

## Seton Hall University eRepository @ Seton Hall

---

Seton Hall University Dissertations and Theses  
(ETDs)

Seton Hall University Dissertations and Theses

---

Spring 5-17-2016

# The History of Chinese Cybersecurity: Current Effects on Chinese Society Economy, and Foreign Relations

Vaughn C. Rogers  
[vaughn.rogers@student.shu.edu](mailto:vaughn.rogers@student.shu.edu)

Follow this and additional works at: <https://scholarship.shu.edu/dissertations>

 Part of the [Asian Studies Commons](#), [Chinese Studies Commons](#), [Information Security Commons](#), and the [International Relations Commons](#)

---

### Recommended Citation

Rogers, Vaughn C., "The History of Chinese Cybersecurity: Current Effects on Chinese Society Economy, and Foreign Relations" (2016). *Seton Hall University Dissertations and Theses (ETDs)*. 2207.  
<https://scholarship.shu.edu/dissertations/2207>

THE HISTORY OF CHINESE CYBERSECURITY: CURRENT EFFECTS ON CHINESE  
SOCIETY, ECONOMY, AND FOREIGN RELATIONS

BY  
VAUGHN C. ROGERS  
B.A., SIMMONS COLLEGE, BOSTON, MA, 2005

A MASTERS THESIS  
SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE  
OF MASTER OF ARTS IN ASIAN STUDIES AND FOR THE DEGREE OF MASTER OF  
ARTS IN DIPLOMACY AND INTERNATIONAL RELATIONS  
AT SETON HALL UNIVERSITY

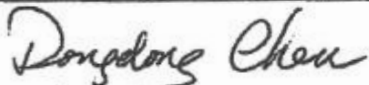
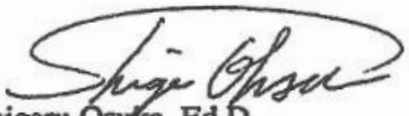
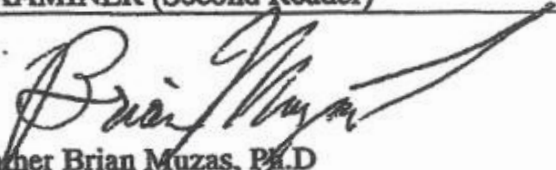
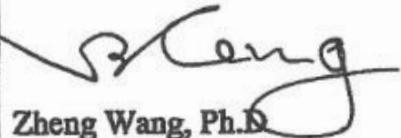
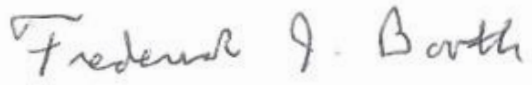
SOUTH ORANGE, NEW JERSEY

MAY 2016

© 2016 Vaughn C. Rogers

THE HISTORY OF CHINESE CYBERSECURITY: CURRENT EFFECTS ON CHINESE SOCIETY, ECONOMY, AND FOREIGN RELATIONS

BY  
Vaughn C. Rogers

APPROVED:	MONTH, DAY, YEAR
 Dongdong Chen, Ph.D. MENTOR (First Reader)	<u>May 12, 2016</u>
 Shigeru Osuka, Ed.D. EXAMINER (Second Reader)	<u>May 11, 2016</u>
 Father Brian Muzas, Ph.D. EXAMINER (Third Reader)	<u>May 12, 2016</u>
 Zheng Wang, Ph.D. EXAMINER (Fourth Reader)	<u>May 16, 2016</u>
 Frederick J. Booth, Ph.D. HEAD OF DEPARTMENT	<u>May 17, 2016</u>

A THESIS SUBMITTED IN PARTIAL FULLFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF ARTS IN ASIAN STUDIES AND FOR THE DEGREE OF MASTER OF ARTS IN DIPLOMACY AT SETON HALL UNIVERSITY, SOUTH ORANGE, NEW JERSEY.

## Table of Contents

<b>Acknowledgements</b> .....	<b>i</b>
<b>Abstract</b> .....	<b>iv</b>
<b>Chapter 1: Introduction</b> .....	<b>1</b>
<b>Chapter 2: The Chinese Cybersecurity Policy</b> .....	<b>13</b>
2.1 <i>The Internet in China (中国互联网状况)</i> .....	13
2.2 <i>White Papers (中国政府白皮书)</i> .....	15
2.2.1 National Defense (2010 年中国的国防).....	15
2.2.2 Military Strategy (中国的军事战略) .....	18
2.2.3 Peaceful Development (中国的和平发展).....	19
2.3 <i>The Constitution of the People's Republic of China (中华人民共和国宪法)</i> .....	20
2.4 <i>Analysis</i> .....	21
<b>Chapter 3: The Opening of China and Its Affects Contemporary Chinese Cybersecurity Policy</b> ....	<b>24</b>
<b>Chapter 4: Chinese Cybersecurity Comparison</b> .....	<b>38</b>
4.1 <i>India</i> .....	39
4.2 <i>United States</i> .....	41
4.3 <i>Cuba</i> .....	44
4.4 <i>North Korea</i> .....	45
4.5 <i>Russia</i> .....	47
4.6 <i>Analysis</i> .....	49
<b>Chapter 5: Chinese Internet Censorship</b> .....	<b>51</b>

<i>5.1 Propaganda as Censorship</i> .....	52
<i>5.2 Education as Censorship</i> .....	57
<i>5.3 Censorship as Safety</i> .....	62
<i>5.4 The Effects of Censorship on Economy</i> .....	63
<b>Chapter 6: Freedom versus Security, or Privacy?</b> .....	<b>65</b>
<b>Chapter 7: Conclusion</b> .....	<b>70</b>
<b>Bibliography</b> .....	<b>78</b>

## **Acknowledgements**

When I first began my Seton Hall career, my first impression, or rather first career goal, was that I wanted to be the United States Ambassador to China. Of course, as I would realize later, that would take a lot more time, work, and effort than I originally thought, but I felt better knowing the paths I needed to take thanks to my professors. Professor Dongdong Chen was the one who accepted my application to Seton Hall, and I remember nearly screaming with joy at my desk in China, where I taught English for two years, when the email arrived. I wrote emails to my mother, then other family and friends, and then immediately received an email from my mother saying that I needed to answer her phone call on Skype. It was late at night for her, but she was so happy and relieved that the Asian Studies department had accepted me that she paid no heed to lack of sleep. Professor Chen really guided me that first semester into the classes and courses necessary, especially since Professor Edwin Leung was going on sabbatical and I had to take his classes as requirements. I had no idea what I was getting myself into when I decided to take his class, let alone graduate school in general, but it was his informational and tough class that helped keep me a step ahead of other students. His class was the first and more rigorous of the courses that I had that first semester, but it rivaled other classes for sheer amount of content and “breaking in” students.

Father Brian Muzas’ class was also a challenge because the material was completely different from that which I experienced as an English major. The journals and class discussions were helpful yet challenging both in terms of the subject International Relations Theory, and for graduate school, and I am so grateful for it. Later, his course in International Security identified and solidified my academic focus in cybersecurity. After these two rigorous courses, other courses were more manageable, and I knew better about what was expected of me. I also

appreciated the vast catalogue of topics and authors Father Brian kept to memory that frequently interrupted class with excursions that kept our interest and gave us new elements to the material. After this point I noticed great differences in style between professors, and that I also had to adapt to what professors understood or expected out of students, and even then it depended upon the course.

Professor Zheng Wang's class on negotiation was unique in the sense that it was highly interactive and I got to argue with people, and it was enjoyable, not emotional, which is what I experienced with most Americans (one of many culture shocks I experienced when I returned from China). It was this class that made me learn more about compassion and about filtering language down to facts, which are the most important things a diplomat can learn. It was also because of the lessons learned in this class that I negotiated an incredible price for my new car, and did so professionally.

Professor Li Xiaoqin, or Li Laoshi, was always there for me when it came to Mandarin, and would let me meet with her whenever I had time to practice. She reminded me of the warmth I had experienced in China, and appreciated my level of Chinese as she did my classmates. She always knew how to push my Chinese to the next level and made sure I spoke exclusively with her in Chinese when I casually saw her in the library. It was in her class that I met my dear friend Kuang Bao and when I first made tea for the whole class.

One of the professors I appreciated the most from a teacher's perspective is Professor Shigeru Osuka's class, mostly because it was so well organized and so clear, as well as empowering and manageable for me as a student. Not only did I get to see a very lucidly formatted lesson, but I also was inspired to learn more about Japan and its culture outside of the classroom, and even consider learning Japanese as a third language. This was a significant



change from my original opinion that I was interested solely in China and thus would focus on that country and culture, and I reconsidered and realized that the more I learn about other cultures, the better for my overall understanding of my focus. Thanks to Dr. Osuka, I presented for the first time a paper in front of an audience about Japanese Gunpowder.

Come the second year of my academic career, I was able to have a class with my counselor, Professor Chen, in Chinese linguistics. She had already helped me apply to one conference about Chinese education, and I was excited to see what else I could learn about Chinese linguistics that could add to my experience. Professor Chen was also a tough but fair, expecting much from all of her students, and that drive inspired me to think more deeply about Chinese as a language and as it is part of a culture. I went to the MAARS conference in October the following year proud and confident to demonstrate what I learned and the ideas I added to it.

I sincerely thank these professors for their guidance and introduction to my graduate school experience.

I would like to thank my friends and colleagues for their understanding, their compassion, and for making arduous situations bearable and even enjoyable. Most notably, Malissa “Missy” Eaddy, Gabriel “Kuang Bao” Thompson, Yi han, Jessie Tao, Bill Golba, Anna Guryanova, Qingqing Lan, Sha Mei, Yue Shen, Michael Stone, Shangke, Sarah Ireland, Sara Valero, and Nina Robinson.

Finally I would also like to thank my parents who always supported my decisions, particularly my father, James A. Rogers, for going to China and sparking my interest. I would especially like to thank my mother, Cynthia V. Fitzgerald for her tireless support, for her time, for her patience, and for her edits when needed. Without her support I would not have reached this point in my academic career and I am forever grateful.

## ABSTRACT

Chinese cybersecurity has become an infamous topic in the field of cybersecurity today, causing a great deal of controversy. The controversy stems from whether or not censorship is hindering Chinese economy, society, and relationships with other countries. The *White Papers* (中国政府白皮书), the *Constitution of the People's Republic of China* (中华人民共和国宪法), and *The Internet in China* (中国互联网状况) all suggest that there is a free flow of Internet both within and without China that promotes peaceful socioeconomic development which the Chinese government seeks to promote. But is China sacrificing lucrative business prospects to secure their country? From whom is China securing its people, and is filtering the Internet truly the cure to insecurity? International Security Studies (ISS) has examined the issue of what is actually being secured, the nation state or its people. More recent schools of thought have asserted that Human Security, which is also concerned with the welfare of the people of the state, is relevant to China's current security questions. China is reacting to its recent economic slowdown by reasserting its dominance over news outlets and increasing censorship of the Internet, which is in direct contradiction to its *National Defense and Military Strategy* policy. The policy dictates informationization and modernization through the use of the Internet and technology, but to control the free-flow of Internet is to limit economic and social development. This paper explores the above documents, other comparable countries' cybersecurity policies, censorship policies throughout China's recent history, news reports, International Relations Theory (IRT), and ISS to see if this is so.

Keywords: China, cybersecurity, censorship, economy, society, foreign policy, national security policy, International Security Studies, International Relations Theory, Human Security, security, history, contemporary

## Chapter 1: Introduction

History books are often timelines told in story form to make events memorable, but here, the “History of Cybersecurity” takes on an entirely different meaning. “History” in this context is more like a person’s past, her medical history, or her life story, not merely a sequence of events that sums up the person’s current state. China is always moving, always changing, especially in this last century. Unfortunately—even unfairly—China is like a person who was traumatized by invaders, wars, and revolutions, who is only emerging from that trauma now, raw and sensitive, unsure of what to do after such tumult, and in a world so completely different from what it has known. Not only did China emerge completely oblivious to new technologies that had been pioneered in its absence from the world stage, but it emerged unsure of how to handle, use, and adopt such technology order to survive the world it newly met. Thanks to Deng Xiaoping (1904 – 1997), that transition went relatively smoothly, and China began to adopt technology in a short period of time to the point where few citizens are without a cell phone and out of range—reception notwithstanding (Carsten 2015).

Technology has brought countries and their people closer together than ever before (Schuman 2011). Where once physical boundaries such as mountains and oceans played a major role in a nation’s security they are now rendered futile (Lenzo 2015). In *The Rise and Fall of Intelligence* Michael Warner writes of anecdote in perfectly exemplifies how technology can redefine warfare and security when hot-air balloons were used for the first time to spy during America’s Civil War (Warner 2014, 20-1). Today, technology has shifted from the mechanical and the tactile to the digital and the cyber, and the concept of intelligence has changed along with it, including terminology. The terms referring to intelligence-gathering began in the 1980s with “Intelligence, Surveillance, and Reconnaissance,” then called it “Command, Control,

Communications, and Intelligence,” and finally called it “Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance” (C4ISR) (Warner 2014, 240). This new technological era brings with it more attacks via the Internet—the ultimate and unavoidable source of information and communication—changing the term to include “cybersecurity.” The digital age has now constituted a leap in socioeconomic development, and now holds the keys to a country’s overall stability, success or failure, or even strength against aggressors. A nation’s personal or official computers are vulnerable either by personal threats such as malware from a hacker, or an official, a governmental cyber-attack which may shut down vital systems.

Cybersecurity is one of the main threats plaguing governments today, and can disrupt operations in many different ways (The White House 1-5; Wilshusen 2015; Watson 2002; Rogers 2015).

Cybersecurity as defined by the National Initiative for Cybersecurity Careers and Studies (NICCS) is “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” (NICCS 2014).

Infiltration can be defined as a cyber-attack, which is a denial of service (DoS) or the prevention of a system such as a computer, or a hack, when malware is introduced into the system and sends information back to the source of the malware. A growing problem in the cybersecurity world is that not only government systems but private entities must be protected from cyber-attacks.

Private companies can be connected to, or part of governmental organizations and can carry information or research and development (R&D) that can be of significant use to other government or other hackers. Improperly guarded and sensitive information makes any government’s system vulnerable to attack because the security of the Internet is only as strong as its weakest link: if one person has connected his computer to the Internet without anti-virus

software, then he has left his computer and whatever other computers or sites to which he is connected vulnerable to the same virus (Cornau 2013). While there is a risk each time a person connects, the Internet is too valuable a tool to regulate.

Governments may regulate the flow of Internet in their particular territories or states, but private companies and individuals are more likely to be the technological innovators that help the economy grow, particularly because they have unfettered access to the Internet. Technological innovation is inextricably linked to economic growth; thus R&D is becoming important and prominent to any economy, especially one in a developing country (Asian Development Bank 2014, 1-2). For this reason, businesses and governments have made investments into technological R&D, sometimes through illicit means (Fitzgerald 2011). Cyber-espionage conducted by government spies or otherwise has been reported since the invention of an intranet in the 1970s (Warner, 261), and used for surveillance, reconnaissance, and especially theft of intellectual property (Rogers 2015). News media has reported many cybersecurity breaches, and has named China as the source.

The Chinese government, most notably People's Liberation Army (PLA), has been implicated as the reason for numerous cyber-attacks on countries throughout the world (The Center for Strategic and International Studies [CSIS] 2014). Until recently, the attacks blamed on the PLA have been on government and governmental organizations, but now reports have indicated the PLA has shifted its focus to the private sector. Many of the countries affected by these attacks are either Western or developed, and those targeted have strong programs in technological research and development. On the other hand, China has also suffered a series of cyber-attacks which have originated from either the United States or Taiwan (CSIS 2014). Because of the Internet's growing importance, China has modified its *White Papers on National*

*Defense (2010 年中国的国防)* in May 2015 to include cybersecurity threats and to lay out the plans on how to cope with the attacks.

Part of the reason for this late legislation is the fact that China had received Internet technology in 1994, twenty years after most developed countries already had such technology (Martin 1999, xxxv-5). Being twenty years technologically behind the rest of the developed world—most of which are powerfully influential countries—China has to “play catch up” not only in technological R&D but also defining its cybersecurity policy. Cyber-warfare is the latest strategy—more valuable and arguably more devastating than physical battles or weaponry—in a nation’s arsenal that could keep an enemy nation’s wealth intact but still cripple its military forces. Cyber-warfare is also the weapon of developed countries which have the monetary means and with it the status to afford and develop such technology. China is one of those countries (Gierow 2014; Gouranga 2015; Hartnett 2011).

China has raced ahead economically in recent years, forming its national security and foreign policy on social and peaceful development; however, this progress is simply in economic, not technological, growth. To be sure, China is the world’s highest producer of technological devices (Marsh 2008), but it has lagged as a developer and inventor. Its general economic success lies in “overseas” manufacturing in that companies from abroad, namely the United States, have consulted with factories in China and financed cheaper labor to make the technology. Between 2001 and 2013, an estimated 3.2 million jobs went overseas to China, 2.4 million of which were solely in manufacturing (Peralta 2014). This street, however, not one-way.

As part of China’s 2009 *White Papers on National Defense*, the Chinese government suggests that in order to be part of a “harmonious world of enduring peace and common prosperity,” China should invite foreign countries to “cooperate,” or collaborate with one another

in “defense-related science, technology and industry. It emphasizes exchanges and cooperation with developed countries” (Information Office of the State Council of the People’s Republic of China [IOSCPRC] 2009, 63) so that China can learn how to develop technology from them. Above all else, China wants to develop technological R&D from within so that it does not have to rely on foreign powers to initiate the invention and building of new technology. The term “science” and its practice have been used commonly throughout the *White Papers*, mostly to emphasize China’s push to be more developed in all general areas, especially technology. The translation of this term in English is accurate, but the term “scientific development” is vague and needs a definition or examples. Chinese governmental policies have a general idea that connects them all: China wants to develop socially, economically, and technologically. In addition the policies stress that China wants to peacefully develop in harmony with the rest of the world.

Despite these policies and their intent, China has had a tumultuous relationship with technology and the Internet. Technologically and technically speaking, China does produce most of the world’s technology, particularly computer hardware, but the developers and the companies hiring the factories are typically Western companies which care about low cost and ignore workers rights (Kimball 2014). With the advent of the computer and intranet the West pioneered this technology and its R&D since the invention of the Internet in the 1970s, and cornered the market for nearly that long as well (Martin 1999). There is an interesting connection between technology and democratic countries in that most of the technology—digital or otherwise—is built for a democratic market that allows information to be disseminated freely to whomever has access. In a way it is difficult for China to embrace access to technology because the Internet and technology was created by, and is governed by, the West. In response, China makes its own brand of technology, for instance the social media sites built for Chinese users in place of

Western brands. More infamous is China's leaning towards Internet censorship which, as a result of its national security policy, is a defining source of Chinese Internet frustration and humor alike (e.g. "The Great Firewall of China").

