leaving a trace. This means the government tools used in preventing such intrusions are relatively outdated. An update and even acquiring new technology may cause a faster response and tracing the technology used in Titan Rain. This could perhaps come from the private sector where evolutions in technology are constant.

The U.S. response to Titan Rain was tepid because most of the action taken by the United States was strictly to blame China. U.S officials asked China to take full responsibility for the attack, but the Chinese government refused, citing a lack of evidence in the United States' claim.[67] The United States was in a bad position because the scanner program did not leave concrete evidence. In addition to this victim attitude, the United States did not take necessary action in improving its defense. Rather, it made little steps but did not change its fundamental problems. Therefore, we can categorize the United States response as a failure.

Titan Rain shows two fundamental deficiencies in United States cyber

[67] Nathan Thornburgh

security. First, the lack of communication between each department once the attack commenced. It took a while for each United States government and military department to realize they were under siege. Secondly, each department lacked up to date technology. The scanner program was undetected and finished its mission without any repercussions. It caught the United States government and military governments off guard, and China gained vital intelligence and logistics. The U.S response to this also proves its inability to learn from this event. Rather than updating its security, it engaged in blaming China. This still did not address its inherent problem in its cyber system. The events of Titan Rain showed the vulnerability of the United States' cyber security system, as well as the United States' hubris.

4.3 Operation Aurora

In 2009, the United States experienced another cyber attack. However, unlike Titan Rain, which aimed at the U.S. government, these attacks were on the private sector. In an unprecedented attack on United States firms - Google, Adobe and other major companies were targeted by a group of Chinese hackers. According to Dimitri Aplerovtich, the McAfee vice president of threat research, there was no attack of this magnitude, outside of the public sector, in commercial industries.[68] It basically is a game changer, in terms of cyber targets from hackers. From this intrusion, countless intellectual property and personal information were compromised, and it became apparent U.S. private firms were targets of cyber intrusions as well.

According to Syphos, the hackers of Operation Aurora used a malware attack that exploited the Internet explorer's zero-day flow. [69] A zero day flaw is a hole in the software that is unknown to the user.[70] By exploiting this hole, they were allowed to upload multiple malware and encryptions, and even hid their activities from U.S firms. The way this was possible was by sending a URL to the website of the hackers, either instant messaging or email.[71] Kim Zetter states, "Once the user visited the malicious site, their internet explorer browser was exploited to download an array of malware to their computer automatically and transparently."[72] After this, they would upload their info into a folder named "Aurora" where it would be compiled and downloaded. The hackers were able to take substantial information, ranging from intellectual property and emails of human rights activist. [73] All in all, over 40 companies were hit by this attack.

[68] Kim Zetter, "Google Hack Attack Was Ultra Sophisticated, New Details Show," Wired

[69] "Operation Aurora," Operation Aurora Malware Removal | Sophos Security Topics, , accessed May 10, 2017, https://www.sophos.com/en-us/security-news-trends/security-trends/operation-aurora.aspx.

[70] "What is a Zero-Day Vulnerability?" *Symatec.*

[71] Kim Zetter

[72] Ibid

[73] Ibid

Google was first to announce this attack, and then Adobe did the same a couple of minutes after. These companies came out in unison said these hackers attacked areas of high importance. It soon became apparent this was a wide campaign against U.S. firms.

Like Titan Rain, this attack proved there was not an effective crisis management plan. Each corporation came out admitting they were hacked, but none were warned by each other. It was only after Google announced it was attacked to the public, did other corporations come forward as well. First, we can infer there is no crisis management plan in dealing with cyber intrusions. This lack of planning may stem from the notion of being oblivious to a foreign entity's attack. It was only after this operation that private firms because aware of such campaigns. Second, private firms do not have any communication with each other about cyber attacks. This is due to the lack of streamline between the private sectors. Each corporation announced the attacks a couple of days/weeks later, and soon realized it was a part of a state-sponsored operation. Unlike the U.S. government and military departments, which work together, private firms work solely for themselves.