Internet censorship in China is considered by other countries to be reactionary because the government has blocked world-famous newspapers, social media sites, and many Western websites in general because the sites do not follow Chinese national security policy or have threatened it. In the case of YouTube among others, the mention of sensitive topics (Xu 2015) like "Tiananmen Square" or "Taiwanese Independence" is the reason for the outlet's subsequent censorship in the early 2000s. Chinese Censorship is in a way ironic in light of China's educational history which includes memorization- and information-focused teaching that has been in practice since Confucius first began his teachings. And only for the sake of social stability would China go against such an ingrained grain. The Internet is the largest source of information on this planet, and in order to develop science and technology it is important to know what other scientists and innovators are doing. One would question China's wisdom of blocking off or censoring one of the most important and prolific sources of information, especially because China declared a desire to "scientifically" build its own technological R&D when both Deng Xiaoping called for reform in the early 1980s and more recently in the *White Papers on Peaceful Development*( 中国的和平发展) (Ventre 2014; IOSCPRC 2011).

In recent years Chinese national security policy and foreign policy has been updated to include cyberspace, but, like civil law (The Economist Staff 2013), it includes it only as a generality, and it will be defined over time on a piecemeal basis in Chinese national and international security. Chinese national security is and has been a virulent topic because of one policy, a "One China Policy." As a member of the United Nations, China has asserted its right to



declare that Taiwan is part of its territory in order to preserve national stability, demanding that other countries must respect that stance when a country enters into agreements with China.

According to Chapter 1 Article 2.1, and Chapter 9 Article 55 of the *United Nations Charter*, China has a right to self-determination, and, for example, if it claims that Taiwan is part of its territory and others support this view, then China's sovereignty is to be preserved. Cyberspace has been treated much in the same way in its 2015 *White Paper on Military Strategy* (中国的军事战略). In this paper we see cyberspace referred to, and treated as, a territory in the physical, pre-technological sense.

Cyberspace is a new concept upon which few definitions have been agreed, and there are also few laws regarding the regulation of the Internet. The terms "cyberspace" and "Internet" are used interchangeably, but they are actually different concepts. Typically, the Internet is a connection between and among computers that must be accessed through an Internet provider, and a program that browses the Internet, such as Mozilla Firefox or Google Chrome.

Cyberspace encompasses the Internet, intranets, and anything that exists on a device such as a laptop or smart phone. However, not all governments base their cybersecurity policy on the same definition of the Internet and cyberspace. The North Atlantic Treaty Organization (NATO) Cooperative Cyber Defense Centre of Excellence (CCDCOE) catalogues definitions of cyberspace that vary depending on the country (NATO CCDCOE 2008). The list includes European, African, and Asian interpretations of cyberspace, which shows a disparity between and among perspectives on cybersecurity. Cyberspace itself has presented a new challenge to define boundaries and conduct when it comes to the law, raising such questions as "does it have a limit or boundary like a nation state?" China already claimed its cyberspace, writing about it in the English *White Paper* as if it were a physical thing to be protected along with national

domains (Song 2015). In this same section of Chapter Four in the *White Paper*, nuclear proliferation and maritime authority are all labeled as part of “critical security domains,” thus making cyberspace as important as territorial disputes.

Much of recent Chinese foreign policy centers around maritime disputes, including claims over several island chains, and many of those claims involve allies of the United States. China’s history is peppered with incidents where territory was lost, most notably, the return of Hong Kong from British rule. China is most sensitive about its territorial disputes because they are closely tied to national security and social stability within the country. The “One China Policy” extends to Tibet, Hong Kong, and other separatist groups, which are considered threats to the country’s safety as a whole.

The point of this rhetoric? Chinese cybersecurity is about a holistic view of security policy. China is the “newest oldest country,” and with that identity comes obstacles and perceptions that few other countries have encountered. Unlike other countries, China plays catch-up in the technology race. Computers were around since World War II (History.com Staff 2011) and China opened to the west around 1978, shortly after the death of Mao Zedong (1893 – 1976). Because of the policies Mao implemented (which were similar to those of the Qing Dynasty [1644 – 1912]), Mao effectively stunted Chinese growth in areas of economy. It took Deng Xiaoping’s tireless efforts over a decade to reform the government and ideology around a closed-off, communist policy and to strengthen China and get it into the international arena. As part of Deng Xiaoping’s policies on economic growth in the late 1970s, Deng visited countries such as Japan and the United States and asked for two things: invitations for foreign business, and the exchange programs for Chinese students.

Deng recognized China's need to grow and realized that there was no way it could grow from within with the help of foreign businesses and educational exchanges. Communism ruined Chinese education and innovation because of its policies: teachers were bourgeois, and to even think critically was frowned upon. Even Confucian temples and effigies were destroyed during the Communist Revolution. Once been part of longstanding traditions, they were treated under Communism as representations of the decrepit past. According to the Communists, the only way that China could have its own industrial revolution would be to copy it from others who had already pioneered the techniques, a practice it continues today. Before this time, foreign policy was non-existent. Other states were treated with suspicion, and the main concern was to make China glorious again. However, because China was so isolated, the country never realized it missed opportunities to grow economically and technology. And who could blame China? Since 1850, China's interaction with Western countries was fraught with misinterpretation, clashes, and the loss of territories that rightfully belonged to the country. The century of humiliation caused a backlash in foreign relations, and China has been wary of other states, especially the West, until these foreign policy changes in the late 1970s.

In comparison, China improved its foreign policy since the Mao era, however. It re-adopted Confucius as a guide to realize its goals in 2005, when former President Hu Jintao (1942 - ) presented the idea of a "harmonious society" like Confucius taught where all people would have their place in the world (Masuda 2006), and China grow socially and economically and promote its soft power around the world. These conditions would pave the way for the Chinese to do business with countries and to achieve the economic growth it put forth in its foreign policy outline. So far, China does whatever it can to ensure that it succeeds in achieving that growth, which has caused other countries to complain. These complaints range from companies who

find their products copied with false logos (Cronau 2013) to government bodies such as the Office of Personnel Management (Nakashima 2015).

According to data collected from the CSIS and the NATO Review, Chinese hacks solely targeted governmental organizations until 2008 when hacks refocused efforts on commercial businesses (CSIS 2010). Suddenly, China-originated attacks shifted from governmental bodies to private businesses. Technology had always been pushing the economy since the Industrial Revolution (Mokyr 2000), but this increase in hacking activity on businesses specializing in technology around the time when the world faced a financial crisis indicates China's motivation to fulfill its goal of "economic development," at least in part. Granted, hacking occurs around the world millions of times a day from many different Internet Provider (IP) addresses on many different entities, but the fact that one of the world's largest and most influential country is being recognized for, or accused of, hacking a particular type of entity is significant. Such recognition is so significant that China is becoming synonymous with hacking (Shih 2015). With this idea in mind, these perceptions unfair and uninformed (Rogers 2015).

What makes Chinese cybersecurity unique and difficult to define is the history of the country itself. This history has affected perceptions of territoriality, national security, censorship, and many other aspects of security. China has undergone more changes in the last fifty years than most countries in the last century (Bol 2016), and with that volatile environment came uncertainty for the fledgling Chinese government. As a result, this situation created unique problems for the Chinese government, particularly since all foundations that had been part of Chinese culture and governance, such as Confucianism, were rejected and destroyed. With this in mind, the first research question is: what are the Chinese cybersecurity policies and how are they implemented? In order to understand this question, this thesis will:

- retrace the history of cybersecurity policy
- examine official government documents stating the policy
- reveal the variables that the Chinese government must take into account in order to form their cybersecurity policy; and
- analyze the perception of Chinese cybersecurity by the Chinese government and other countries.

Much of the rhetoric about Chinese hacks today come from reports made by Western media, and rightfully so: has any nation announced when it has hacked another? On the one hand, even though reports from Western countries are able to identify China as the origin of the hack, China comes away from those reports vilified. Chinese spokesmen have come before news media and defended the Chinese government, saying that the news outlet “has become a ‘political tool’ used to vilify China’s government” (Couts 2011), but the remarks are dismissed or criticized. On the one hand, accusing China of cyber-attacks does nothing to stop them from happening, but on the other hand, reactionary comments or criticisms of the media outlets do nothing to win empathy. The second research question this thesis will explore is what are the effects of Chinese cybersecurity on Chinese economy, society, and foreign policy?

In order to understand Chinese cybersecurity policy and its affects this paper will work backwards in time. Much in the way teachers use “scaffolding techniques” to build a logical pattern of learning, this paper will analyze Chinese government perspectives on cyber security by looking at them in the *White Papers on National Defense, The Internet in China (中国互联网状况)*, among other documents, and then the history of how they came to be. To reveal the variables affecting how Chinese cybersecurity was developed in China, this paper will analyze China’s history with the opening of the country in 1978 to explore how industry, education, and

foreign trade policy methodology was developed, as well as to assess its efficacy. The literature review will include *White Papers*, *The Internet in China*, and *The Constitution of the Peoples Republic of China* (中华人民共和国宪法). For a cybersecurity comparison this paper will present the cybersecurity policies of other countries, both of democratic and communist governments in the West and the East. From there, this paper will explore Chinese censorship, in terms of what will be censored and why from, from both a Chinese and a Western perspective.

This paper will analyze the data and put forth reasons for why Chinese cybersecurity has been modeled the way in which it is, especially in the context of a potential “West versus East” conflict which has arisen in this sphere, as well as internal contradictions in the policies. Data from the CSIS will be analyzed and explain the cyber-attacks made on governments and private businesses that cause these contradictions in cybersecurity policy. Lastly, International Relations Theory of “Freedom versus Security” will be applied in order to measure the efficacy, power, and wisdom of Chinese cybersecurity policy with comparison to the other countries mentioned in Chapter 4. From this investigation, this paper will draw conclusions about Chinese cybersecurity policy from China’s experience in the last century and its attempt to grow and be counted among the developed nations of the world. This paper predicts that current Chinese cybersecurity policy is negatively affecting its economic and social development and its foreign relations.

## Chapter 2: Chinese Cybersecurity Policy

To “hear straight from the horse’s mouth,” this author contacted Chinese Consulate in New York City for information. A few weeks later, the Public Relations section of the Consulate was kind enough to respond, and sent one of the documents analyzed in this paper. The public documents *The Internet in China* are for the Chinese people to see the genesis and evolution of the Internet in China, and to show the ideology behind Chinese Internet security. It will be analyzed along with the Chinese *White Papers on National Defense, Military Strategy, and Peaceful Development*, and *The Constitution of the People’s Republic of China* as the primary sources for understanding how the Chinese government views the Internet and Internet use.

### 2.1 *The Internet in China (中国互联网状况)*

*The Internet in China*, a document provided by the Information Office of the State Council of the People’s Republic of China (IOSCPRC), is a brief outline of the obtaining, establishment, maintenance, and regulation of Internet in China. It discusses the ideological and philosophical uses for the Internet, making a case as to why the Internet is important to China. For instance, the Internet can be a tool for economic growth, which is immediately cited to be in line with Chinese national social and economic policy (IOSCPRC 2016). Claims in the Forward and at the start of each section, such as “The Internet has brought profound impacts on the world,” are without precedent or citation, are more opinion rather than fact, and are used as a lead-in to the main topics of the section. The fact that the opinion is stated is significant in and of itself. This perception of the Internet is imperative to understand how the Chinese government perceives, and writes laws, policies, and regulations for the Internet.

The first section of *The Internet in China* starts with a historical account of how China acquired the Internet from the Sino-US Joint Committee of Science and Technology. Section I continues to discuss how the primary purpose of the Internet in China is to develop economic industry, to spur overall economic growth, and to enable more communication between and among all regions of China, as well as government officials with the people themselves. The positive impact that the Internet in China has made in terms of access and users, as well as the negative impact of socio-economic and rural/urban divides are acknowledged. Section II promotes the use of the Internet and touts the importance of its use for Chinese daily lives, for government-to-citizen contact, and for the development of economy. Sections III and V are closely related as they deal with citizens' freedom of speech and Internet security. Laws on the regulation of the Internet define what is allowed and prohibited on the Internet, and as long as citizens adhere to the law, their freedom of speech is allegedly inviolable.

Section IV briefly summarizes basic principles and practices of Internet use. It immediately mentions citizen rights of Internet use and then lists incompletely how the Internet is regulated by law. In this section the various laws and departments that regulate the Internet are listed, but the list is also incomplete. It also includes how the Chinese government wants citizens to use the Internet, and that any "illegal dissemination of information online" is to be avoided, but the policy lacks a definition of "illegal information." The Internet here is treated as if its only use is for education, which is the "correct" way to use it. As the Chinese government has said before, it purportedly monitors the Internet—especially sites originating in the West—because the government wants to "guarantee online safety for minors" which are "China's biggest online group." The Chinese government states what it wants to protect, but does not state why.



## 2.2 *White Papers* (中国政府白皮书)

Chinese *White Papers* on any policy—whether it be national, foreign, or military—are available online in English and Chinese (IOSCPRC 2015; IOSCPRC [中华人民共和国中央人民政府] 2015) and tend to read like a summary rather than an official policy or law. They are goals and general plans that the government has for aspects of society, economy, and foreign policy. Somewhat based on what we know as “common law,” Chinese law deals with issues on a piecemeal basis. It takes time for Chinese law to develop and to be put into practice; when it comes to Internet security, Chinese law has lagged behind other security policies. Considering China’s more recent history, this tactic is wise: a “slow and steady” approach to new ideas and inventions is arguably more stable but can also prevent necessary changes in law or policy from coming to fruition in a timely manner. Internet regulation is handled by the PLA as part of the National Defense Policy.

### 2.2.1 National Defense (2010 年中国的国防)

China’s *White Papers on National Defense*, published in 2011, outlined national defense goals, catalogued then-current methods to fulfill such goals, and made improvements to the People's Liberation Army (PLA), nuclear proliferation and disarmament. In this *White Paper*, the idea of cybersecurity is barely mentioned, and when it is mentioned, it refers to defense measures other countries have taken (IOSCPRC, 2011). This *White Paper* focuses on three points: the development and improvement of the Chinese military, overall foreign policies in relation to national security, and technological R&D. All aspects of the Chinese military are to be improved from better-educated manpower, to fostering technological R&D, to adherence to rule of law. It also touches on Chinese foreign policy goals which involve an agreement of the

“One China Policy,” protection of state sovereignty over regions such as Taiwan, and that China simply wants to promote peaceful, economic development throughout the world. The section on technological security was brief and gave a vague idea of how science and technology were to be used for national defense. In sum, the paper’s idea of technological security and use was “weaponry equipment” (IOSCPRC, Section VII, 2010).

Another section of the 2010 *White Papers* define civilian Internet use. The Internet in these papers is about developing technology, improving industrialization, promoting news, ensuring nation-wide access, “[disseminating] illegal information online” (IOSCPRC 2010), keeping the free and safe flow of information, and preventing online threats. This policy focuses on the civilian arena, particularly when rule of law is concerned. The *White Papers* also discuss using the Internet to communicate with foreign countries and the United Nations in order to do business and to maintain social stability. However, because of the increase in cyber-attacks worldwide since the beginning of the new millennium (Center for Strategic and International Studies, 2005), China has had to change its definition of technology to include the term “cyber” and has had to define how to combat the problems presented by being connected to the Internet.

The drive for the new policies was to promote peace and economic stability both within and without China (Sutter 2012, 5). China’s execution of that plan, so far, has been in Foreign Direct Investment, investment in other countries’ infrastructures such as with Nigeria and the Democratic Republic of the Congo, and other forms of “soft power” (Perlez 2012). Presidents Xi Jinping and Barak Obama met in September 2015 to discuss cyber-attacks among other topics; both leaders promised to cooperate on cybersecurity issues and policy (The White House, 2015). As has been the case, what leaders promise and what they actually deliver are often two very different things (Runciman 2008). Adam Segal blames Chinese leaders who do nothing about

developing home-grown technological innovation, and end up cyber-attacking governments as well as private companies to steal information (Segal 2013). Private companies are vulnerable to cyber-attacks from either ignorance, laws requiring certain information to be available online (such as the United States Patent Office making patents available online) or hard- and software that are out of date. Most government and private entities allow these attacks to happen because of insufficient cybersecurity, and only properly arm themselves in the event of a cyber-attack. “Most private companies that are hacked today specialize in technology, which is indicative of the nature of the attacks” (Rogers 2015).

The Chinese government supports its economy by whatever means it can, like injecting money into the economy or by buying stocks (Magnier 2015). Chinese foreign policy has been tailored to ensure peaceful economic stability within and without China and focuses on soft power to work in harmony with the international community (Ministry of National Defense of the People’s Republic of China, 2015). China seeks to drive the country to modernization through growing the economy which will trickle into other areas such as social stability (IOSCPRC 2015). To achieve these goals the *White Papers on Military Strategy* assert that China must increase technological R&D. “There are many ways to improve technological R&D, such as technology conferences or symposiums, but in order to build technological R&D foundation of its own, it must build an educational system that fosters such creativity” (Rogers, 2015). Unfortunately, when this policy was adopted and implemented by the Chinese government, there was an uptick in cyber-attacks made on private, technologically-focused companies, some of which were blamed on China (CSIS 2014).

### 2.2.2 Military Strategy (中国的军事战略)

The *White Papers on Military Strategy* that was published in May of 2015 outlines ideas and plans for how China will protect itself (Miou 2015). Because of new national and foreign policies that focus on developing peacefully both inside and outside the country, as well as recognizing the technologically advancing world, the CCP has implemented policies that work in tandem with these ideas. The PLA, which is the umbrella term for China's military will technologically develop like the rest of the nation, and will be part of the harmonious society the Chinese government wishes to share with the rest of the world. The PLA is to maintain a defensive posture only and will attack if and only if it is attacked. Until this happens, the PLA is to practice the "strategic concept of active defense" which is indistinctly defined as maintaining a defensive posture while preparing for a "post-emptive strike."

The general goal of the PLA is to protect and strengthen China, its borders and its people. The policy takes this goal from the surface of the earth to outer space and cyber space, saying that security needs to be holistic and organic like that which it protects. The PLA realizes that in order to protect China it must adapt and modernize its forces as well as work more with civilians and "civilian infrastructure" through Civil-Military Integration (CMI). Without specifics, the policy's basic strategy regarding CMI is to "enhance education in national defense and boost the awareness of the general public in relation to national defense" and to make "military and civilian resources [more] compatible, complementary and mutually accessible."

Here, the main strategy is to develop the military in such a way that it will adapt to any situation. The policy mentions how wars have been shifting and changing from being conducted on the physical battlefield to cyberspace, and reiterates the importance of adaptation and allowing the PLA to be more holistic. In order to follow through, the plan is to reduce the size of the military and steer away from "mechanization," (physical forms of protection like guns and

bombs) towards “informationization” or 信息化 (xin xi hua). This shift means that the military will focus on obtaining information—most likely from the Internet—and use it to secure the country as well as bolster cybersecurity forces. The PLA must do so while supporting economic and social development within China.