Furthermore, the private sector does not have the information to repel a foreign nation intruding in its intellectual property. Unlike the public sector, where defense against a foreign power is well versed, the private sector is relatively unknown to the concept of a foreign entity intruding its servers to gain an advantage. According to William Jackson's interview of George Kurtz, – McAfee's Chief Technology Officer -, "..these sorts of attacks happen all of the time from government to government. There is a lot of speculation that it was China, and if you believe that was the case, you have a situation in which you have attacks from government into corporate entities".[74] To many security experts, this is unheard of. However, this is a common occurrence for governments and their military.

The U.S. response to the attacks was in twofold. The private firms warned its user about the potential of getting hacked. Microsoft, the creator of Internet Explorer, issued a warning to individual and companies using its products about the hacks.[75] It further investigated on what happened and how the Internet Explorer hole was exploited. Google, conversely, thoroughly researched the attack and traced it back to 2 Chinese schools that have relations with the Chinese military.[76] With this information, they blamed the Chinese government. As for the United States government, it assisted the private firms in recovering and investigating these attacks; the National Security Agency's computer experts assisted Google in tracing these attacks. This is one of the first times the private and public sector

[74] William Jackson, "How Google attacks changed the security game," GCN
[75] Elinor Mills, "New IE hole exploited in attacks on U.S. firms," CNET
[76] John Markoff and David Barboza, "2 China Schools Said to Be Tied to Online Attacks," The New York Times

worked together, which is a complete contrast to Titan Rain. Even though it was not a full partnership, it proved that these two entities working together could make headway in cybersecurity.

Operation Aurora represented an attack against U.S. firms by a foreign nation. By exploiting the zero-day flaw on Internet Explorer, the hackers gained access to intellectual property of over 35 United States firms. This attack showed U.S. firms were caught unaware of a foreign entity engaging in cyber attacks on them, as well as the lack of communication between private enterprises. The response by the private sector was a full on investigation by each corporation. In addition to this, the United States government assisted these private firms and made breakthroughs in their investigation. This proved that the private and public sector working together could improve its defense and detect potential intrusions. Even though it was a small partnership, it shows the potential of a full on partnership.

5. U.S.- China Cyber agreement

With cases such as Titan Rain an Operation Aurora, the United States accused China of endorsing cyber warfare. The hostility of these two nations became more intensified when the U.S. Department of Justice indicted 5 Chinese nationals, accusing them of assisting Chinese firms by taking information from U.S. firms and handing it to Chinese firms.[77] The counts by the Department of Justice against these 5 defendants included a multitude ways of cyber espionage against United States interests. The government of China expressed outrage in the ruling. This caused the President of China to send delegates to Washington D.C. to negotiate, which created a landmark agreement on cyberspace between the two nations.

In 2015, The U.S. and China made the U.S.- China agreement. According to the Office of the Press Secretary of the White House, the tenets of the U.S. cyber agreement are:

> *"The United States and China agree that timely responses should be provided to requests for information and assistance concerning malicious cyber activities. Further, both sides agree to cooperate, in a manner consistent with their respective national laws and relevant international*

[77] "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage." The United States Department of Justice

obligations, with requests to investigate cybercrimes, collect electronic evidence, and mitigate malicious cyber activity emanating from their territory. Both sides also agree to provide updates on the status and results of those investigation to the other side, as appropriate." [78]

"The United States and China agree that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors "[79]

"Both sides are committed to making common effort to further identify and promote appropriate norms of state behavior in cyberspace within the international community. The two sides also agree to create a senior experts group for further discussions on this topic." [80]

"The United States and China agree to establish a high-level joint dialogue mechanism on fighting cybercrime and related issues. This mechanism will be used to review the timeliness and quality of responses to requests for information and assistance with respect to malicious cyber activity of concern identified by either side. As part of this mechanism, both sides

[78] "FACT SHEET: President Xi Jinping's State Visit to the United States," The White House: President Obama
[79] Ibid
[80] Ibid

> *agree to establish a hotline for the escalation of issues that may arise in the course of responding to such requests. Finally, both sides agree that the first meeting of this dialogue will be held by the end of 2015, and will occur twice per year thereafter."*[81]

- The White House: Office of the Press Secretary; September 25, 2015

There are two major takeaways from this agreement. The first is by using aggression; the United States was able to engage in talks with China. By threatening to prosecute 5 Chinese nationals, the United States finally got the Chinese to come to the table. This display of forced showed that the Chinese government was willing to talk if the United States was going to charge these 5 nationals. It showed a weakness in China's constant denial in its cyber intrusions in the United States by displaying a use of judicial force.

The second takeaway is dialogue is possible with the Chinese government. Looking at the deal itself, it is a great step forward in ensuring dialogue with China and protection of United States interest. Both sides agreed to engage in dialogue and implement changes that would reduce the amount of cyber attacks. This proves that mutual dialogue between the United States and China possible in dealing with the Cyber realm.

[81] Ibid

For the United States, this is a landmark deal that shows progress can be made with dialogue, as well as a show of force. After years of trying to get China to deal with cyber security, it finally happened. However, it remains to be seen if China still holds up to its bargain.

6. Recommendations

Even though the cyber agreement is step forward, the United States cyber security policy is still inefficient. By looking at the case studies and statistics of cyber attacks, we can see the United States is still vulnerable. In order for the United States to prevent attacks by China, such as Titan Rain and Operation Aurora, I recommend a partnership between the public and private sector that entails a multifaceted approach. These recommendations may cause a decrease in attacks, as well as a strong firewall against further intrusions. It must be noted that some of these steps are being taken by the United States, but others are still needed.

6.1 Private and Public Sector Dialogue

Titan Rain and Operation Aurora showcased attacks on the public and private sector. Each sector was compromised one way or another by hackers in China. In Titan Rain, we saw individual U.S. departments get hacked, without any giving each other warnings during the attack. In Operation Aurora, individual corporations were attacked and all came out in unison after Google announced the cyber espionage. One way to strengthen cyber security is data sharing between the two sectors. If the United States department of Homeland Security, as well as other departments, were in constant contact with private sector representatives it would mean the United States can hastily respond to a cyber intrusion.

A way to strengthen this partnership is for the United States government should invite leaders in the tech, financial and other important private interests to congressional hearings or even meeting high profile U.S government leaders. Inviting these leaders can lead to discussion of appropriate measures to be taken to ensure safety of public and private assets. It would be wise to invite the leaders, such as Jeff Bezos (Amazon), Sataya Nadella (Microsoft) Mark Zuckerberg (Facebook) and Sundar Pichai (Google) to discuss the most pressing issues in cyber security, whether it be in the private or public sector. Currently, we have seen positive steps in this direction. Senator John McCain, the current chairman of the senate armed service committee, has invited representatives of the private sector to discuss a cyber strategy in the United States.[82] Their insights proved to be constructive on improving U.S. cyber defense. From these hearings, we can see a stress in importance on this subject. In addition to Senator John McCain’s numerous hearings on cyber security, President Donald Trump has invited leaders in the tech world to discuss these issues as well.[83] The main discussion pertained to cyber security and how the U.S. government can work with the tech world to protect United States interests. These are all steps in the right direction. A dialogue

[82] United States Senator John McCain, "Floor Statements," OPENING STATEMENT BY SASC CHAIRMAN JOHN McCAIN AT HEARING ON CYBER STRATEGY & POLICY - Floor Statements - United States Senator John McCain,

[83] Conger, Kate. "Donald Trump meets with tech leaders." TechCrunch

between the government and U.S. firms can spark improvements.