### 2.2.3 Peaceful Development (中国的和平发展)

The policy *White Paper on Peaceful Development (中国的和平发展)* begins with a summary of Chinese history. It relates a different point of view of the events beginning with the Opium Wars all the way up to Deng Xiaoping’s opening to the rest of the world in 1978. It describes how China was forced to open to the West, how it was aggressively turned into a semi-colonial, semi-feudal state, and how its people have struggled for class equality. It alludes to other “difficulties and setbacks,” such as nationwide starvation just before Deng’s reforms, and concludes that through the struggles, China has “succeeded in finding a path of development . . . the path of socialism with Chinese characteristics.”

The defining characteristic which runs throughout China’s 2006 policies is “peaceful development” (Fan 2006). It has also been translated as “harmonious” development or interpreted as promoting a “harmonious society” (和谐社会, hexie shehui) (Fan 2006). China’s map for peaceful development is to “[uphold] world peace and contribute to world peace through its own development. . .with its own efforts and by carrying out reform and innovation; at the same time, it should open itself to the outside and learn from other countries” (IOSCPRC 2011). With help and cooperation from other countries who wish to mutually develop—in this context, development of the economy—China plans to accomplish this goal. Two other concepts that are mentioned frequently in tandem with peaceful development are scientific development and

independent methodology. Scientific development is defined here as adhering to rule of law to allow the economy and society, among others, to develop naturally. To accomplish this goal, the CCP needs to “[put] people first,” to respect human rights, and respect the balance of the Chinese ecosystem from the people to the government to businesses to the world at large.

### *2.3 The Constitution of the People’s Republic of China ( 中华人民共和国宪法)*

In the United States, the Constitution is the law that not only protects the people’s rights but also defines what it means to be American. In addition, this document was written almost in defiance of the British who ruled unfairly and caused Americans to rebel; the British displayed what governance should *not* do. *The Constitution of the PRC ( 中华人民共和国宪法)* is similar in these aspects. The Preamble has a short history of China, briefly describing the ages of imperialist rule in two sentences, and then casually but nebulously mentions Sun Yat-sen (1866 – 1925) and his accomplishments—or lack thereof—in another two sentences. After this, Mao Zedong is credited with overthrowing imperialism, bureaucracy, capitalism, and feudalism and with establishing a great democratic society for the people. The preamble explains why China had to shift from communism to socialism under Deng Xiaoping, and gives reasons for territorial rights and privileges such as relate to Taiwan. It also warns against “chauvinism” in the form of “big-nation,” Han nationality, and “local-national,” patriotism instead of identifying as Chinese. This is to say that China is diverse, that separating into groups will split the nation, and that the people should be loyal to China. It subtly supports political decisions that were made for the past century, referring to them as “struggles,” and concludes that “the future of China is closely linked with that of the whole world” and that cooperation and harmony at home and abroad will “preserve national independence and develop their national economies, and [strive] to safeguard

world peace and promote the cause of human progress” (National People's Congress of the People's Republic of China 1982).

#### 2.4 Analysis

The *White Papers* are a vague summary of policies that China has or intends to put into practice. It lacks data on most of its claims, but where it does have data there are no citations or reasoning from which a layperson could make connections or search for the information herself. There are also ideas and concepts that, because they are unexplained, are contradictory with reality, such as taking scientific measures to peacefully develop economically and socially, and yet there is civil unrest in places such as Hong Kong. The *White Papers* write that in order to protect its people and adapt to the changing world, China must be innovative, develop peacefully, and educate its citizens better. But how can China be innovative and close-minded at the same time? Innovation is original, analytical, and creative thought put first into a design, and then put into use. Innovation is the backbone of technology today, especially since the strength of any government is in its technologically advanced arsenal, an idea that has proved true since the Cold War. With this definition in mind, why do Chinese hackers look to patents and private businesses and take their ideas? The answer to that question lies in the place where creativity and analytical skills originate: the classroom. China’s curriculum is lacking, and Chinese parents know it. *The New York Times* article entitled “The China Conundrum” reveals that most Chinese students are being sent abroad to Western schools even if the student’s English (or host country language) is poor to non-existent (Bartlett 2011) because Western countries have been successful, especially economically. English is the language of business, and Chinese parents want their children to function in business and know that a Western education is valued more than a Chinese school education (Bartlett 2011).

The fact that Chinese education does not support innovative thinking has been noted by its own leaders. President Xi Jinping visited the United Kingdom and gave a speech at the Institute of Education talking about the importance of education and its effects on economy, and said “do not play enough” (Richardson 2015), referring to the rigid and derivative educational system China has. “Sir Anthony Seldon, an author and academic on education at Wellington College, gave his own speech in Shanghai saying that the human element is what pioneers innovation, and that robbing individuality and social skills from students will keep them from improving their financial lives” (Richardson 2015; Rogers 2015).

“Having a wider-range of experiences and skills in school can give students a set of holistic problem-solving skills which they can use in the real world. Chinese schools are often in session twelve hours a day, which means, with few other opportunities to learn such skills, curricula must reform and adopt methods to teach such skills. Lack of analysis and self-reflection fuel an inability to problem-solve and to even create. Cheating is rampant on college entry exams in China (Bartlett 2015), and it is a practice that is carried over into college applications. This behavior of cheating is also prevalent in other forms of Chinese society: the government. Xi Jinping’s mission when he entered office was to end corruption in the government (C. Li 2014), which is a reaction to a set of behaviors expressed by Chinese students, but on a smaller scale. Cyber-attacks on governments and private corporations are no different” (Rogers 2015).

The media has revealed that both China and the United States hack other countries for different reasons. U.S. cyber-attacks collect information from not only other countries but also from its own citizens because of its policies on counterterrorism (Toxen 2014); Chinese cyber-attacks collect information on technology because of its policies on technological R&D. Are either to blame? Warner cites Sunzi and Kautilya who first wrote on espionage, saying that it was essential for each government’s survival (Warner 2014, 11-14). President Xi Jinping’s recent visit to the United States revived this topic. Just before the two leaders met the *BBC* reported that Chinese police arrested hackers on a list supplied by the U.S. government. This gesture was significant on China’s part because it demonstrated a desire to cooperate with other



countries, but China must generate its own R&D and respect third parties' intellectual property. China must find its own community of creators from within, and reforming their cybersecurity and education systems will develop a talent pool willing to play with technology and push its boundaries. "By changing the strict culture that exists in Chinese classrooms now, China can catch up to Western countries' growth in economy and technological R&D. Only then can China hope to solidify its economic future and begin to protect its cyberspace" (Rogers 2015).

At the same time, any country, not just the United States, must educate and secure its country's information and intellectual property. In light of the data presented by CSIS on cyber-attacks and in the Committee on Foreign Affairs Hearing, there is an increase in attacks made on private companies and individual patents. To secure their information and intellectual property, the U.S. and Chinese governments must rethink how to interconnect intelligence safely and learn to appreciate why these attacks are occurring as well as to understand why the other country is reacting the way in which it is.

## **Chapter 3: The Opening of China and Its Effect on Contemporary Chinese Cybersecurity Policy**

This chapter will briefly retrace Chinese contemporary history focusing on economic, national security, and foreign policies. Once that is accomplished, how China came to establish the Internet and its contemporary cybersecurity policies will be retraced and explained. Based on the reasons for the genesis of these policies, their effect on aspects such as economy, education, and foreign policy will be explored. Then, an examination of cybersecurity incidents and definitions of cybersecurity terms will precede an analysis and comparison of the cybersecurity policies themselves, how they are put into practice, and their effects on China. In addition, data provided from news reports, CSIS, and the United States Computer Emergency Response Team (US-CERT) will demonstrate how Chinese cybersecurity affects the rest of the world and determine if China succeeds in harmonizing with other countries. We begin where Deng Xiaoping began to reintroduce China to the world.

It was Deng Xiaoping who brought China out of its dark age, just after the death of Mao Zedong. In 1976 Deng Xiaoping opened China to the West, the first time since the Communist Party first came to power in 1949. Mao Zedong had closed the “iron curtain” on the West which represented both the capitalist bourgeois and century of shame in which Chinese territory was occupied by foreigners. Mao had to move the country forward, and in order to do that he would unite the people under Marxist doctrine (Vogel 2011). Anything that resembled the West including capitalism, elitism, and classism, all of which would have helped sustain the economy, was disavowed by Mao who was a philosopher, not economist. Through exile, purges, and almost losing his son, Deng Xiaoping rose through the ranks and came to power in 1976 when Mao Zedong suffered a stroke. Once in power, if he did not know already, Deng realized that he

had his work cut out for him. One of the most important decisions he had to make was to transform China while maintaining the ideology that kept the country unified and him in power.

Deng Xiaoping realized that China suffered under the communist model, so he set out to change Chinese national and foreign policy. He knew that China's economy as a whole was backwards with no innovation or original creation, that China's military was weak and undeveloped, and that working with Western countries provided the solution to these problems. His goal was to work economically with the West in order to improve "backwards" China (Vogel 2011, 218), which meant government reforms as well (224). This "light spark" (227) launched China into a new technological era which consisted of Chinese delegations to foreign countries, including Japan and several countries in Europe, which learned from experts and copied the techniques and technologies to bring back to China (342).

Although it changed its ideology by working with Western countries and by implementing new methods of doing business and growing industry, China was nowhere near being able to develop technology needed to improve industry. Today China still continues this practice of inviting companies, especially companies that outsource labor (Jordan 2013, 118) and uses them as teachers instead of fostering its own technological growth. As Gu Jibao suggests in *The Importance of Social Capital to Student Creativity within Higher Education in China*, in order to achieve this desired goal of innovation and growth within Chinese society, creativity must be taught and encouraged in education, even graduate school (Gu 2013, 14). Deng Xiaoping was well aware of this need (Vogel 2011, 17) and decided to do the same with his own government by sending delegations of his own to various countries, particularly Eastern Europe in the early 1980s, to learn how to "reform" Chinese economy and industry (459).

There were educational exchanges with Western schools and with foreign companies which established themselves in China and trained Chinese workers and managers (Vogel 2011, 456), but reform in educational curricula never included fostering skills such as creativity or analysis for innovation (Jin 2011, 28). And it shows: examples of cyber-attacks on Western companies mentioned later in the chapter will show this method still in use. Stating its desire to promote peace and economic prosperity China has continued to foster its economic growth both at home and abroad (IOSCPRC 2010). These above policies continued into the twenty-first century and were applied to the Internet and computer technology when they became more widely used.

Conferences such as Internet Networking (INET) and Internet cooperation were becoming frequent occurrences in the early 1990s, and Chinese computer specialists were sent to request access to such technology by the government, most notably, the China-U.S. Joint Committee of Science and Technology Cooperation held in early April of 1994. The Committee worked with the U.S. National Science Foundation to gain access to the Internet, and on April 20<sup>th</sup>, China made its first network called CAINONET (中国高速信息示范网) in Beijing on a 64 kilobyte bandwidth (Ventre 2014, 3).

“China has made inroads on its technological innovation, and has even poured more concrete in the past decade than that of the whole United States in the twentieth century (Gates 2014), but China would need to continue to rely on foreign businesses “setting up shop” and learning the trade in order to keep up growth. To generate growth and innovation inside of China, in order to improve its economy, China needs to nurture critical thinking and creativity in its educational system” (Rogers 2015).

China tried to generate creativity and innovation among the Chinese people, not borrow it from elsewhere like an American or European government cooperation or private company. However, without the educational or societal foundations that would allow creativity to flourish, how could

China invent and innovate? Most intellectuals were either killed or silenced during the Great Leap Forward or the Cultural Revolution. So it is not a wonder that China borrowed innovation and not made its own.

There is a fundamental flaw in Chinese education that has been left over from Deng Xiaoping's reign. At that point in time it might not have been a flaw, but keeping the education system in China relatively the same while sending students abroad leaves China without a foundation to generate its own ideas and its own growth. Deng's original efforts were suited to the time in which he lived, when complete economic and industrial overhaul was needed, but now that China is on its feet, it still relies on other countries for sources of revenue. China is still lagging behind in its technological output relative to its creativity (The Economist Intelligence Unit [EIU] 2014; Asian Development Bank). According to the Asian Development Bank's particular Creative Productivity Index, Chinese technological research and development is low, meaning that incentives and the fostering environment needed for innovation are missing and that patents or new research generated in the science fields are low (EIU 2014, 5-6). Because of the constant growth of technology, there is an increasing need for fostering flexibility and adaptability in our modern world, but the growth in technology is coming from Western countries, not China. So far, the only hand that China has played in the technological revolution is manufacturing. If China could both develop its own products and manufacture them in country, it would be self-sufficient, but as it stands, China would need to overhaul its educational system to nurture skills in creativity, critical thinking, and analysis. The only way that students can learn how to adapt, to be creative, and to innovate is to change the curriculum to one that teaches critical thinking and analysis.

Charles Kivunja of the University of New England makes a case that lesson plans must focus and prepare students for flexibility with “21<sup>st</sup> Century Skills” (Kivunja 2014, 3) that will help the students navigate this constantly evolving world. Other studies, such as those conducted in the European Union, have also supported the claim that there is not only an important link between creativity and sustainable technological development but also that, in theory, proper curriculum will foster its growth (Detterbeck 2014; Sleuwaegen 2014). Famous educators such as Sir Ken Robinson have talked extensively about how the current education system in both the United Kingdom and the United States “kills creativity” (Robinson, 2006) and thereby affects all other aspects of a country’s population, including the economy (Robinson, 2010).

Sir Robinson criticizes modern Western education in general for adhering to an industrial model created during the industrial revolution which now serves no purpose in a modernized, digitized world. He points out that education is now wholly standardized, and that it focuses on teaching students how to take tests rather than how to analyze or to “think outside of the box.” The current Chinese education system is largely based on Western industrial-age paradigms because of the educational exchanges that Deng Xiaoping began in the late 1970s, and this model is one that Chinese parents want to use for their children’s education (Rogers 2013, 9-13). Teaching for the sake of testing is, according to Robinson, continuing a paradigm that has no support for different kinds of skills or intelligences. Classes in China have followed this industrial model closely, so much so that more Chinese students are leaving the education system for Western schools than ever before (Bartlett 2011).

Deng’s policies were able to get China’s foot into the international economic door, but since the economy in China depends on foreign companies for innovation, China recently turned to cyber-espionage as a faster means of economic growth. Cyber-espionage and “hacks” are

both similar terms which mean they hide programs such as malware within a computer system that transfer information back to the malware's origin. A cyber-attack is different from these because it can shut down a system, Internet access or computers, and disrupt communication. Hacking is more common than cyber-attacks because of the information it can procure, and, as the CSIS timeline shows, hacks on government entities were also more common. American-based news organizations report Chinese hacks on American companies more frequently than before (CSIS 2014) because most hacks that were reported pre-2014 were government hacks, not civilian. That being said, numerous reports from other countries revealed Chinese hacks on private companies were dated earlier than those reported by American media. American-based company Symantec, provider of Norton Anti-virus software, reported in 2011 that nearly fifty chemical companies worldwide, mostly in Western and developed countries, reported data stolen by hackers in China. According to the report, the company attacks were in the industries of "research, development, and manufacture of chemicals and advanced materials" (Chien 2011). However, cyber-espionage was a small news-item until more private companies were hacked, and Edward Snowden's National Security Agency (NSA) revelations were reported.

As mentioned before, as early as 2007 Western media reports blamed China for the few cyber-attacks and hacks made on private facilities, but beginning in 2009 there was a switch from mostly attacks on government facilities to a proportionate smattering of attacks on both government facilities and private companies. Laboratories, power supply stations, supermarkets, and even presidential campaigns were claimed to have been hacked by China (CSIS 2014). Cyber-attacks on Google have now become infamous in the wake of Google's announcement that attacks made on its systems originated in China (Burton 2011). In 2013 the National Intelligence Estimate identified China to be the "country most aggressively seeking to penetrate"

American businesses to steal data for economic gain (Nakashima 2013). Despite the 2013 visit between Presidents Xi Jinping and Barak Obama, cyber-attacks and hacks on private American systems and institutions continued to multiply, and companies which were the victims of hacking had to resort to relief from the judicial system.

According to Jones' 2013 report, approximately thirty-two Internet security cases were conducted through the Department of Justice accusing Chinese citizens, some of them PLA officers, of hacking into United States government computers. Because of the upsurge in attacks, the United States government has taken measures to protect not only government intelligence but also intellectual property. In May of 2014, a Federal District Court in Western Pennsylvania charged six PLA officers with various cyber-attacks. Director Huang Chengqing of the National Computer Network Emergency Response Technical Team/Coordination Center of China (CNERT) pointed out that the court cases charging PLA officers in absentia were counter-productive and that had the United States government been willing to talk with either him or other Chinese government agencies, the problem would have been solved. The same report claimed that CNERT has been working with the U.S. government on those thirty-two Internet security cases, most of which were “[handled] most promptly except for a few that lacked sufficient proof” (Jones 2013).

Any computer connected to the Internet is subject to hacks, no exceptions, and if companies want to keep information safe, they need constant and consistent updates to their cybersecurity protocols. Jones paraphrased Director Huang saying that he “did not deny [the report on the hacks], but suggested that if the U.S. government wants to keep weapons programs secure, it should not allow them to be accessed online . . . . ‘Even following the general principle of secret-keeping, it should not have been linked to the Internet,’ Huang said” (Jones 2013).



Director Huang is correct. The testimony of Pat Choate, director for the Manufacturing Policy Project, before the Oversight and Investigations Subcommittee on Foreign Affairs (OISFA) places responsibility for the hacks not on China, but on the United States itself. He points out that, by law, all patent applications must be posted on the Internet eighteen months after the filing date and that it is the government's responsibility to change the law to protect intellectual property (OISFA 2011, 7; Rogers 2015). Because U.S. patent applications are on the "oldest computers in the Federal Government" and wait for about six months on the servers before review (Burton 2011), they are easy prey for the constant cyber-bombardment. According to Western media outlets, the attacks originate in China, and the Chinese government has largely remained silent save for Mr. Huang's comments.

Chinese policy says that it must peacefully, scientifically, economically, and socially develop in harmony with the rest of the world, but that contradicts accusations made by Western news outlets and the United States Congress. Along with these contradictions, the *White Papers'* vague claims undermine its authority. Official Chinese statements to the press may deny cyber-attacks and the *White Papers* may claim that China wants to peacefully develop in harmony with other countries, but without the sufficient data to support the claims how can either be taken seriously? To check the data's authenticity one would look to the most likely source of statistics in China: the National Bureau of Statistics of China. It shows data about population and GDP among others, but outside of social and economic issues, there are no other statistics. In addition, much of the data on the site are dated anywhere from as late as 2012 to as early as 2002 (National Bureau of Statistics of China 2012). The alternative way of finding who attacks whom is through the US-CERT and the Government Accountability Office. Both provide detailed statistics with defined terms, and a logical trail of information to follow and replicate if necessary.