6.2 United States Cybersecurity Special Committee and Cybersecurity Legislation

With the help of tech leaders by constructive dialogue, the United States congress should create a special committee that deals with this issue: a special subcommittee that can focus on cyber security with the help of the private sector. As of now, there United States congress does not focus on cyber, compared to armed services, foreign affairs, veteran affairs, and etc. Creating a subcommittee can focus on this issue, as well as gain funds for its research. If this were to happen then the United States can have a committee on cyber security that can invite private sector leaders to discuss a wide array of issues. We currently see this push by the United States congress. Jessisca Schulberg and Laura Barron-Lopez state, " The panel will draft legislation related to cybersecurity and call on the incoming Trump administration to develop a strategy to deter and respond to cyber attacks."[84] It is a step in the right direction

With the subcommittees in depth knowledge, the United States government should pass laws that protect and update U.S. cyber security in the public and

[84] Jessica Schulberg and Laura Barrón-López, "John McCain To Create New Senate Cybersecurity Subcommittee," The Huffington Post

private sector. Currently, there are insufficient amount of laws by the United States that deal with cyber security. Most of the attention has been towards conventional warfare. However, cyber security should be at the forefront of United States National Security. The laws should include: funding towards cyber security in Homeland Security and U.S. military; private and public partnerships in cyber defense; laws that protect intellectual property in the private sector, and

6.3 Block chain and a Crisis Management Plan

The public and private sector it should also reanalyze the current system of open source by considering block chain. Open Source is a software design that the public can modify and share because it is publicly accessible.[85] Anyone can access it as well as change its contents. This makes it very vulnerable to outside forces. However, block chain is a secure system that as minimal risk of being compromised. Block chain is a system that can be digitally redistributed but not modified as all.[86] In addition to this, experts in cyberspace consider Block chain very secure. An example of a company using block chain is Bitcoin. Bitcoin is a digital payment system that has gained steam over the past few years. Many experts tout its success due to its secure system of block chain. It is near impossible

[85] "What is open source?," Opensource.com
[86] "What is Blockchain Technology? A Step-by-Step Guide For Beginners," Blockgeeks,

to hack a system like this because of its safe and secure programming. The United States should consider integrating this system into servers in the private and public sector. It would ensure safety and create a buffer against cyber intrusions.

In addition to using block chain as a more secure system, there should be a crisis management plan by the public and private sector to respond to cyber attacks. Both Titan Rain and Operation Aurora showed us that both sectors were novice in reacting to a cyber intrusion. Therefore, there should be a plan formulated so both can react when an attack occurs. Leaders from corporations and the U.S. government can convene to formulate a plan to respond to these attacks. Whether it is a defense mechanism that lockdowns information or alerts all parties involved, a crisis management plan in these circumstances are necessary.

6.4 Honor the U.S.- China Cyber agreement and engage in dialogue

The United States should also abide by the U.S.-China Cyber agreement. The agreement outlines guidelines that both parties must follow. By abiding by the agreement, it can show the world that the United States is a responsible power in cyber security. Furthermore, this agreement makes China acknowledge there is a problem with cyber espionage, which they have outright denied. According to Garry Brown and Christopher D. Yung, “China seemed to adopt the U.S. position that there is a type of spying distinct from national security espionage. If both

China and the U.S. agree that states spying to benefit corporate profit is distinct from — and less acceptable than — states spying for national security, it could have a profound effect on international norms in this area".[87] Finally getting China to adopt a United States perspective has been a long-standing goal. By having China agree to this agreement, it helps United States interests, for private and public interests.

By honoring this agreement, the United States can also talk to Chinese stakeholders and firms. There should be common ground met on the issues of cyber attacks. In today's global commerce, most worldwide firms work together. An attack on a U.S firm may harm the Chinese firm one way or another. Products, such as Apple's Iphone, reply on components from China. A hack on Apple Corporation may hurt Chinese firms in the future. Furthermore, the very notion of a private firm being attack by a foreign entity should give Chinese stakeholders a reason to worry. The leaders of the private sector should discuses these issues with Chinese firms in order for them to pressure their own government.