It is the US-CERT findings that are significant because of their focus on connections to official government systems.

US-CERT monitored the flow of data and records of connections that were made to federal IT systems by looking at the IP addresses that made those connections (US-CERT 2012). In this data set government systems were investigating other government systems only. US-CERT studied government “scans” used to gain information from “multiple targets” and to identify whoever is accessing the system (Gates 2006). A scan is used either by “system and network administrators to assess the security of a network” or by a “malicious actor [who uses the scan] to discover computer systems known to be vulnerable on a target network” (US-CERT, 4). All computers or systems that connect to the Internet send “packets” of data, each of which has a unique address like a fingerprint. Sometimes the address can be re-routed to make it appear that the packets came from somewhere else, but the origin can always be traced. Virtual private networks are similar in this way because they use the Internet from the host country but borrow an IP address from elsewhere. US-CERT collected data from scans made on what it calls “federal executive agency IT systems” (US-CERT, 27) or government systems. Below is a chart from the US-CERT 2012 findings from “Countries from Which Scans Originate”:

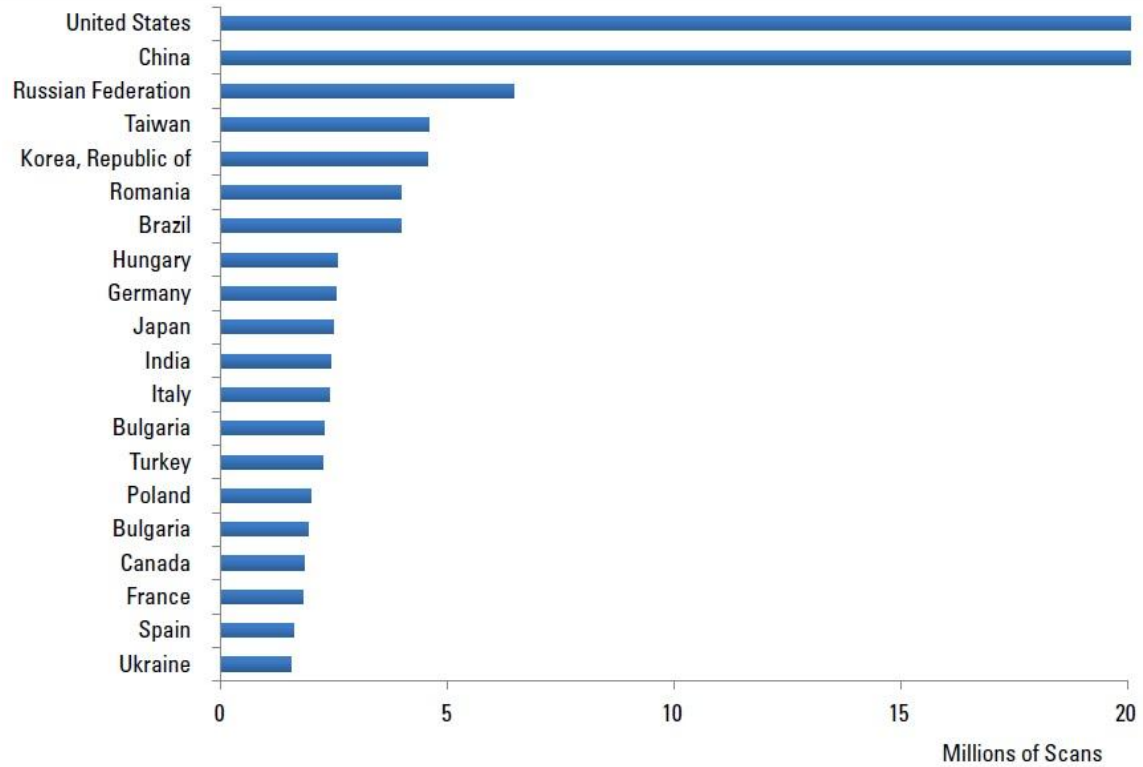


Figure 3.0 Countries from Which Scans Originate, U.S. Computer Emergency Readiness Team. 2012. “US-CERT Security Trends Report: 2012 in Retrospect,” 27–28.

This chart shows that the greatest amount of scans, or investigations, come from China and the United States, which means that China and the United States were accessing the most networks. Both countries are scanning the most out of all others in this sample, which indicates that they are more curious about other governments’ information. US-CERT provides insufficient data to say whether the scans are simply hacks or cyber-attacks, and also withhold other information, probably for the sake of security. Moreover, what the chart does not show are the dates, the times, the IP address, and the source and destination ports or the origin and ending of the access. Essentially this data shows that in 2012, the two major cybersecurity players, China and the United States, account for the most traffic on their respective government’s IT systems. This

data may show traffic but needs to identify better who scanned, or the location of the original scans, and on whom. That volatile piece of information is for foreign policy since one party could accuse another of espionage, as well as show the systems' vulnerabilities.

Since China provides little information about who cyber-attacked its systems, more data needs to be collected from different sources. News outlets have publically catalogued accusations and speculations of who scanned whom, and CSIS's timeline of global cyber-attacks provides documented incidents that serve as another guideline for gauging cyber-attacks. The timeline CSIS provides begins in 2006 and ends in 2014, and, when data is available, identifies three kinds of entities: the entity attacked (either a government or private enterprise), the entity suspected of attacking, or an unknown entity that attacked or malware such as a virus that was left over and infected systems (CSIS 2014). The chart below shows the number of attacks reported each year, and who was attacked.

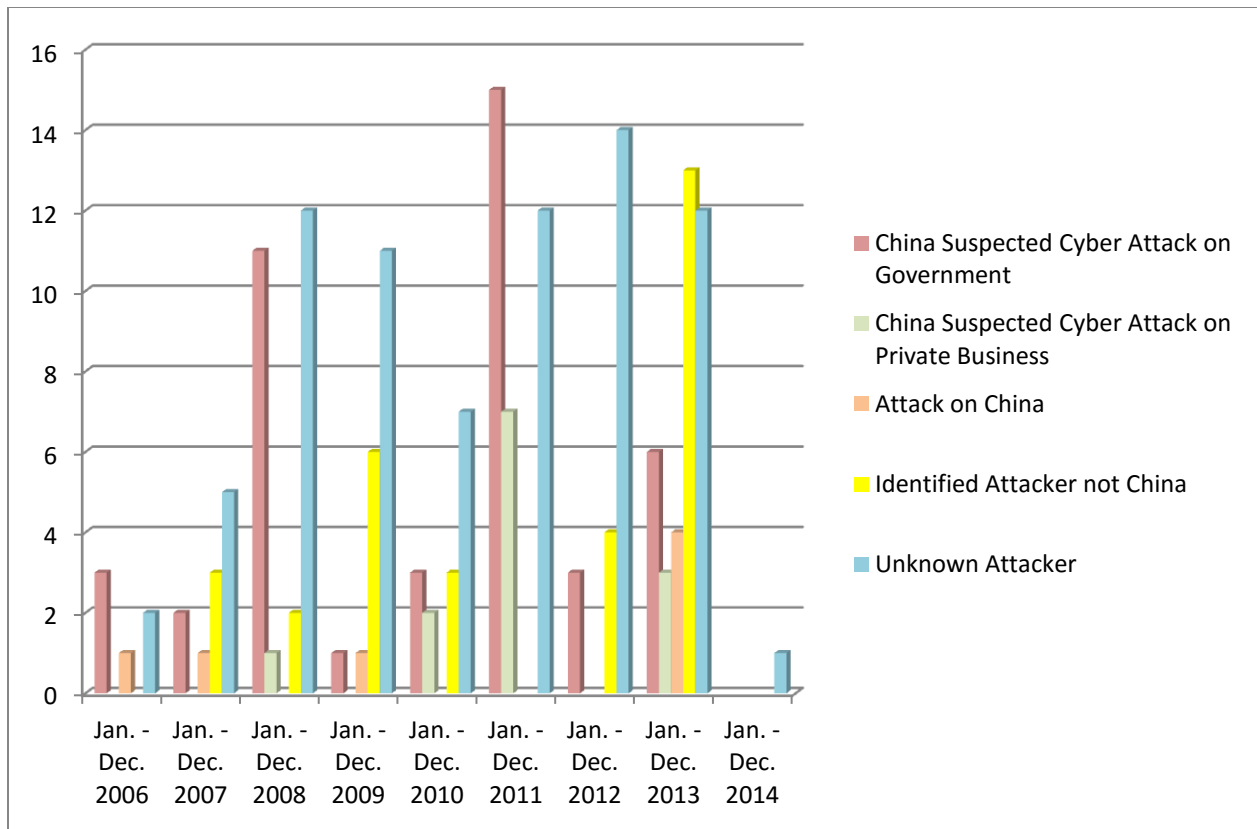


Figure 3.1, table based on CSIS data with specific focus on Chinese cyber-attacks. CSIS. 2014. "Significant Cyber Incidents Since 2006." Center for Strategic and International Studies, 2012. Accessed April 27, 2016. [http://csis.org/files/publication/140310\\_Significant\\_Cyber\\_Incidents\\_Since\\_2006.pdf](http://csis.org/files/publication/140310_Significant_Cyber_Incidents_Since_2006.pdf).

The Unknown Attacker and the Identified Attackers act as a baseline for comparison on the chart, which include not only states suspected in attacks but also private groups and individuals who have hacked into government systems or private businesses. However, few attacks on China are mentioned in the timeline, and that indicates a lack of information from both Western media and Chinese media. Granted it is not in China's best interest to admit to a cyber-attack on a government, but if Western media is reporting attacks on Western governments and private businesses, why not report that China suffered a cyber-attack just as often? Many of

the attacks on CSIS's timeline were reported by Western entities, and many also claimed they traced the IP address to China.

Even though there was an overall increase of reports of Chinese attacks on government systems, there was also an increase in reports of Chinese cyber-attacks on private businesses. The businesses, according to the timeline, claim that they lost intellectual property and suffered fiscal losses (CSIS 2014). These reports indicate that the suspected Chinese attacks on businesses are economic in nature, and have been supported by companies like Codan which received returned products that were not made by their company but whose design were copied and manufactured with inferior parts (Cronau 2013). These hacks come as no surprise knowing how China had built its economy at the beginning of Deng's administration because Chinese companies learned from, and borrowed ideas from, foreign businesses to jumpstart their industry. China is far more modernized than it was in the late 1970s and has learned to use new technologies to benefit the country, such as using the Internet as a means of economic growth (IOSCPRC 2011), but China still has a long way to go before it sees inventions and patents of its own coming into the market. One of the ways that it can innovate faster is through Internet use and the Chinese government has recognized that in the *White Papers*.

Chinese Internet capability has grown, and China is trying to expand its use in remote parts of the country to stimulate economy, education, and communication between and among citizens, and has seen most accessibility growth in the past decade (McKirdy 2015). The *White Papers* see Internet accessibility as a driver of these three things, especially economy but recently China has seen a halt in economic growth. So why is its economy slowing now? Economists suggest that, just as there are natural peaks, there are also natural valleys or even plateaus in economic growth (The Economist Staff 2015); others write that the dying momentum

is due to inaccurate information (Magnier 2016); and the rest think that China's slowing economy "has been hit by shrinking foreign and domestic demand, weak investment, factory overcapacity and oversupply in the property market" (Evans 2016). Whatever the case may be, lack of access to information or other markets can hinder economic growth.

Chinese cybersecurity policy is supposed to accelerate informationization, help build a modern logistics system, help exchange and cooperate internationally, and support national economic and social development (IOSCPRC 2010; IOSCPRC 2008). But how can it accomplish those goals with a closed Internet policy, which is in complete opposition to Deng's ideas on how to build the Chinese economy? The Great Firewall of China has eliminated a huge corner of the international economic market, not only in advertising but also product information (Frizell 2014), foreign trade, news, and business collaboration (Mozur 2016). Instead of allowing private businesses or individuals to collaborate online, the Chinese government has hacked into companies and governments, as international media has revealed (Cronau 2013), and taken patents for the sake of security. As the Chinese economy continues to slow, President Xi Jinping tightens his grip on censorship (Henchowicz 2016). If Deng Xiaoping were alive today, he would have taken complete advantage of the international portal that is the Internet, and, yes, would have censored some sites that spoke out against Chinese policy, but not to the point where a backlash from news organizations would erupt or where Chinese inventive growth would be stunted. He might have looked to other countries' policies on cybersecurity before forming his own, and analyzed how that would benefit the Chinese people.

## Chapter 4: Chinese Cybersecurity Policy Comparison

In this chapter the cybersecurity policies of five countries will be compared. Two countries are democratic: the United States and India. The others are either communist or dictatorial: Russia, North Korea, and Cuba. Russia and the United States are considered to be developed countries, while North Korea, Cuba, and India are considered to be developing countries (The Department of Economic and Social Affairs of the United Nations Secretariat 2012, 135). Once the policies are summarized a comparative analysis will end the chapter.

China has had to catch up to other countries who are twenty years ahead of it in computing and digital technology, and, as a result, China is now one of the largest consumers of technology on the planet. China could never have predicted this surge in technology use when CAINONET (中国高速信息示范网) was first established in Beijing in 1994, and, like other countries, China has yet to see its laws catch up as well. China's law is done on a piecemeal basis, much like common law in the United States or in the United Kingdom, meaning that a case which comes to court that has never been addressed before sets a precedent in the law. Other countries, like France, lack this problem because Civil Law is like an umbrella: the precedents are numerous and broad enough that they can apply to a case in court when needed. Although China is a Communist/Socialist state, its legal practices and policies resemble that of democratic states. An examination of other nations' policies will show how Chinese cybersecurity policy affects not only Chinese national policies but also its foreign policy. The countries that will be examined are democratic, communist, socialist, or dictatorial governments located in either the West or the East.



#### *4.1 India*

The Indian government first established Internet capabilities in 1986 with the Education and Research Network (ERNET) (Press 2003) but had computing technology since the mid-1950s (India Department of Electrical Communication and Engineering 2016). Nearly sixty years later, Indian national cybersecurity policy was codified. Therein are nine pages which discuss the importance and the pervasiveness of the Internet and how cyberspace is the medium to which people connect and interact with each other. For India, the Internet is a way to make a living, to educate oneself if necessary, and to carry out tasks more quickly and efficiently. In the next paragraph of the policy, cyberspace is defined as a place that renders the visitor vulnerable: any connection to it can let in a hack or a virus. These “cyber incidents” will cause the government to respond, and the policy continues to identify the kinds of incidents that can occur. The main point of this section is the preservation of safety and security for individuals and for the government in cyberspace; this protection is at the heart of cybersecurity policy (India Department of Electronics and Information Technology 2013). Overall, the policy is holistic in the sense that it recognizes when a device is connected to cyberspace (which includes the Internet and intranet) (American Civil Liberties Union et al., v. Janet Reno, Attorney General of the United States, American Library Association, Inc., et al., v. United States Department of Justice et al., Nos. CIV. A. 96-963, CIV. A. 96-1458) and/or the Internet and is vulnerable to whatever else is connected to it or within it.

The Indian government’s vision for their cybersecurity policy is “to build a secure and resilient cyberspace for citizens, businesses, and Government.” Its mission is “to protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents

through a combination of institutional structures, people, processes, technology and cooperation”(India Department of Electronics and Information Technology 2013). This outline is in lieu of a description of how to handle situations that may arise within the cybersecurity realm. This cybersecurity policy was published in 2013, but India has had to deal with cyber issues since long before that. India’s Information Technology Act (IT Act) of 2000 established rules and guidelines for Internet conduct. Cyberspace and cybersecurity is viewed in the 2013 policy as an entity—much like a dog—that has to be watched and handled with care. In the IT Act defines the Internet is a tool that, if abused, would cause the violator to be prosecuted. The IT Act took on an internal, national-security focus, instead of a policy that is for international parties to read and understand. The IT Act, because of the way in which it defined the Internet and how it is governed, thus came into conflict with an individual’s right to privacy.

India is a signatory to the UN’s Universal Declaration of Human Rights (India Department of Electronics and Information Technology 2013) which states an individual has the right to privacy; this right is at odds with security of the state and its laws on Internet. The IT Act was a way for the Indian government to “regulate the interception, monitoring, decryption, and collection of information of digital communications”(Krishna 2015, 4) which includes monitoring any information on any device and names hacking in Chapter 11 Section 66 as illegal. That being said, however, there is a failsafe in place. The only way that this monitoring would be sanctioned is if these above measures protected India’s sovereignty, defense, security, “friendly relations with foreign states,” and the status quo (Krishna, 12). If there is any such violation, the local government addresses the situation.

China is similar to India in this respect, in that decentralization may aid the government, which is understandable since the populations of both countries are at least four times that of the

United States (Demographic Internet Staff US Census Bureau 2016). Chinese law on cybercrime has a wider definition on the type of persons who can commit a crime, as well as whether or not they collaborate with others (China Law Translate Staff 2014). The *Supreme People's Court/ Procuratorate & The Ministry of Public Security's Opinion on Several Issues Regarding the Application of Criminal Procedure in Handling Cases of Internet Crime Public Announcement 2014 No. 10* describes the procedures. Because this law is concerned with both security and privacy, personal or property rights are to be preserved in preliminary investigations if there is no hard evidence. There is no mention if those same laws will apply or if the government will step in if there is hard evidence in the case or under what circumstances security will trump privacy.

#### 4.2 United States

In 2013 Edward Snowden shed light on American cyber security policy by revealing that the NSA collected and surveiled citizens' telephone and computer data without warrants (Toxen 2014). It was a controversial leak, and demonstrated that individual privacy rights had been violated. It also came as a shock because the United States was one of the principal drafters and promoters of the Universal Declaration on Human Rights which, although not legally binding, upholds the idea of an individual's right to privacy. To add insult to injury, the United States was perceived as a country concerned with freedom—the very concept of that perception, among others, is apparent in massive immigration to the United States in the twentieth century (History.com Staff 2009)—and yet it violated its citizens' freedom of privacy. Since then, the United States has attempted to improve its cybersecurity policy so that it balances citizen privacy with security and data collection.

The United States has one of the longest—if not, the longest—history in cyber technology. The first technological innovations in digital and Internet computing were

introduced in the 1960s and came from developed, Western countries, the U.S. in particular (Martin 1999). The United States made technological inroads in the late 1960s and early 1970s when it experimented with the concept of an intranet which allowed the military and law enforcement to communicate securely. Almost as soon as the intranet was developed cyber-attacks were reported by the Central Intelligence Agency (CIA) or the Pentagon (Warner 2014, 243). This is indicative of increasing technological growth and especially innovation in both computer hardware and software. Computers began to process more data at more rapid rates, and the only way to support the growth in technology was to fund its R&D.