[87] Gary Brown and Christopher D. Yung. "Evaluating the US-China Cybersecurity Agreement, Part 1: The US Approach to Cyberspace." The Diplomat. January 19, 2017. Accessed May 11, 2017. http://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/.

6.5 Punishment and International Law

Coupling with dialogue and honoring the Cyber agreement, the United States should punish Chinese citizens who engage in espionage. In the case of the U.S. cyber agreement, it was initiated by charging 5 Chinese nationals on espionage of U.S. firms. By threatening to use judicial force, it can deter China from engaging in cyber espionage. A way for the government to catch these actors can be private firms. Private firms can alert the United States government of suspicious activity in its servers. Since private enterprises are more sophisticated in a technological aspect, it would be imperative for them to report to the government. The government should punish Chinese citizens who engaged in these acts and private firms can help the government in tracing these actors.

The United States should also push for international law against cyber attacks. As of now, there are no concrete laws that dictate cyber warfare. This is unlike other types of espionage, which are outlawed by international law. *Jus ad bellam* is the body of law that governs the resort by states to force in their international relations, and most of this is in the United Nations Charter.[88] The United States government can ask the private sector for its input on economic issues if this push for international law was undertaken. It can be a collaborated

[88] Melzer, Nils. "Cyberwarfare and International Law." UNIDIR Resources. 2011

push by the private and public sector. If the United States were to push for international law in cyber warfare, it would keep China more accountable for its actions.

A partnership between the private and public sector that engages in a multifaceted approach is ideal for the United States. By using these tenets, the United States can improve its cyber security structure and protect its interests. Unlike previous studies, which have a one step approach, this strategy tackles all issues that can help the United States. It is a solid approach in the vital interests of the United States in all aspects.

7. Conclusion and Limitations

7.1. Limitations

There are a few limitations in this thesis that may hinge the recommendations. One limitation is the U.S.-centric view it takes. Most of this data and information is from the United States, while perspectives from China are not given. This may give a sign of bias because a Chinese perspective is not represented. However, we must take in account that China rarely admits its actions in cyber attacks. In Titan Rain and Operation Aurora, we see the Chinese government outright deny any involvement, even when the United States government and U.S. firms blame China. The undeniable trace of information that leads back to China, even though it might take a while to find this evidence, shows China's involvement. If the Chinese government presents evidence then we might have another discussion.

Another limitation in this thesis is the lack of data. Most of the information pertaining to cyber attacks is secret and it is only through leaks that the public knows these attacks. Most of the information given about attacks is from leaked sources or non-government officials. This makes sense because usually a government wants to keep its breaches or attacks secret. If the United States were to announce an attack relatively right after it happened, it would cause a sense of panic. Furthermore, it may give off the impression the government and private sectors are incompetent in preventing cyber attacks. The private and public sector want stability and causing panic may cause a lack of confidence from the public. Therefore, the lack of data is a limitation in this thesis.

7.2 Conclusion

A rising China presents a challenge to the United States global hegemony. With the decrease in U.S military spending and weakening economy, coupled with a robust Chinese economy and growing military, all points toward a power transition. At the same time, cyberspace is being used as an outlet by both powers to engage in espionage that leads to precious intelligence and innovative technology being stolen. Previous studies for the United States cyber security go in the right direction, but there are a few limitations to them because of their constant one-step approach. Therefore, a different approach is needed in order to combat this pervasive problem.

By looking at the statistics of Chinese cyber attacks, Titan Rain and Operation Aurora, we see a preponderance of cyber of attacks from China. In Titan Rain, we see an attack on the public sector, while Operation Aurora we see an attack on the private sector. In addition, the U.S.-Cyber agreement shows that there has been progress by using aggression and dialogue, but much more is needed. Therefore, the multifaceted approach by the public and private sector is ideal for the United States. This entails dialogue between the public and private sector that involves tech leaders meeting government officials who can act as advisors, create a special commission on cyber security that passes legislation to update and protect cyber security, reanalyze open source by considering block chain and create a comprehensive crisis management plan, honor the U.S.-China cyber agreement and discuss the potential dangers of cyber warfare with Chinese stakeholders, and punish Chinese citizens who engage in espionage and while pushing for international law on cyber warfare.

This approach may reduce the amount of attacks and prevent China from gaining a foothold on the hegemony of the United States. It is imperative for the United States to re-strategize in order to prevent an emulation of Titan Rain and Operation Aurora. If changes are not made, then China will have an upper hand in the power transition between these two rival nations.

References

"Akamai's State of the Internet: 2013 Q4 ." Akamai. Accessed May 8, 2017. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-q4-2013-state-of-the-internet-connectivity-report.pdf.

"Akamai's State of the Internet: 2014 Q2 ." Akamai. Accessed May 8, 2017. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-q4-2013-state-of-the-internet-connectivity-report.pdf.

"Akamai's State of the Internet: 2014 Q4 ." Akamai. Accessed May 8, 2017. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-q4-2013-state-of-the-internet-connectivity-report.pdf.

"Akamai's State of the Internet: 2015 Q4 ." Akamai. Accessed May 8, 2017. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-q4-2013-state-of-the-internet-connectivity-report.pdf.

Amadeo, Kimberly. "Did Obama's Stimulus Plan Work?" The Balance. https://www.thebalance.com/what-was-obama-s-stimulus-package-3305625.

Badar, Jeffrey. "A Framework for U.S. Policy Towards China." Brookings, March 2016, 1-13. https://www.brookings.edu/wp-content/uploads/2016/07/us-china-policy-framework-bader-1.pdf.

Blackwell, Robert D., and Ashley J. Tellis. "Revising U.S. Grand Strategy Towards China." Council on Foreign Relations, no. 72 (March 2015): 3-39.

"China GDP Annual Growth Rate 1989-2017 | Data | Chart | Calendar." Trading Economics. Accessed May 03, 2017. http://www.tradingeconomics.com/china/gdp-growth-annual.
Data from National Bureau of Statistics of China

Chang, Amy, and Joseph Nye. "Warring State China's Cybersecurity Strategy." Center for a New American Security (2014): 1-38.

Conger, Kate. "Donald Trump meets with tech leaders." TechCrunch. December 14, 2016. Accessed May 10, 2017. https://techcrunch.com/2016/12/14/donald-trump-meets-with-tech-leaders/.

"Cyberspace," Merriam-Webster.

"FACT SHEET: President Xi Jinping's State Visit to the United States." The White House: President Obama. Accessed May 10, 2017. https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

Gary Brown and Christopher D. Yung. "Evaluating the US-China Cybersecurity Agreement, Part 1: The US Approach to Cyberspace." The Diplomat. January 19, 2017. Accessed May 11, 2017. http://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/.

"Global Internet Report 2016." Internet Society. Pg. 32, https://www.internetsociety.org/globalinternetreport/2016/wp-content/uploads/2016/11/ISOC_GIR_2016-v1.pdf.
Data from ITU 2016

"Global Internet Report 2016." Internet Society. Pg. 37, https://www.internetsociety.org/globalinternetreport/2016/wp-content/uploads/2016/11/ISOC_GIR_2016-v1.pdf.
Data from Breach Level Index, Gemalto, 2016

Harold, Scott Warren, Martin C. Libicki, and Astrid Stuth Cevallos. "Getting to Yes with China in Cyberspace." RAND. 2016.

http://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1335/RAND_RR1335.pdf.

Jackson, William. "How Google attacks changed the security game." GCN. Accessed June 30, 2017. https://gcn.com/articles/2010/09/06/interview-george-kurtz-mcafee-google-attacks.aspx.

Ji, Baocheng. "China's economic recovery and the China model." Renmin University of China 8, no. 3, 215-26.