“Warner wrote about the Soviets losing ground in the cybersecurity arena because of lack of funding which caused static growth in their technological development and economy, and the United States almost fell into the same trap. Nevertheless, the Soviet Union was less fortunate: not only did economic instability threaten its intelligence, but also a political coup” (Rogers 2015, 7).

The United States continued R&D for technology despite a shortage of funds, enlisting the help of students and civilians who pioneered IT from the 1960s onward. A scientist at M.I.T. and the Advanced Research Projects Agency (ARPA), J.C.R. Licklider first invented Internet technology in 1962 (Martin 1999). His idea to link computers that could send and receive data between and among themselves reinforced government systems and telecommunications in case they were destroyed (History.com Staff 2010); an important advantage to have in the Cold War. This system, called “ARPAnet,” was the first way that computers could send “packets,” or small amounts of data, from place to place.

“It was because of the Cold War threat from the Soviet Union that the United States continued to allow technological R&D within its military, but if small businesses and other civilian enterprises to do business had to use government-run servers and Internet (Warner 2014, 261). In the late 1980s, the Pentagon renounced its policing of the Internet, and businesses could finally use privately or civilian-provided Internet without logging into government-run servers, as an easier and swifter means of communication. Warner implies that by allowing

civilian access to this technology that anything from computer hardware to software was improved” (Rogers 2015).

From this point on, the United States government used “commercially designed devices running the now-ubiquitous Microsoft operating systems...many of which in turn were linked in 1994 by an Intelligence Community-wide network called Intelink” (Warner 2014, 261). Instead of relying on weather-prone satellites, intelligence could be passed quickly from the field to the office via a landline. For the first time all U.S. government intelligence agencies and military branches were connected, and all had access to each-others’ information, with proper clearance of course (Martin 1999, 6) much to the joy of General H. Norman Schwarzkopf who complained of delayed intelligence reports (9).

“Intelink was technically an “intranet” which means that connections to the Internet were partially blocked off from outside use, because intelligence data still had to pass through the Internet which long distances. So while there were security measures in place to prevent outsider-access, Intelink was still exposed to spies, such as Ana Montes and Robert Hanssen (Warner 2014, 261). In this case, because of technological improvements, these spies were able to find the access points via the Internet to Intelink, were able to circumvent various “protocols” or “firewalls,” and take information. In this way the intelligence community was able to see the “chinks in the armor,” and either patch them, or find other ways around the blocks. Once Intelink’s dated technology was overwhelmed by computer innovations, commercially-owned networks and devices were used more frequently by consumers for their homes and businesses (Warner 2014, 261), as well as contracted by government agencies (Warner, 262)” (Rogers 2015).

In 2002, one of the last laws written about cybersecurity before a lapse in cybersecurity legislation was the Homeland Security Act. The Act did four things: defined cybersecurity terms, established the Department of Homeland Security, outlined procedures and who to contact in the case of cyber threats, and even immigration procedures. There was a notable shift in cybersecurity law around 2011, two years after an increase in cyber-attacks on private businesses (NATO CCDCOE 2008). It was during this time the United States Congress began passing bills to protect technological R&D (United States Congress 2011), such as bills for the National

Institute of Standards and Technology Act, the Cybersecurity Enhancement Act 2011, and The Cybersecurity and Internet Freedom Act 2011. Crudely put, the acts wanted to protect American intellectual property from a cyber hack or attack while allowing the free flow or “Netflow” of Internet traffic.

### 4.3 Cuba

China is considered isolated in comparison to other countries because of its censorship (Anderson 2010), but Cuba is more isolated in terms of infrastructure and outside influence. Its history is tumultuous, full of power struggles and instability followed by a dictatorship which brought about stability. Since the Cuban Revolution in 1959, Cuba nationalized all businesses, American establishments included (BBC Staff 2015), and denounced “Yankee imperialism” (Myre 2014). Cuba began forming ties with the largest communist country in the world at that time, the Soviet Union, so President Eisenhower placed economic sanctions on Cuba and cut diplomatic ties. Cuba chose the slow and steady route, much like China, developing wealth and fair distribution slowly over time (Glennie 2011). Cuba eventually exchanged its communist identity for a socialist one and Fidel Castro, who had led in troops to dethrone the democratically elected Fulgencio Batista, became president. Wars on the African continent and tightening embargoes from the U.S. had put a strain on Cuban citizens, which caused a mass exodus to the United States. Ties between the now Russian Federation and the United States were fragile at best, and, although Cuba did receive help from both in the form of either food or technology, Cuba still suffered economically and technologically.

On a technological level, Cuba is even more impoverished. According to Daniel Ventre in his book *Cyber Conflict: Competing National Perspectives*, “Cuba has one of the world’s lowest ratios of Internet users to head of population,” and views the United States as the cause of

it, whether it be because of sanctions or lack of technological cooperation (Ventre 2013, 3). Cuba's cybersecurity goal is to generate and preserve national doctrine on the Internet (which is actually an intranet that only the Cuban people will view). The reason for this is to stop foreign nations from influencing public thought. Foreign ideas are considered by the Cuban government to be counter-revolutionary, a Marxist precept that values revolution and struggle against capitalism and socio-economic class, in a way to make all equal, no one above or below anyone else (Riegel 2005). When the United States passed a bill in 2015 allowing American telecommunication businesses to expand into Cuba, it was an opportunity for more Cubans to have access but a challenge for providers like Verizon and Google to understand and deal with Cuban censorship (Markowitz 2015).

#### *4.4 North Korea*

North Korea is an incredibly cloistered country, so what little the outside world knows of North Korean cybersecurity and military capabilities comes from reporters who cross the border to retrieve information about anything from the cyber-attacks it claims to have executed to census data (A+E Networks 2010; Haggard 2015). The most famous of the cyber-attacks from North Korea is the hack on Sony Pictures Entertainment which postponed release of *The Interview*, revealed private employee emails, and the employees' personal information (Grisham 2015). This is not to say that the government's sole mission for the Internet is a means of attack. Since the death of Kim Jong-Il, the North Korean government made a point of changing its communications policy to increase its Internet use (Altenberger 2014). This move would be contradictory to a regime bent on isolating its nation; however, in order to survive in our globalizing world, and to demonstrate the regime can be flexible and provide for its people, the new administration has adapted the use of Internet.

If designed and monitored properly, the “Hermit Kingdom” can preserve its solitude and effectively create an intranet much like Intelink. The whole purpose of giving the North Korean people the Internet—albeit a small percentage of the population—is to allow more communication between citizens. Much like China’s national policy for peaceful and sustainable economic and social development, North Korea is planning to use the new Internet capabilities to increase economic development and carry out national reforms. If the Internet in North Korea were to be improved, then news outlets such as the Korean Central News Agency (KCNA) could reach the outside world and carry on the ideology and rhetoric of the North Korean regime. In this way, North Korea is very similar to that of the so-called Islamic state or ISIS, wanting its message accessible to the rest of the world—although ISIS contradicts itself by using social media and the Internet to spread its propaganda even though it is a Western creation and Western-run. At present, whether the North Korean citizens have access to Internet is unclear.

So far as we know, only government employees and specially chosen citizens can go to government approved, or “government blessed,” sites (Keneally 2014). In this way it is emulating Chinese policy on the Internet in that, although there are only 10 or 15 government approved websites, the Internet is still controlled and monitored by the North Korean government for the sake of national security and the control of information. The KCNA was originally created just after the Second World War, around 1946, to foster the control of information within North Korea. When it gained Internet capabilities, it used the Internet to spread ideology through servers in Japan (Altenberger 2014, 632). Ever since, North Korea has kept tight control over citizens’ access to any information or even trade goods coming from outside of the country, of anything from newspaper articles and clothing to books and movies. Kim Jong Il is reported to have a library of thousands of contraband DVDs, which if a citizen is



found to have, that citizen would be charged with crimes against the state (Altenberger, 632). Ironically, the KCNA created channels and accounts on the U.S.-based social media outlets Twitter and YouTube. If state media is controlled, then the movement of information is also controlled, therefore the Korean people will have no idea that others are starving as they are, or are suffering as they are.

Other than through the use of social media, brave reporters, and dramatic events, there is no way of knowing the exact North Korean cybersecurity policy, but one can speculate. It is logical to assume that because of past behavior, North Korean cybersecurity policy is to limit citizen access to the Internet, to control whatever Internet access is allowed, and to fill those channels with propaganda and rhetoric. Granted, this approach may allow for more “communication” within the state in the sense that more people can possibly receive news—even if the likelihood is higher out of country—and it can reinforce Kim Jong-Un’s power by pretending to grant more access to its people. The death of Kim Jong-Il has forced Jong-un to prove his legitimacy; to increase Internet use could be his way of doing so.

#### *4.5 Russia*

Much like China, the Russian Federation has had a tumultuous recent history, going from a monarchy, to a Communist state, to a Socialist/Dictatorial state, to a Democracy, and back to a dictatorship. Under Boris Yeltsin the country did suffer economic hardship and relative governmental chaos, but under Putin the economy improved and the government was organized (McFaul 2008). Vladimir Putin is in his third term as President, and so far his policies have been focused more on military rather than economic improvement, all in exchange for more safety (Bershidsky 2014). This freedom-versus-security issue is more economic-based since free flow

of news information is not blocked by a firewall (Bershidsky), and, unlike China before 2013, Russian citizens can protest—even if it is illegal—and still walk away without being arrested.

After 2013 when Russia decided to “welcome” Crimea back into the fold, Russian citizens wildly accepted the move and supported Putin’s efforts. Western economic sanctions incited more anger, and citizens were willing to take more hits to their purses and their freedoms because of their pride in their government. From then on Russia behaved more like China and North Korea in the sense that those with different viewpoints were thought of as dissenters and were punished. While the execution of Russian National Security policy has changed in the last two decades, the policy itself has remained the same.

As of the year 2000, Russian cybersecurity policy acts an extension of the *Russian National Security Concept*. It outlines how the Russian Federation wants to interact in the world community on the Internet, what its national interests are, identifies and defines threats to Russian national security, and how to carry out those policies. In the first section of the *Information Security Doctrine of the Russian Federation* acknowledges how access to information is increasing and the imperativeness that information be secured. There is also the premise that “Russia’s national interests in the information sphere comprises observance of the constitutional rights and freedoms of man and the citizen to receive and use information” while the “information sphere,” anything on an Internet or intranet, needs to support the Russian Federation’s national security and state policy (Ministry of Foreign Affairs of the Russian Federation 2000). The Doctrine continues to assert that developing technological R&D, whether soft or hardware, will help prevent cyber-attacks or hacks, as well as secure data, and “expand international cooperation.”

The Russian Federation and China share much of their history, and in China's fledgling Communist stage, Russia fostered its growth and bolstered its defenses against the West. In the Korean War, each came to the other's aid and supported their Communist-in-arms, North Korea, but since then their relationship has been rocky. When Khrushchev came to power and changed his rule from a communist regime to a "dictatorship of the bourgeoisie," doctrines that China had held dear were changed, and Mao Zedong was forced to step away from the Russian partnership. In order to preserve the status quo in China, Mao had to paint Russia as an enemy which had completely abandoned its communist principles (Cienciala 1999).

#### 4.6 Analysis

India's cybersecurity policy protects a citizen's right to privacy if and only if that person has not violated a law. As mentioned, China's definitions on cybercrimes are wider or general, thus giving China more room to prosecute if necessary. India and China both respect the UN's Declaration of Human Rights within the limits of their respective national laws. They have both decided to decentralize the implementation of the laws. The United States has similar laws where American citizens' privacy is protected. The *Constitution of the United States of America* as well as the *Constitution of the People's Republic of China* both protect an individual's right to privacy, but recent reports have shown that these rights have been violated. U.S. cybersecurity wants to protect government and individual property and privacy from prying eyes, but Chinese cybersecurity policy lacks a specifics on what will be protected and how. Chinese cybersecurity, however, is much more open than that of Cuba's, and wants the Chinese people to have some outside access to businesses and other economic markets. In order to encourage national economic growth, China has chosen to offer comparable Chinese sites to that of Western sites, so

that it creates competition and encourages Chinese citizens to buy locally. North Korea's cybersecurity policy—or any policy for that matter—is extreme even in comparison to China's policies, and China would never agree to take such restrictive lengths. The similarities between the two countries are in the kinds of sites they censor, such as Western sites or sites that challenge government authority, but the degree is significantly different. China and the Russian Federation share a similar history and policy development. Russia is focused more on military development and safety rather than privacy, but also endures protests of any kind. China takes issue with protests and can arguably prevent or prosecute such a thing if it upsets the status quo. Russia, like China, uses the Internet for disseminating propaganda, and also both are guilty of sacrificing the freedom of speech of their people.

## Chapter 5: Chinese Internet Censorship

This chapter will identify types of Chinese censorship, how they were created, examine how they are implemented, and analyze their effects on foreign policy, economy, and society. It will begin with the evolution of censorship and its purpose in contemporary China. Then the chapter will discuss other spheres of censorship such as propaganda, specifically in education and how it affects technological innovation in China. Finally, the effects of censorship on Chinese economy will be discussed and analyzed. The three aspects of censorship in China identified here are propaganda, education, and safety. The idea of censorship as a means to economic prosperity will be questioned and analyzed.

Contemporary Chinese censorship dates to the beginning of the Mao regime with propaganda posters and slogans that demonized Western states or any voice that spoke against communist ideology. Theodore Chen wrote in 1951 that China had declared itself to be a “democratic dictatorship” in which the state would crack down on counterrevolutionaries who would disrupt the system while allowing certain kinds of democracy to flourish (Chen 2016). Here he reiterates that force is not the only means of control. He describes this kind of rule had two branches which used two methods: the dictatorship which used force and the democracy which used propaganda to manipulate information. Propaganda was perfectly suited to Chinese Communist ideology, because Communism was a concept the Chinese people had to learn—and in a way, unlearn imperialistic culture—it comes as no surprise that propaganda posters were a way to send information and to teach to the Chinese people. From here, controlling information meant government security, and assurance that laws would be followed.

That idea continued until today with Xi Jinping’s crackdown on political corruption and tightening of his rule; his methods smack authoritarian. He has been seen visiting newsrooms

and shaking hands with newspaper editors, saying that they must continue their loyalty to the Communist party in “their thoughts, politics, and action” (Simpson 2016). Xi Jinping visited media outlets because they are the only way mass amounts of information can reach across China: if they are controlled, Xi Jinping keeps the status quo. Mao Zedong also had this idea when he used posters, his “little red book,” and encouragement of fanatic groups such as the Red Guard to distribute information and support and maintain government propaganda. There can be a host of reasons why China adopted its censorship policies today, but from observing and analyzing the history of how information was disseminated in China—a foundation, if you will, of how knowledge was taught and received—three pillars to the current foundation are apparent: propaganda, education, and safety. If these three pillars are controlled by the government without a freedom of expression, or even the possibility of an alternate interpretation, then that is censorship. Propaganda here is defined as information provided by the government in a way that not only promotes its superiority but also comes in the form of advertisement such as the propaganda posters of the Mao Era. Education is that which is taught in schools (if at all, considering the Cultural Revolution deemed teachers elitist and schools were shut down) (History.com Staff 2009). Safety here, as we will further investigate in Chapter 6, is maintaining the status quo as a meant to protect citizens. Each pillar will be discussed below.

### *5.1 Propaganda as Censorship*

This author defines propaganda as the government control of how information is disseminated in a country that supports its superiority. The way for any country to disseminate massive amounts of information is through media, such as television, radio, Internet, and even mobile access. To understand censorship in state-controlled countries, one must examine the experience of the press, the only official way to communicate with the outside world. Journalists

are either “self-censoring” because they choose to keep information from the people, or being “censored” by the state or political group which prevents the information from getting to the people (Mužíková 2013). Propaganda is a way to do both. Propaganda can be done for the improvement of the country, but it is or does either improve or harm the nation depending upon how it is carried out. “Good” or “bad” here can mean morally good and bad as well as good and bad with respect to intentions. The Great Leap Forward and the Cultural Revolution are two examples of these intentions and moral decisions.

Mao Zedong’s goal was to improve China from the failing economy, destitution of war, and shame that his country endured since the Opium War, and his Great Leap Forward was a chance to reclaim China from the devastation of the nineteenth century. The Great Leap Forward was a chance to change China for the better. It was Mao’s five-year plan, announced after the fruitful 1957 harvest, to increase agricultural production without realistically taking into account facts such as statistics from the previous years, or the ultimate failure of the Soviet Union’s attempt to collectivize agriculture, upon which they based their system. As Ezra Vogel states in his book *Deng Xiaoping and the Transformation of China*, the Great Leap did mostly the opposite.

“The misguided Great Leap Forward caused devastation throughout China . . . After peasants were organized in huge communes with mess halls so that more of them could work on large poorly planned construction projects or in fields, they could see that those who performed no work were fed as well as the others and they lost any incentive to work . . . statistics compiled by mainland officials estimate that about 16 to 17 million people died from unusual causes” (Vogel 2011, 41)

Vogel writes earlier in the chapter that Mao had created the “One Hundred Flowers” which allowed intellectuals to criticize what the government was doing. The amount and kind of criticism Mao received was far stronger than he expected. Thereafter, Mao branded intellectuals

as rightists, and alienated scientists and innovators, precisely the people he needed to carry China to a better socioeconomic place. Mao began to ignore his officials and silenced loyalists in a display of intolerance of dissent (Vogel 41). Mao's censorship translated into self-censorship by the people. To further support censorship, Mao communicated with the citizens in ways that were noticeable, accessible, and reflected Communist mentality: the use of posters.

Throughout this time, famous propaganda posters littered the streets of China, telling people how to behave and to function in this new society. Because China had a high illiteracy rate with most of the population composed of farmers, the simplest and clearest way for Mao to communicate his policies were through posters in common areas (Huang 2013). The United States' Central Intelligence Agency (CIA) made a documentary film in 1958 displaying propaganda about the Great Leap (CIA 1958). Many shots were of murals painted along long walls in Beijing, depicting achievements in industrialization, arts, education, and sport through images of Chinese citizens also among these were posters demonizing capitalism and the West, ideas completely opposed to the Great Leap. The agent also filmed the making of a movie which he claimed artistically demonstrated the principles of the Great Leap. From an artistic standpoint, the murals resembled Qing Dynasty art, particularly of battlefields but without a landscape or background.