Kentish, Ben. "China announces plans to increase military spending by 7 per cent." The Independent. March 04, 2017. Accessed May 04, 2017. http://www.independent.co.uk/news/world/asia/china-military-spending-7-per-cent-beijing-south-china-sea-donald-trump-a7610981.html.

Khimm, Suzy. "The sequester, explained." The Washington Post. September 14, 2012. https://www.washingtonpost.com/news/wonk/wp/2012/09/14/the-sequester-explained/?utm_term=.5499f5717271.

Lewis, James Andrew. "Computer Espionage, Titan Rain and China." Center for Strategic and International Studies. December 14, 2005. Accessed May 09, 2017. https://www.csis.org/analysis/computer-espionage-titan-rain-and-china.

Lee, Chungmin. "Escalation and De-escalation." Crisis Management. Yonsei Gsis, Seoul. Lecture.
Lieberthal, Kenneth, and Peter W. Singer. "Cybersecurity and U.S.-China Relations." Brookings, February 2012, 1-33.

Lui, Kevin. "Meet the Chinese Billionaire Who's Moving Manufacturing to the U.S. to Cut Costs." This Chinese Billionaire Is Moving Production to the U.S. to Cut Costs | Fortune.com. December 22, 2016. Accessed May 08, 2017. http://fortune.com/2016/12/22/us-china-manufacturing-costs-investment/.

Markoff, John, and David Barboza. "2 China Schools Said to Be Tied to Online Attacks." The New York Times. February 18, 2010. Accessed June 30, 2017. http://www.nytimes.com/2010/02/19/technology/19china.html.

McLeary, Paul. "Pentagon: Chinese Military Modernization Enters." Foreign Policy. May 13, 2016. http://foreignpolicy.com/2016/05/13/pentagon-chinese-military-modernization-enters-new-phase/.

McCain, United States Senator John. "Floor Statements." OPENING STATEMENT BY SASC CHAIRMAN JOHN McCAIN AT HEARING ON CYBER STRATEGY & POLICY - Floor Statements - United States Senator John McCain. Accessed May 10, 2017. https://www.mccain.senate.gov/public/index.cfm/2017/3/opening-statement-by-sasc-chairman-john-mccain-at-hearing-on-cyber-strategy-policy.

Melzer, Nils. "Cyberwarfare and International Law." UNIDIR Resources. 2011. http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.

Mills, Elinor. "New IE hole exploited in attacks on U.S. firms." CNET. January 14, 2010. Accessed June 30, 2017. https://www.cnet.com/news/new-ie-hole-exploited-in-attacks-on-u-s-firms/.

O'Harrow, Robert, and David Linch. "Timeline: Key events in cyber history." The Washington Post. Accessed May 02, 2017. http://www.washingtonpost.com/wp-srv/special/investigative/zeroday/cyber-history-timeline/.

"What is open source?" Opensource.com. Accessed May 11, 2017. https://opensource.com/resources/what-open-source.

"Operation Aurora." Operation Aurora Malware Removal | Sophos Security Topics. Accessed May 10, 2017. https://www.sophos.com/en-us/security-news-trends/security-trends/operation-aurora.aspx.

Organski, A. F. K. World Politics. New York: Alfred A. Knopf, 1968. Print

Panda, Ankit. "International Court Issues Unanimous Award in Philippines v. China Case on South China Sea." The Diplomat

Rollins, John W., Susan V. Lawrence, Dianne E. Rennack, and Catherine A. Theohary. "U.S.–China Cyber Agreement." Congressional Research Service Reports. October 16, 2015. https://fas.org/sgp/crs/row/IN10376.pdf.

Schell, Orville, and Susan L. Shirk. "U.S. Policy Toward China: Recommendations For a New Administration." Asia Society , February 2017, 8-67.

Schulberg, Jessica, and Laura Barrón-López. "John McCain To Create New Senate Cybersecurity Subcommittee." The Huffington Post. January 05, 2017. Accessed May 11, 2017. http://www.huffingtonpost.com/entry/john-mccain-cybersecurity-subcommittee_us_586ec07ae4b099cdb0fc5c1d.