The Cultural Revolution in comparison was a less practical and more philosophical attempt at socioeconomic stability and equality. The intent was to reinstate equality intellectually and socially among the people according to Marxist values, but it created the opposite effect. Intellectuals, such as teachers, were shamed and even attacked by Red Guards made up of youths, possibly former students. Although the campaign was promoted as a way for the Chinese people to unite and foster equality, it was truly because "Mao's own position in



government had weakened . . . Mao gathered a group of radicals . . . to help him . . . reassert his authority” (History.com Staff 2009). Mao wanted to reestablish his strength, ideology, and power within Chinese leadership, so he tightened his control through returning to China’s revolutionary roots. By showing the people why China changed from an imperialist to a Communist state, Mao was able to develop and enforce a strict set of beliefs and behaviors that people followed so religiously that a cult-like retinue grew in its wake. Mao Zedong kept his power because he was able to communicate the rules through the highly-accessible form of propaganda. For Mao, the status quo was maintained because his believers’ radical actions after the Cultural Revolution and Great Leap Forward were so well controlled and communicated that it kept the ruling body intact.

Many Western news outlets, including *Time* (Beech 2016), have made comparisons between Mao Zedong and the current president Xi Jinping. As an example, Xi Jinping’s visits to news stations in March of this year, during which he insisted that the stations maintain their loyalties to the Communist Party, is a clear way to reinforce a journalist’s practice of self-censorship, and even a form of intimidation. In a way, Xi Jinping backed himself into a political corner: his anti-corruption campaign is philosophically nationalistic (if an official is corrupt, the official is disloyal), and, in a time when the economy is slowing for China and there is more civil unrest, Xi is taking conservative steps to secure his control and his idea of status quo. Unfortunately, “In the past few weeks, we have already seen a backlash against increased censorship from independent media [and] employees of state media” (Henochowicz 2016). A less subtle and more modern way to control and censor information is to change leadership within media outlets, such as firing editors, or to defund prominent figures and make examples out of them (Wen 2016). The most recent instance is the cancellation of Ren Zhiqiang’s social

media accounts. The tycoon-cum-political-activist wrote an open and critical post of the Chinese government on his Weibo account which was subsequently closed (Henochowicz; Wen).

Depriving the user's platform for criticism is one way of censoring unwanted criticism; this action is relatively harmless compared to legal action.

The most infamous way to censor a critic, be it journalist or lay-person, is to jail him. In 2015 the Committee to Protect Journalists researched the most censored countries on the planet; the top three included North Korea (Taibi 2015). China, ranked eighth on this list (Committee to Protect Journalists 2015), is reported to have jailed forty-four journalists, the most out of any country researched (Committee to Protect Journalists 2014). It is true that if a post online is considered false by censors, then the post can be removed and the writer can spend three years or more in jail (Risen 2014). The most famous imprisonment is that of Ai Weiwei (1957 - ), who was arrested in 2011 as he tried to board a plane to Hong Kong. Ai was always an outspoken critic of the Chinese regime. During 2011 the government feared of a "jasmine revolution," a parallel reaction to the *Arab Spring*, and began arresting critics and dissidents (Richburg 2011). To justify the arrest, the dissidents, as claimed in Richburg's article, are were charged with "inciting subversion of state power" but were actually arrested because they criticized the state. A modern and more subtle way to censor dissidents without inciting more protest involves inserting false information, disrupting the flow of knowledge, or even stopping it completely. But there are many information outlets with which governments must contend, and a more critical and analytical outlet is the education system.

### *5.2 Education as Censorship*

China's long history records its education systems were government-controlled since the Shang Dynasty (1600 BCE – 1046 BCE) (Hu 1984; Encyclopædia Britannica Online 2015). The

Chinese government had designed, structured, and provided education to its population through a system based in classical study and on a student's ability, to which Confucianism, the Five Classics, and others were added later. The civil service examinations tested a person's knowledge of the Six Arts, the teachings of Confucius, and the Classics, among others, and were open to anyone who wished to participate (Tao 2006). Much like the Standard Aptitude Test in the United States, but even more stressful, this test granted not only a guaranteed job but also prestige for the student and his family. Although the system allowed for poor yet intelligent and capable subjects to rise through the ranks and attain wealth and social influence, such rarely was the case. The imperial structure based the examinations on the Confucian tradition of self-cultivation; "the implied meritocratic ideal, though rarely achieved, inspired the government examination system of China, Korean, and Vietnam, which went to great lengths to prevent cheating, and theoretically selected men according to the breadth and depth of their Confucian learning" (Clark 2004, 15).

Confucianism was the backbone of Chinese tradition for many years, even in its recession during the Han, Song, and Yuan dynasties; it lasted even through the Cultural Revolution to today. After looking at Chinese education in a "big picture" perspective, we can see that the education system provided by the government incorporated culture, philosophy, was structured to receive and work with the structure, and was practically applied to society at large. Education was highly structured, decided by government officials, and reinforced by culture and most aspects of life. This kind of censorship was more innocent in nature because values were placed on culturally-important documents and practices. Ultimately, these examinations determined the structure of the Chinese government, and, although considered "the first standardized tests based on merit," they were also socioeconomically exclusive. Despite the fact that "the examinations

were open to all,” “the need for years of intensive study favored candidates from elite families who could afford to dispense with the labor of their sons and to educate them” (Clark 2004, 26). This exclusivity was the reason why Cixi, the Dowager Empress (1861 – 1908), was forced to cancel them on the eve of the Qing dynasty’s fall.

The culturally-specific, government-controlled education caused China’s isolation from the rest of the world. To be sure, China was far more advanced than other cultures for centuries, but a lack of exposure to other countries or cultures that challenged intellectually or militarily caused China to lag behind technologically and militarily. In comparison, Europe had many countries and cultures situated in close proximity, giving this area of the world the incentive and competition to innovate and generate new ideas. In contrast, China was the “Father of Asia” in the sense that other states paid tribute to it and sent students to learn a Chinese curriculum. This lack of diverse education consequently made China vulnerable to outside powers. The control the government exacted on education isolated China, ended up costing China territories, and threw it into chaos at the beginning of the twentieth century. Chinese Communism viewed this kind of education, especially the imperial examinations, as a representation of the class struggle, and as such an integral part of ancient Chinese tradition, and needed eradication. This was the kind of change for which the Cultural Revolution called.

In the time between the Opium War (1839 – 1860) and the Communist Party’s rise to power (1949)—nearly a century in length—modeling China after a Western-style system was enticing. Since many Western countries were controlling territories in China little by little, leaders in the late Qing Dynasty and Sun Yat-Sen of the Goumingdang, had the idea of reforming education to match the West’s. They thought that system would help the Chinese work with Western countries practically, rather than philosophically as was practiced during the

“century of shame.” The government had to give the Chinese people the information to handle or simply understand the West in order to preserve China and Chinese culture. Cai Yuanpei (1868 – 1940), the first education minister of Sun Yat-Sen’s Republic, proposed that John Dewey’s pragmatism should be the new model for the Chinese education system: each local district would control the education system from a university which would organize all other levels of schooling beneath it (Tao 2006). The Japanese invasion put education reform on hold, and it was in 1953 when education was put into the hands of locals (Tao 2006). The Great Leap forward and the Social Educational Movement sought equal opportunity education but had silenced and alienated many intellectuals (Vogel 2011, 41). Most of the schools established during this time were specialized technical institutes rather than general universities.

Beginning in 1962, a radically new kind of education system was implemented: the Socialist education movement. In his article *Recalling Bitterness*, Guo Wu writes about the importance of collective unconscious in Communist society (Wu 2014, 8). This education movement had to come from the “bottom up” or what we call a “grassroots movement” today. It was designed to have peasants and workers tell their life stories and to show their struggle for class equality in a way that they were never able to do before. The stories were distributed locally, in either written or oral format, the latter in meetings. Any “rich peasant” or anyone in a higher position before the Revolution refrained from telling their stories at these meetings (Wu 2014, 252). Mao Zedong went as far as to re-write history books, or the *Four Histories*, and hired famous historians Liu Danian and Li Shu among others to alter to suit Communist philosophy. The histories they were commissioned to write focused workers’ and factory history, the topic of which they knew little. Other writers were brought in to write fictional stories based on facts; they tended to demonize capitalism. Another method of “recalling bitterness” which

occurred in the classroom was to eat a “recalling-bitterness meal” of low-quality ingredients, and sometimes made with mud (Wu 2014, 265).

The Cultural Revolution in 1966 made this situation no better. Education as they had known it had been transformed into either a factory for political and social struggle or eradicated. The Communist Party Central Committee wanted the students to focus on the revolution and to contribute to the society at large. Eventually this policy hurt teachers because any thought or idea that was different from the Party-defined system was defamed and came under suspicion (Tao 2006). Without intellectual stimulation, Chinese society as a whole suffered economic effects. Creativity is an important factor in innovation, and Deng Xiaoping had made strides to change technological development in China to create a sustainable model (Vogel 2011, 220-228). He wanted to reform Chinese curricula, and he knew that he would need the help of Western powers to do it much in the way “that Japan, South Korea, and Taiwan had relied heavily on U.S. science, technology, and education to achieve modernization” (Vogel, 312). Even though China attempted to reform its system, it ended up creating a model similar to what Cai had suggested in 1916 a more Western-based curriculum.

Today, Chinese schools heavily value three subjects: English, math, and Chinese. The government provides curricula based on textbooks developed by the Ministry of Education (MOE) in China (Ministry of Education of The People’s Republic of China 2013). The difference is that the MOE recognizes the importance of opening to other countries and cultures, as per Deng Xiaoping’s policies at the beginning of the 1980s. Because of Deng’s recognition that China needed to learn from other developed countries, he insisted upon establishing cooperation between China and foreign companies, organizations, or governments; on inviting businesses to develop in China; and on sending students abroad to study and return with the

knowledge they learned. From these policies China has adopted many models of industrialization, education, and especially standardized testing. Despite the abolishment of the ancient imperial exams (which focused mostly on an “eight legged” [Clark 2004, 45] essay system), China has recently adopted entrance exams. The infamous Gaokao entrance exam began with the idea, unlike the old system, that more students had access to universities (Chen 2013). Today the exams include English sections as well as Chinese and math.

Education through China’s history has shifted from intrinsic cultural appreciation or patriotism, to a political agenda, to a political and economic agenda. With regard to the teaching of English as a foreign language in Chinese schools, the agenda is largely financial. English is today’s business language as Chinese is becoming its equal, but some critics have argued that the way in which the MOE structures the curriculum is a detriment to English language education if “the political agenda prevails over the long-term economic and education agenda regardless of the global tide” (Chang 2006). Censorship in any form of education will cause some educational harm, as some acts in the United States have done (Fuglei 2014). Many Chinese laws and policies on Internet censorship for example are as a result of the “protection of minors” from unsavory topics such as pornography (IOSCPRC 2010). Other unsavory topics, such as questioning or analysis of the Chinese government, are also subjects blocked on Chinese Internet.

“More information will glean more ideas and ‘may actually increase incidents of censorship. Literacy assumes the power of texts and encourages exposure to competing ideas and beliefs. Critical thinking implies questioning, the analysis and evaluation of those beliefs to come to a personal judgment that empowers young people to take ownership . . . and control their own intellectual and moral lives” (Vandergraft 1997).

### 5.3 *Censorship as Safety*

Censorship can be a block of information or a distribution of false information (Schmid 2011). It can do harm and it can shield, and it can be implemented with the intention of safeguarding a country as well as protecting political power. The less the public has access to information, especially government activities, the less likely the public will react to it. Lawyers and doctors censor themselves for the sake of their patients' welfare, so why not governments? A lack of information or controlled information access by a government could also stifle economic growth, as China has seen during the Great Leap and the Cultural Revolution. A good case study of protective censorship use is to look at the current Chinese administration.

Xi Jinping's anti-corruption and patriotism methods grow more authoritarian as the economy in China stalls in growth. As a consequence, in speeches and public visits he reiterates that "the media should fully identify with the party's agenda—or as he put it, be 'surnamed "Party"'—and that this standard should apply to the full spectrum of media content, from party-run outlets and commercial newspapers to advertising and entertainment" (Cook 2016).

Censorship is a way of controlling the population to maintain the safety and status quo of the nation. *The Internet in China* embodies this idea in its reasoning that the Internet is censored for the sake of minors' protection. Some countries, like the U.S., have debated such policies and in some cases, such as the Children's Internet Protection Act (CIPA), implemented them. In the same vein, censorship can apply to blocking terrorists and their hateful ideas or even recruitment on social media sites. This example identifies an important philosophical and political idea that International Relations Theory and International Security Studies have been discussing since Thucydides: freedom versus security which will be discussed in Chapter 6.



#### 5.4 *The Effects of Censorship on Economy*

Is it wise to censor the Internet? We read in the last chapter that the Chinese government has written in the *White Papers* and other documents that the Internet is to be used for the sake of education and the building of the economy, and, as the largest source of information and connection on this planet, it would be in China's best interest to be as open as possible to this source. However, censorship deemed as "porn" or other unsightly topics ends up restricting more than just those incidents, such as an entire economy. If China decides to shut itself off to some of the most popular social media sites, such as Twitter and Facebook, it also decides to shut itself off from a giant customer base. In addition, China isolates itself from other countries which could be allies and could offer better economic ventures. On the one hand, China maintains social stability by controlling the flow of information within the country, but on the other hand it is sacrificing access to valuable economic partnerships. The censorship has grown to be such a problem that "United States trade officials have for the first time added China's system . . . known as the Great Firewall . . . to an annual list of trade impediments" (Mozur, 2016). Because of a restriction of the world's largest sources of information, the Chinese government has made it difficult for technological development or informationization which the *National Security* and *Military Strategy* policies have made top priority (IOSCPRC 2011, 2015). Now that there have been reports of a slowing Chinese economy (The Associated Press 2016), it would stand to reason that Xi Jinping would do more to open up the economy. Instead, Xi Jinping has sought to control more media outlets to the point where his methods are labeled "authoritarian."

Of course the economic slow-down has caused "considerable uncertainty in financial markets and has led to sharp falls in commodity prices" (BBC Staff 2016), and for a country that

has relied on industry and manufacturing, that very idea can significantly affect its markets. No matter how much Xi Jinping tries to control either the economy or the Internet, there is always a human factor for which he cannot account. The international economy is like an organism—much in the same way computers, which are built by humans, are similar to the human brain—meaning that it will grow and decline and change according to the environment (Peltoniemi 2004). The Chinese government may inject it with stimulus money, or Xi Jinping could ensure that the media reports are in favor of what the Chinese government is doing, but that can only fix doubts or job losses for so long.

Whether or not Internet censorship can actually affect an economy has been researched, but as of yet its effect is unconfirmed, and by its “architecture [the Internet] makes censorship [difficult to test] at the core” (Zhao 2008). The Internet is a network of an overwhelming amount of information, which is great for business and bad for censorship. To keep order in China, or even to keep it secure, the government has implemented policies that filter and block sites that block both unsightly content and business opportunities alike. In the next chapter, Internet censorship will be explored from a security perspective, and whether or not the sake of informational, Internet freedom should be sacrificed for the sake of security.

## **Chapter 6: Freedom versus Security, or Freedom versus Privacy?**

This chapter will explore the IR Theory and ISS theories surrounding, freedom, security, and privacy in a state. First an examination of security will look at the reasons a state would secure itself and what from. Then how digital technology changed these theories will be identified and analyzed. Finally, contemporary Chinese cybersecurity policy will be discussed in light of Xi Jinping's new agenda on tightening the government's control on Chinese media outlets. To begin, what is the main reason today for tightening state security? Terrorism of the late twentieth century has changed freedom versus security as we understand it today, especially with new technological innovations such as the Internet. The change in perception has affected the ideas of what government, nation, state and what terrorism mean. Terrorism has morphed into both a physical and digital threat and has forced the world to rethink the very idea of it as well. The term "terrorism" itself is an ambiguous idea, and so far there has been no universal agreement on its definition whether it be in law or academia (Williamson 2009; Schmid 2011). Myra Williamson's definition of terrorism includes the idea that terrorism today is an attack of a citizen on its government, whereas historically it was a government's attack on its people (Williamson 2009). To paraphrase David J. Whittaker's definition: terrorism is unlawful, calculated use of force for a political, religious, or ideological cause or to instill change that targets innocent people and causes them to be fearful or harms them (Whittaker 2007).

Two aspects of terrorism that are in both definitions is that they are violent acts which cause fear. Whether the violent acts which cause fear are for political or ideological reasons is another matter entirely, and the matter causes the most debate, a debate that defines the terrorists as either right or wrong. Unfortunately, no one knows the reason or reasons for the violence until the violence occurs, which leaves authorities grappling for ways to stay ahead of the

attackers. The plot to cause fear would require the greatest secrecy and privacy, as was demonstrated in the September 11th attacks (Pais 2004), and that situation brought with it the question of privacy. If authorities had access to private phone records, emails, or any other number of communication media, could the United States have been protected? In this instance, the United States wanted to protect its people, but is that what it is truly protecting? What is the most important thing to protect in a nation/state/government? Does the state protect itself for the sake of the people or for itself? When the threat of the safety, stability, and status quo of the state is presented, should the people of such a state make sacrifices for its preservation?

For a better understanding of this issue, a brief look at International Security Studies (ISS) is worthwhile. ISS began focusing on state-centric, military defense that were influenced by a pre-Cold War understanding of security and International Relations. Drawing from Buzan and Hansen's book *The Evolution of International Security Studies*, security has changed drastically in the last century. Once the Cold War ended, strategies on how to deal with outside threats to a state or government were changed. Just like digital technology changed the arena of security in the new millennium, the introduction of weapons of mass destruction (WMD) changed national and international security after World War II. A physical object (such as a bomb, or a hill or river) could mean the difference between whether a state survived or was decimated, and that concept governed ISS for centuries. The first writers on ISS, such as Thucydides, thought in "realistic" terms, meaning that they were suspicious of other states and were concerned with power, its achievement, and preservation within the state. To Hobbes, the ultimate goal was to secure the state which was the "referent" object, or that which needed to be protected so that the people would also be protected. The state was the primary provider and stabilizer for the people. It was the American and French Revolutions which added the elements of nationalism,

patriotism, and universal-rights, turning the protection of the state as a whole, collective entity, to identifying the safety and security of an individual (Buzan, 30). It is this idea that the new invention of the Internet has enhanced and put “center stage” in the current security of the world (Human Security Unit 2016).

Technology has brought a new dimension to the lives of those who can afford it, some of whose—even most of whose—lives exists digitally on the Internet. Before the digital age, terrorism was limited to the physical world, but because peoples’ identities have shifted to the digital sphere, a whole new wave of terrorism can be conducted through computers, smart phones, and other devices. Terrorists can use Western social media to recruit and to threaten, and outlets such as Google and Facebook will allow them to do so because of freedom of speech. If the outlets censor certain words, topics, or even accounts, then they set a precedent of “acceptable” censorship and any repressive government could use it as a reason to censor its own media; the outlet could be seen as a tool of the government. If the outlet keeps its platform open to all, then terrorists can use it as a soapbox or recruitment station (Menn 2015). This idea is only one side to this problem. Edward Snowden leaked that the National Security Agency (NSA) collected information on all Verizon customers in the United States without a warrant (Greenwald 2013). Why the NSA chose to spy on Americans for three months is unclear, but the unadulterated access to metadata—knowing who called whom, for how long, and where—could reveal patterns of, say, behavior exhibited by terrorists. While there are still parts of the world which need physical security, there is a growing need for privacy as well.

The Internet has created a digital existence for netizens, as more people choose to keep personal data, such as resumes or personal information, on computers or phones. With so much of our lives on machines, in cyberspace, it becomes imperative to protect our information. If a

government is the referent object, and its power is used to protect the people, then the people's privacy is less important than that of the government. Or, if the government is the referent object, then it would be imperative to protect this digital organism to which it and its people are attached. However, if the government respects the people's privacy, the status quo is maintained, but it may leave the state vulnerable to attack.

Another section of I.R. Theory, human security offers the same idea, but the *individual* is the referent object, and not the state. According to Buzan and Hansen, not only is the individual the referent object, but also his well-being, such as socioeconomic status, or his integrity (Buzan 2013, 36). For as complex as a world this is, one that grows more complex and more multi-dimensional with the introduction of the Internet, is the idea of human security. The concept of Human Security can easily be applied to China since Xi Jinping now faces privacy issues that have arisen from the current socioeconomic situation which in turn has been affected by cybersecurity policy. Xi Jinping's countrymen number in the billions: he has little choice but to take their security into account. Chinese political philosophy (i.e. communism) and ideology, as well as national policy, is people-centric. China is to build its wealth on peaceful social and economic development for not only the sake of China but also for the sake of harmonizing with the rest of the world, but censorship further isolates China.

China currently uses censorship and promotes it by saying it protects the people, yet this policy has caused it to suffer economically, a direct violation of its national security policy to promote peaceful economic and social development. Increasing censorship also has caused high-profile controversies such as Ren Zhiqiang's exile from social media accounts at the hands of the Cyberspace Administration of China (Chin 2016). According to the *Constitution*, Ren Zhiqiang had the right to say what he wanted to say, but, according to *The Internet in China*, it

subverted state power and disrupted order, which is “illegal” and “had a vile influence on society” (Kuhn 2016). He had the freedom to say what he wanted, but what he wrote, according to the Chinese government, was a threat to the society, and, ultimately, to the government itself. The government here is looking to secure the whole of the population, the whole of the nation, at the expense of the individual’s freedom of speech.

Another side to this coin—or perhaps now a die—is that censorship also secures China from outside influence. *The Global Times*, a Chinese government-run English newspaper, wrote that the Great Firewall only blocks a “tiny number of foreign websites,” of which it named *The New York Times* and *The Economist*, and continued to say that it takes a sophisticated system to block not only these but also “harmful content” (The Global Times Staff 2016). This quotation identifies the idea that China has taken great pains to block only certain websites while allowing the flow of much more important sites that would promote the Chinese economy. The Internet is a Western invention and, to this writer, the Internet is governed by Western rules and ideology, something China does not want. This situation then raises the question: is less information is safer and more secure than more information and having access following to more information?

With any kind of information, whether as innocent as a fact or as dangerous as a rumor, “a little knowledge is a dangerous thing,” (McGraw-Hill 2002). Since the country has experienced instability, not only from foreign powers but also from protesters, China has sought to keep status quo through “realistic” (in International Relations Theory terms), almost draconian measures, such as disappearing booksellers who were to sell copies of *Xi Jinping and His Lovers* (习近平与他的情人们) (Liu 2016). In short, China allows freedom of speech if it is in accordance with the law, i.e. maintains status quo, but how long can China continue to censor its Internet in any sphere before it suffers economically and loses power?

## Chapter 7: Conclusion

China as a culture has existed for centuries; China as a state has existed for perhaps fifty years, even less if one were to begin when Deng Xiaoping opened China to the West. Years of isolation during Mao's reign stunted China's social, economic, and political growth within the international community. Although it has the second largest economy in the world, the United Nations still classifies China as a developing country. Even though China has "opened," what information about China is limited? The news that does come from China is reports on anti-corruption or conflict around censorship issues, at least those articles that are written in English. China's education squelches the potential for creativity and invention. Because of the educational structure and censorship of information, a disconnect between Chinese citizens and the outside world has formed. The focus on memorization and regurgitating information reduces the potential for analytical thought, but increases the potential for security, which China needs. Censorship of seemingly unsavory topics controls the pool of information, and can drive a population toward the same opinion, thus creating social stability.

China's recent history has been fraught with challenges including war, famine, and fear. It was able to emerge from its self-imposed-isolation only because of one man's vision. Deng Xiaoping's biography and memoir is banned in China, unless it is censored or redacted (Burry 2013), but he is thought of either as a hero or the father of modern-government-corruption (Tong 2015). On the one hand Deng opened China to new possibilities in innovation that helped improve its economy, but on the other, the way in which he implemented the change allowed corruption to blossom. Xi Jinping has tried to control the corruption by controlling the media and by reminding his people that China is part of one family, and must work together, not for the individual. In so doing, his methods have caused self-censorship within the media. Because of



Xi Jinping's compelling display of Party loyalty and because of China's contemporary history, Western democratic states see these measures as suppressing freedom of speech.

Many Western states consider censorship on any level to be a violation of fundamental human rights, or plain evil, but if governments share with their peoples all information to which they are privileged, is that safe? Now that information can pass from one side of the planet to the other in an instant, the control of intelligence has become more important than a country's physical strategic position. The *Arab Spring* demonstrated the strength of and ability for information and communication to change the political climate of a country, even overthrow a ruler. The Internet has all but nullified physical borders and forced together cultures that would never have met had it not existed. It has given a louder, more accessible voice to Internet users, as well as access to more people, their resources, their machines, and their knowledge base. Today, a government's Internet security affects its national security, and is only as strong as its weakest link. The Chinese government sees the Internet not only as a weapon for gathering intelligence or for cyberattacks but also as a tool for supporting unity and political agenda, one which could backfire. Originally, the Internet was used as a tool to increase communication between and among different Western branches of the military and intelligence agencies, but has since developed other uses to suit the needs of governments and consumers alike. When the Internet came into commercial/civilian use, the sharing of information was predicated on the principles of Western democracy. Information on the Internet can be correct, incorrect, once top secret or public, and once it is available it can exist indefinitely. Thus, actively removing information on the Internet appears to be either a suppression of free speech or a shady redaction in a place meant for sharing information.

Because the Internet was created in the West, its form follows Western ideology. Western ideology at its core supports the idea that no idea should be silenced, and all who use it see it as a place to share information. In the Western perspective, information on the Internet, whether true or false, or classified or not, is to remain uncensored. If a leak occurred that was the fault of that organization's security, or lack thereof. The United States express that right to freedom of speech no matter how volatile a voice or perspective or information arguably allows unfettered information to flow on the internet. Such is the case of the Westboro Baptist church which is allowed to continually and openly condemn the United States, to protest funerals of dead soldiers, and to preach that their perspective as the only true perspective, without censorship unless circumscribed by the courts (Certiorari to the United States Court of Appeals the Fourth Circuit 2011). The idea that no perspective should be silenced stems from the Western ideal that all ideas matter, and that silencing one sets a precedent for silencing others, that there is a danger of marginalizing unpopular opinions. Another, more pragmatic danger is that a lack of information prevents innovation, practicality, or education. With more access to more ideas there is a wider base of information from which new ideas, opinions, and technologies can be formed. Not all cultures share these ideas, and, in the case of China, the idea of information or informationization takes on a businesslike, not philosophical, role.

Informationization, says the Chinese *White Papers on National Defense and Military Strategy* policies, is most important for social and economic development, yet the Chinese government censors the most easily accessible, pervasive, and largest source of information on our planet from which new ideas and innovations occur. Of course Chinese censorship extends to those sites that which have subverted the Chinese government because the mere act of subversion is illegal. At the same time, newspapers, email services, and large companies which

are important sources of both business capital, and information, are also censored when information they disseminate is deemed by the Chinese government to be subversive or wrong. What information *is* acceptable under government standards? So far, no policy has defined what is authorized: this ambiguity gives the government more leeway and control over the Internet. Xi Jinping has very publicly reminded his listeners that the Party is the patriarch of the family that is China. He has gone to television stations and newspapers to demonstrate this, which perfectly represents how much power the Chinese government can have and how fragile the government can be if media disseminated just the right information that could lead to *Jasmine Revolution*.

The answer to the first research question about what China's cybersecurity policies are and how they are implemented is as follows. The policies state that the Internet is to be used for educational, economic, and social development. That which is censored by the government is irrelevant to education, economy, or society. Any censorship that takes place is because the information disseminated online is either wrong or undermines the stability of the government. Of course the policies do not define precisely how the policies will be implemented, save the few examples deemed censored, such as "porn." The *White Papers on National Defense, Military Strategy*, and *Peaceful Development* all treat the Internet as a tool to help China develop, even in cooperation with the rest of the world. The only limit on the Internet has is when it conflicts with Chinese law or tries to destabilize national security.

With this in mind, the second research question asks what are the effects of Chinese cybersecurity on Chinese economy, society, and foreign policy? There is no conclusive evidence to suggest that China's economy suffers due to its Internet security measures; in fact, we see a slow-down only in recent months. Aside from a snail-paced bandwidth that may add up over

time (Schuman 2011), the only inhibiting quality is that of reporting to the outside world.

Chinese citizens can use Virtual Private Networks (VPN) or travel to the United States to access sites like Google or Facebook; the cybersecurity policies within the *White Papers* do not limit Chinese society necessarily. Chinese citizens can still research Western businesses to see new technologies and new ideas, and bring them into China or build off them if possible.

Cybersecurity policy encourages cooperation with other nations to grow economically and encourage world peace and stability. By looking at the *White Papers* only, Chinese cybersecurity policy actually does not restrict Chinese citizens from information they wish to gather for development. Those who are critical of the government are asked to do so anonymously and privately (Wertime 2015) because if government corruption were made public, that would mean undermining the government's credibility. We heard of the Bo Xilai scandal and of Xi Jinping's efforts to eradicate corruption, but the specifics largely emphasize the fact that the person found to be corrupt was dismissed and the job was done. This, by no means helps the argument that unpopular opinion of the government should be censored. In fact, censoring critical thought online has upset foreign policy.

Other governments perceive Chinese censorship immediately as a silencing of free speech and call Xi Jinping's administration oppressive and even authoritarian. It is true that Xi Jinping has reminded Chinese media that its family name is "the Party," and that appears to Western countries as authoritarian. The cultural difference, however, is that Western countries view freedom of speech as being able to say whatever one wants without repercussions, while China limits that freedom of speech by alleging requiring truth and freedom from harm. The West would see censorship of certain sites and posts to prevent certain ideas from reaching other Chinese citizens or the outside world, and, arguably, as a halt in progress. The question then

becomes can Chinese society progress with its current cybersecurity policy or will it need less censorship to continue growing? How can one progress without seeing a starting point or innovate without seeing what needs exist? The lack of information to make *informed* decisions can hinder the ability to think critically and thus innovate. There is, so far, no evidence that China is hacked for its technological information or ingenuity, and part of the reason for this is anemic information about China coming from within China. This very idea is exemplified in the charts tracking cyber-attacks above.

There is insufficient evidence to suggest that China is cyber-attacked as much as other governments are. The evidence of actual attacks was through Western media outlets. Even still, the number of reports was low in comparison to other countries who blamed China for their attacks. Out-of-date information on cyber-attacks are available through such organizations as the United States Department of Homeland Security, but that data lacks specifics, such as the source or victim of the scan. There is also insufficient data from official sources on cyber-attacks in general because such sensitive data would be considered an accusation, thus volatile for foreign relations. It would be unwise to suggest that China should publicize authors, dates, and times for cyber-attacks on its systems. However, if it were to divulge that information as often as other governments do, then China would look less like an instigator and more like the other governments who fell victim to attacks in the eyes of Western media. There is also insufficient data to show the specifics of whom China is scanning, when, and from where. While cybersecurity data can be a threat to national or international security and is a volatile foreign policy issue, specific data collected on who scanned whom would obviously reveal reasons why a government would take steps to spy on others. In China's case the data would demonstrate what economic, social, or technological needs need fulfilling and why. More research needs to

be done on whom, how, and how many times China has been cyber-attacked by other governments or even private entities, and vice versa. More studies on Chinese censorship and how it affects the Chinese economy is also important to determine how China moves forward in its economic, social, and foreign relations development.

Chinese economy has blossomed in recent years despite the givens of its cybersecurity policy and censorship. Chinese society has benefitted from economic growth, and now has more billionaires than the United States despite censorship (Frank 2016). What cybersecurity policy has actually affected is China's foreign relations. China wishes to develop on its own and in its own way without the West interfering, but we see a growing number of accusations that China has appropriated Western intellectual property. Looking at China's history one could argue that China has managed to keep relatively stable foreign relations. However, in light of draconian methods of censorship, the West is understandably concerned. Xi Jinping's visits to bolster unity and Party support are a reminder that the government is still the "referent object" that needs protection in order to secure the Chinese people. If Xi Jinping continues to assert Party dominance over the flow of information, he is denying his citizens the ability to learn and to grow with the rest of the world and forcing his government to copy innovation rather than generate it. At the same time he will jeopardize China's foreign relations. Chinese foreign and national policy is about informationization, development, growth, and working harmoniously with the rest of the world, but what the government is doing with cybersecurity promotes just the opposite. More research is needed to discover whether or not censorship truly squelches economic growth. With more data and time, it can be determined whether censorship will help or harm the economy or society; nevertheless, it can be said already that censorship is affecting China's foreign relations.

With the information at hand, this author predicts that if Xi Jinping continues to tighten censorship on the Internet, Western countries will continue to view him as authoritarian, thus impacting foreign relations. Claims reported by Chinese netizens that posts were removed or topics generated by Chinese citizens online blocked by *The Great Firewall* will ring in the ears of Western listeners as a violation of freedom of speech. Xi Jinping must reconsider a second opening to the West for the sake of peaceful and cooperative development between China and Western countries. Chinese cybersecurity allows for enough economic and social development to the point where it balances freedom of Chinese citizens and security of the state. For the sake of peaceful and harmonious cooperation with other countries as is stated in the *White Papers*, the Chinese government should communicate more, or make news more open.

Understandably, China wants to move forward with its policies in its own way and without Western interference, but censoring more information makes China look more like North Korea to the West and can erode foreign relations. After this look at Chinese cybersecurity, it is less restrictive than previously thought, and the real problem affecting foreign relations is actually the export of information from China. Xi Jinping's administration has to walk a fine line to preserve the freedom and security of China while communicating with the West. However, as long as China's economy continues to do well, there is no reason to change censorship policies. It would be wise for China to consider opening more to the West and to attempt more collaboration to achieve a mutual understanding.

## Bibliography

- “admin.” 2015. “Millions of Cyber-attacks Happening Each Day.” *Firtus*.  
<https://cybermap.kaspersky.com/>.
- 107th Congress. 2002. *Public Law 107 – 296 107th Congress An Act ( a ) S H O R T T I T L E .—  
This Act May Be Cited as the ‘ ‘ Homeland. Public Law*. Washington D.C.: Congress.
- A +E Networks. 2010. Inside North Korea. The New York Times Company, 2010  
NYTimes.com Video Collection Opposing Viewpoints in Context, EBSCOhost. Accessed  
April 27, 2016. <https://www.youtube.com/watch?v=mxLBywKrTf4>
- Altenberger, Lisa-Maria. 2014. “Likes for the Leader: North Korea’s Use of the Internet and  
Social Media.” *Asian Politics & Policy* 6 (4). Wiley-Blackwell: 631–34.
- American Civil Liberties Union et al., v. Janet Reno, Attorney General of the United States,  
American Library Association, Inc., et al., v. United States Department of Justice et al., Nos.  
CIV. A. 96-963, CIV. A. 96-1458, (United States District Court, E.D. Pennsylvania 1996).
- Anderson, Nate. 2010. “Hillary Clinton Slams ‘Information Curtain’ of Censorship.” *Ars  
Technica*. Accessed April 27, 2016. [http://arstechnica.com/tech-policy/2010/01/hillary-clinton-slams-information-curtain-of-censorship/?tid=a\\_inl](http://arstechnica.com/tech-policy/2010/01/hillary-clinton-slams-information-curtain-of-censorship/?tid=a_inl).
- Asian Development Bank. 2014. *Innovative Asia: Advancing the Knowledge-Based Economy -  
The Next Policy Agenda*. Mandaluyong City: Asian Development Bank.
- Bagby, John. 2012. “IST432Team4 - China and North Korea.” *Penn State University Online*.  
Accessed April 27, 2016.  
<https://faculty.ist.psu.edu/bagby/432Spring12/T4/pages/china.html>.
- Bali, V. 2007. “Data Privacy, Data Piracy: Can India Provide Adequate Protection for  
Electronically Transferred Data.” *Temp. Int’l & Comp. LJ* 21: 103. Accessed March 13,  
2016. [http://heinonlinebackup.com/hol-cgi-bin/get\\_pdf.cgi?handle=hein.journals/tclj21&section=6](http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/tclj21&section=6).
- Barboza, David. 2008. “In Chinese Factories, Lost Fingers and Low Pay - The New York Times.”  
*The New York Times*. Accessed April 27, 2016.  
<http://www.nytimes.com/2008/01/05/business/worldbusiness/05sweatshop.html>.
- Bartlett, Tom, and Karin Fischer. 2011. “The China Conundrum.” *The New York Times*,  
November 3. Accessed March 13, 2016.  
<http://www.nytimes.com/2011/11/06/education/edlife/the-china-conundrum.html>.
- BBC Staff. 2016. “Moody’s Cuts China Outlook to Negative.” *BBC News*. Accessed April 3,  
2016. <http://www.bbc.com/news/business-35704022>.