Siboni, Gabi, and Y. R. "What lies behind Chinese Cyber Warfare." Military and Strategic Affairs 4, no. 2 (September 2012): 49-64.

Tabansky, Lior. "Basic Concepts in Cyber Warfare." Military and Strategic Affairs 1st ser. Volume.3 (2011): 75-92. Web. <http://www.inss.org.il/uploadimages/Import/(FILE)1308129610.pdf>.

Tammen, Ronald L., and Jacek Kugler. "Power Transition and U.S.-China Conflicts." Oxford Journals: Chinese Journal of International Politics 1 (2006): 35-55. Web. <http://cjip.oxfordjournals.org/content/1/1/35.short>.

Thornburgh, Nathan. "Inside the Chinese Hack Attack." Time. August 25, 2005. Accessed May 09, 2017. http://content.time.com/time/nation/article/0,8599,1098371,00.html.

"United States GDP Growth Rate 1947-2017 | Data | Chart | Calendar." Trading Economics. Accessed May 03, 2017. http://www.tradingeconomics.com/united-states/gdp-growth.
from U.S. Bureau of Economic Analysis

"U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage." The United States Department of Justice. May 19, 2014. Accessed May 05, 2017. https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

"What is Blockchain Technology? A Step-by-Step Guide For Beginners." Blockgeeks. March 30, 2017. Accessed May 11, 2017. https://blockgeeks.com/guides/what-is-blockchain-technology/.

What is a Zero-Day Vulnerability?" Symatec. http://www.pctools.com/security-news/zero-day-vulnerability/.

Walker, Dinah. "Trends in U.S. Military Spending." Council on Foreign Relations. http://www.cfr.org/defense-budget/trends-us-military-spending/p28855.

Windrem, Robert. "Exclusive: Secret NSA Map Shows China Cyber Attacks on U.S. Targets." NBCNews.com. July 30, 2015. Accessed May 09, 2017. http://www.nbcnews.com/news/us-news/exclusive-secret-nsa-map-shows-china-cyber-attacks-us-targets-n401211.

Zetter, Kim. "Google Hack Attack Was Ultra Sophisticated, New Details Show." Wired. January 14, 2010. Accessed May 11, 2017. https://www.wired.com/2010/01/operation-aurora/.

Korean Abstract

하이테크 전쟁: 중국의 부상에 대응하는 미국의 사이버 안보에 관한 연구

미국과 중국은 현재 사이버분야에서 권력 전이 상황에 놓여 있다. 본 연구는 미국이 중국에 맞서 자국의 이익을 지키기 위해서는 공공부문과 민간부문 모두에서 다면적 접근법을 이용한 협력적 관계를 형성해야 한다고 제안하고 있다. 다면적 접근의 구체적 방법들은 다음과 같다: 1. 사이버 안보 분야 관련 전반적인 이슈들에 대해서 토론할 수 있도록 미 정부와 민간부문의 지도자들이 좌담을 가지는 것; 2. 공공부문과 민간부문을 보호하고 이들 부문에 관련된 정보가 지속적으로 업데이트 되도록 해당 제정법을 통과시키는 사이버안보 관련 특별위원회를 설립; 3. 오픈소스를 재분석, 블록체인을 검토 및 포괄적인 위기 관리 계획을 창안; 4. 미·중 간 맺은 사이버 협정을 준수하고 중국 관계 당국자들과 사이버안보의 중요성에 대해서 논의; 5. 사이버 스파이 행위에 가담한 중국인들을 처벌하고 국제법에서 사이버안보 분야와 관련된 법 제정을 하도록 요구. 이러한 다면적 접근법은 경쟁국인 중국에 대해 미국의 사이버안보 방어력을 높이고 미 정부의 중요한 이익을 보호하는 전략이다.