- . 2015. “Cuba Profile - Timeline.” *BBC News*. Accessed March 13, 2016. <http://www.bbc.com/news/world-latin-america-19576144>.
- Beech, Hannah. 2016. “China’s Chairman Builds a Cult of Personality.” *TIME*. Accessed April 27, 2016. <http://time.com/magazine/south-pacific/4278204/april-11th-2016-vol-187-no-13-asia-europe-middle-east-and-africa-south>
- Bershidsky, Leonid. 2014. “2015: The Year of the Putin Dictatorship.” *Bloomberg View*. Accessed April 27, 2016. <http://www.bloombergtview.com/articles/2014-12-29/2015-the-year-of-the-putin-dictatorship>.
- Bilton, Richard. 2014. “Apple ‘Failing to Protect Chinese Factory Workers’ - BBC News.” *BBC News*. Accessed April 27, 2016. <http://www.bbc.com/news/business-30532463>.
- Bol, Peter K. 2015. “China and the Modern World.” *Harvard edX Online*. Accessed May 4, 2016. <https://www.edx.org/xseries/china-modern-world>.
- Burry, Liz. 2013. “Author Bows to Chinese Censorship of His Deng Xiaoping Biography.” *The Guardian*. Accessed April 27, 2016. <http://www.theguardian.com/books/2013/oct/22/author-chinese-censorship-den-xiaoping-biography>.
- Burton, Dan, Gary L Ackerman, New York, Brad Sherman, Russ Carnahan, Connie Mack, Gerald E Connolly, et al. 2011. “Communist Chinese Cyber – Attacks , Cyber – Espionage and Theft of American Technology.”
- Buzan, Barry, and Lene Hansen. 2009. *The Evolution of International Security Studies*. Cambridge [U.K.] ; New York, N.Y. : Cambridge University Press, 2009.
- Carsten, Paul. 2015. “China’s Internet Population Hits 649 Million, 86 Percent on Phones | Reuters.” *Reuters*. Accessed April 27, 2016. <http://www.reuters.com/article/us-china-internet-idUSKBN0L713L20150203>.
- Center for Strategic and International Studies. 2010. “Significant Cyber Incidents Since 2006.” No. 1. June 2007: 2006–11.
- Center for Strategic and International Studies. 2014. “Significant Cyber Incidents Since 2006.” *Center for Strategic and International Studies*, 2012. Accessed April 27, 2016. [http://csis.org/files/publication/140310\\_Significant\\_Cyber\\_Incidents\\_Since\\_2006.pdf](http://csis.org/files/publication/140310_Significant_Cyber_Incidents_Since_2006.pdf).
- Central Intelligence Agency of the United States of America. 1958. *China’s Great Leap Forward | 1958 | History of China Under Mao Zedong | CIA Documentary Film*. China: The Best Film Archives. Accessed April 3, 2016. [https://www.youtube.com/watch?v=ro4X\\_fVvDR8](https://www.youtube.com/watch?v=ro4X_fVvDR8).

- Certiorari to the United States Court of Appeals the Fourth Circuit. 2013. Supreme Court of the United States 1–36.
- Chang, Junyue. 2006. “Globalization and English in Chinese Higher Education.” *World Englishes* 25 (3-4): 513–25. doi:10.1111/j.1467-971X.2006.00484.x.
- Chen, Gang, Emily Dimmitt, and Allie Schexnayder. 2015. “GAOKAO 高考.” In . Oklahoma City: Oklahoma City University. Accessed April 27, 2016. <http://www.okcu.edu/students/ocureads/previous/2009/>.
- Chen, Hanqing. 2014. “A Recent History of China’s Cyber-attacks on the United States - Pacific Standard.” *Pacific Standard*. Accessed March 13, 2016. <http://www.psmag.com/nature-and-technology/chinas-cyber-attacks-united-states-89919>.
- Chen, Theodore Hsi-en. 2016. “Education and Propaganda in Communist China.” *American Academy of Political and Social Science* 277: 135–45.
- Chien, Eric, and Gavin O’Gorman. 2011. “The Nitro Attacks: Stealing Secrets from the Chemical Industry,” 1–8. Accessed April 27, 2016. [https://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/the\\_nitro\\_attacks.pdf](https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_nitro_attacks.pdf).
- Chin, Josh. 2016. “China Muzzles Outspoken Businessman Ren Zhiqiang on Social Media.” *Wall Street Journal*. Accessed April 24, 2016. <http://www.wsj.com/articles/china-muzzles-outspoken-businessman-ren-zhiqiang-on-social-media-1456712781>.
- China Law Translate Staff. 2014. “SPC, SPP, MPS on Violations of Citizens’ Personal Information.” *China Law*. Accessed March 13, 2016. <http://chinalawtranslate.com/spc-spp-mps-on-violations-of-citizens-personal-information/?lang=en>.
- China Law Translate Staff. 2015. “China Law Translate | 网络安全法（草案）.” *China Law Translate*. Accessed February 21, 2016. <http://chinalawtranslate.com/cybersecuritydraft/?lang=en>.
- China Law Translate Staff. 2014. “SPC, SPP MPS Procedural Rules for Internet Crimes.” *China Law Translate*. Accessed February 21, 2016. <http://chinalawtranslate.com/spc-spp-mps-procedural-rules-for-Internet-crimes/?lang=en>.
- China Law Translate Staff. 2015. “China Law Translate | 网络安全法（草案）.” *China Law Translate*. Accessed February 21, 2016. <http://chinalawtranslate.com/cybersecuritydraft/>.
- Cienciala, Anna M. 1999. “COMMUNIST NATIONS SINCE 1917.” *Web.ku.edu*. Accessed February 21, 2016. <http://acienciala.faculty.ku.edu/communistnationssince1917/>.
- Clark, Conrad Schirokauer Donald N. 2004. *Modern East Asia: A Brief History*. Belmont: Thomson/Wadsworth.

- Committee to Protect Journalists. 2015. "10 Most Censored Countries." *Committee to Protect Journalists Online*. Accessed March 13, 2016. <https://cpj.org/2015/04/10-most-censored-countries.php>.
- . 2014. "2014 Prison Census: 221 Journalists Jailed Worldwide." *Committee to Protect Journalists Online*. Accessed March 13, 2016. <https://cpj.org/imprisoned/2014.php>.
- Congress, United States. 2011. "U.S.C. Title 15 - COMMERCE AND TRADE." *Government Printing Office*. Accessed February 21, 2016. <https://www.gpo.gov/fdsys/pkg/USCODE-2011-title15/html/USCODE-2011-title15-chap7-sec271.htm>.
- Constitute Project. 2013. "China's Constitution of 1982." *Constitute Project*.
- Cook, Sarah. 2016. "The Gamble Behind Xi Jinping's More Restrictive Media Policy." *The Diplomat*. Accessed April 24, 2016. <http://thediplomat.com/2016/03/the-gamble-behind-xi-jinpings-more-restrictive-media-policy/>.
- Couts, Andrew. 2011. "China Calls Google a 'Political Tool' after Hacking Accusations." *Digital Trends*. Accessed April 24, 2016. <http://www.digitaltrends.com/computing/china-calls-google-a-political-tool-after-hacking-accusations/>.
- Cronau, Peter, and Andrew Fowler. 2013. "HACKED!" Accessed November 19, 2015. <http://www.abc.net.au/4corners/stories/2013/05/27/3766576.htm>.
- Demographic Internet Staff US Census Bureau. 2016. "International Programs, Country Rank." *The United States Census Bureau*. Accessed February 21, 2016. <https://www.census.gov/population/international/data/countryrank/rank.php>.
- Detterbeck, Klaus. 2014. "Innovation Policies in European Regions." *Politologický Časopis - Czech Journal of Political Science* 21 (2): 85–93. doi:10.5817/PC2014-2-85.
- Encyclopædia Britannica Online, s. v. "Shang dynasty." Accessed April 20, 2016, <https://www.britannica.com/topic/Shang-dynasty>.
- Evans, Stephan. 2016. "Why Is China's Growth Slowing?" *BBC News*. Accessed April 24, 2016. <http://www.bbc.com/news/business-35348202>.
- Fan, Maureen. 2006. "China's Party Leadership Declares New Priority: 'Harmonious Society.'" *The Washington Post*, October 12. Accessed April 24, 2016. [http://www.washingtonpost.com/wp-dyn/content/article/2006/10/11/AR2006101101610\\_2.html](http://www.washingtonpost.com/wp-dyn/content/article/2006/10/11/AR2006101101610_2.html).
- Fischer, Ea. 2012. "Federal Laws Relating to Cybersecurity: Discussion of Proposed Revisions." *Congressional Research Service* 7-5700 (R42114): 66. [www.crs.gov](http://www.crs.gov).

- Fitzgerald, Eugene, and Andreas Wankerl. 2011. "Why The Government Needs To Invest In Innovation." *Forbes*. Accessed May 4, 2016. <http://www.forbes.com/sites/ciocentral/2011/01/31/why-the-government-needs-to-invest-in-innovation/>.
- Frank, Robert. 2016. "China Has More Billionaires than US." *CNBC*. Accessed May 17, 2016. <http://www.cnbc.com/2016/02/24/china-has-more-billionaires-than-us-report.html>.
- Frizell, Sam. 2014. "Here Are 6 Huge Websites China Is Censoring Right Now." *TIME*. Accessed April 24, 2016. <http://time.com/2820452/china-censor-web/>.
- Fuglei, Monica. 2014. "How Internet Filtering Can Affect Education." *Concordia University Online*. Accessed April 24, 2016. <http://education.cu-portland.edu/blog/news/how-Internet-filtering-affects-education/>.
- Gates, Bill. 2014. "A Stunning Statistic About China and Concrete." *Gates Notes.com*. Accessed April 24, 2016. <https://www.gatesnotes.com/About-Bill-Gates/Concrete-in-China>.
- Gierow, Hauke Johannes. 2014. "Cyber Security in China : New Political Leadership Focuses on Boosting National Security Restructuring Internet Regulation. Placing Restrictions on Foreign Software . Developing the PRC'S Own IT Standards." *Mercator Institute for China Studies*, 1–9. Accessed May 3, 2016. [http://www.merics.org/fileadmin/user\\_upload/downloads/China-Monitor/China\\_Monitor\\_No\\_20\\_eng.pdf](http://www.merics.org/fileadmin/user_upload/downloads/China-Monitor/China_Monitor_No_20_eng.pdf).
- Glennie, Jonathan. 2011. "Cuba: A Development Model That Proved the Doubters Wrong | Jonathan Glennie | Global Development." *The Guardian*. Accessed March 20, 2016. <http://www.theguardian.com/global-development/poverty-matters/2011/aug/05/cuban-development-model>.
- Gouranga, and Gopal Das. 2015. "Why Some Countries Are Slow in Acquiring New Technologies? A Model of Trade-Led Diffusion and Absorption." *Journal of Policy Modeling* 37 (1). The Society for Policy Modeling: 65–91. doi:10.1016/j.jpolmod.2015.01.001.
- Greenwald, Glenn. 2013. "NSA Collecting Phone Records of Millions of Verizon Customers Daily." *The Guardian*. Accessed April 24, 2016. <http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>.
- Grisham, Lori. 2015. "Timeline: North Korea and the Sony Pictures Hack." *USA Today*. Accessed February 28, 2016. <http://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/>.
- Gu, Jibao, Yanbing Zhang, and Hefu Liu. 2014. "Importance of Social Capital to Student Creativity within Higher Education in China." *Thinking Skills and Creativity* 12 (96). Elsevier Ltd: 14–25. doi:10.1016/j.tsc.2013.12.001.

- Haggard, Stephan, and Jon R. Lindsay. 2015. "North Korea and the Sony Hack: Exporting Instability Through Cyberspace." *Asia Pacific Issues*, no. 117 (May). East-West Center: 1–8.
- Hartnett, Stephen John. 2011. *Google and the "Twisted Cyber Spy" Affair: US-Chinese Communication in an Age of Globalization*. *Quarterly Journal of Speech*. Vol. 97. Quarterly Journal of Speech.
- Hechinger, Fred M. 1984. "About Education – Censorship Rises in the Nation's Public Schools." *The New York Times*. Accessed April 24, 2016. <http://www.nytimes.com/1984/01/03/science/about-education-censorship-rises-in-the-nation-s-public-schools.html>.
- Henochowicz, Anne, David Schlesinger, Charlie Smith, and Yaqiu Wang. 2016. "What's Driving the Current Storm of Chinese Censorship?" *ChinaFile*. Accessed April 24, 2016. <http://www.chinafile.com/conversation/whats-driving-current-storm-chinese-censorship>.
- . 2016. "Why Xi Jinping's Media Controls Are 'Absolutely Unyielding.'" *Foreign Policy Magazine*. <http://foreignpolicy.com/2016/03/17/why-xi-jinpings->
- The History.com Staff. 2011. "Invention of the PC." *A+E Networks*. Accessed November 17, 2015. <http://www.history.com/topics/inventions/invention-of-the-pc>.
- . 2009. "U.S. Immigration Before 1965 - Facts & Summary." *A+E Networks*. Accessed February 28, 2016. <http://www.history.com/topics/u-s-immigration-before-1965>.
- . "Cultural Revolution." *History.com*. Accessed April 24, 2016. <http://www.history.com/topics/cultural-revolution>.
- Hu, C.T. 1984. "The Historical Background: Examinations and Control in Pre-Modern China Comparative Education." *Comparative Education* 20 (1): 7–26.
- Huang, Jing. 2013. "The Role of Government Propaganda in the Educational System during the Cultural Revolution in China." *Pembroke College at the University of Cambridge*. Accessed April 17, 2016. <http://www.pem.cam.ac.uk/wp-content/uploads/2013/04/Cultural-Revolution-in-China-paper.pdf>.
- Human Security Unit. 2016. "Human Security Approach | UN Trust Fund for Human Security." *The United Nations*. Accessed April 24, 2016. <http://www.un.org/humansecurity/human-security-unit/human-security-approach>.
- India Department of Electrical Communication and Engineering. 2016. "History - Department of Electrical Communication Engineering - IISc Bangalore, India." *Indian Institute of Science*. Accessed March 20, 2016. <http://ece.iisc.ernet.in/index.php/about-us/history>.
- India Department of Electronics and Information Technology. 2013. *National Cyber Security Policy -2013*. Ministry of Communications & IT Online. India:

<http://deity.gov.in/content/cyber-laws-security>. Accessed March 20, 2016.  
[http://deity.gov.in/sites/upload\\_files/dit/files/National\\_cyber\\_security\\_policy-2013\(1\).pdf](http://deity.gov.in/sites/upload_files/dit/files/National_cyber_security_policy-2013(1).pdf).

Information Office of the State Council of the People's Republic of China. 2016. "Govt. *White Papers*." *White Papers (中国政府白皮书) Online*. Accessed March 19.  
<http://www.china.org.cn/english/features/book/194485.htm>.

———. 2015. "Govt. *White Papers* - China.org.cn." *China.org*. <http://www.china.org.cn/e-white/>.

———. 2015. "Full Text: China's Military Strategy." *China Daily*. Accessed April 17, 2016.  
[http://www.chinadaily.com.cn/china/2015-05/26/content\\_20820628.htm](http://www.chinadaily.com.cn/china/2015-05/26/content_20820628.htm).

———. 2011. "The Path of China's Peaceful Development." *China.org.cn*. Accessed April 17, 2016. [http://www.china.org.cn/government/whitepaper/2011-09/06/content\\_23362449.htm](http://www.china.org.cn/government/whitepaper/2011-09/06/content_23362449.htm).

———. 2009. *China's National Defense (2010 年中国的国防) in 2008*. Vol. 2008.

———. 2008. "The Internet in China - China.org.cn." *China.org.cn*. Accessed April 17, 2016.  
[http://www.china.org.cn/government/whitepaper/node\\_7093508.htm](http://www.china.org.cn/government/whitepaper/node_7093508.htm).

———. (中华人民共和国中央人民政府). 2015. "Chinese Government *White Papers* - China Online (中国政府白皮书-中国网)." *Information Office of the State Council of the People's Republic of China Online*. Accessed April 17, 2016. [http://www.china.com.cn/ch-book/node\\_7114918.htm](http://www.china.com.cn/ch-book/node_7114918.htm)

International Relations Security Network. 2016. "Defense *White Papers* and National Security Strategies." *International Relations Security Network Online*. Accessed February 11, 2016.  
<http://www.isn.ethz.ch/Digital-Library/Publications/Series/Detail/?id=154839>.

Jin, Yu-le, and Ling Li. 2011. "A Postmodern Perspective on Current Curriculum Reform in China." *Chinese Education & Society* 44 (4): 25–43. doi:10.2753/CED1061-1932440402.

Jones, Terril Yue. 2013. "China Has 'Mountains of Data' about U.S. Cyber Attacks." *Reuters*. Accessed April 24, 2016. <https://ecf.paed.uscourts.gov/cgi-bin/ShowIndex.pl>.

Jordan, Tiffany L, and Dwobeng Owusu-Nyamekye. 2013. "China: An Emerging Asian Power in Manufacturing Production Outsourcing." *Journal of Global Intelligence & Policy* 6 (11): 116–23.

Kaspersky. 2015. "Cyberthreat Real-Time Map." Accessed October 15, 2015.  
<https://cybermap.kaspersky.com/>.

Keneally, Meghan. 2014. "Here's What the Internet Looks Like in North Korea." *ABC News*. Accessed February 28, 2016. <http://abcnews.go.com/International/Internet-north-korea/story?id=27789459>.

- Kimball, Will, and Robert E. Scott. 2014. "China Trade, Outsourcing and Jobs: Growing U.S. Trade Deficit with China Cost 3.2 Million Jobs between 2001 and 2013, with Job Losses in Every State." *Economic Policy Institute*. Accessed May 20, 2016. <http://www.epi.org/publication/china-trade-outsourcing-and-jobs/>.
- Kivunja, Charles. 2014. "Innovative Pedagogies in Higher Education to Become Effective Teachers of 21 St Century Skills : Unpacking the Learning and Innovations Skills Domain of the New Learning Paradigm." *International Journal of Higher Education* 3 (4): 37–48. doi:10.5430/ijhe.v3n4p37.
- Koh, Harold Hongju. 2012. "International Law in Cyberspace." *United States Department of State Legal Conference*. Accessed January 7, 2016. <http://www.state.gov/s/l/releases/remarks/197924.htm>.
- Krishna, Prasad. 2015. "State of Cyber Security and Surveillance in India A Review of the Legal Landscape." *Center for Internet Society*, no. Article 12.
- Kuhn, Anthony. 2016. "In Social Media Battle, Real Estate Mogul Takes On Chinese Government : Parallels : NPR." *National Public Radio Online*. Accessed April 24, 2016. <http://www.npr.org/sections/parallels/2016/03/01/468573357/in-social-media-battle-real-estate-mogul-takes-on-chinese-government>.
- Lenzo, Krysia. 2015. "The New Global Cyberwar without Boundaries—or Winners." *CNBC*. Accessed April 17, 2016. <http://www.cnb.com/2015/09/02/the-new-global-cyberwar-without-boundaries-or-winners.html>.
- Lewin, Arie Y., and Liu Yi. 2013. "The Future of China's Outsourcing Industry: Fuqua Research Looks into China's Ability to Leapfrog India." *The Fuqua School of Business at Duke University*. Accessed March 20, 2016. [http://www.fuqua.duke.edu/news\\_events/feature\\_stories/china-outsourcing-arie-lewin/#.Vr0SH\\_krKUL](http://www.fuqua.duke.edu/news_events/feature_stories/china-outsourcing-arie-lewin/#.Vr0SH_krKUL).
- Li, Amy. 2014. "Xinhua's Twitter Account Creates Uproar on Weibo." *South China Morning Post*. Accessed April 17, 2016. <http://www.scmp.com/news/china/article/1102860/xinhuas-twitter-account-stirs-uproar-among-chinas-weibo-users>.
- Li, Cheng, and Ryan McElveen. 2014. "Debunking Misconceptions About Xi Jinping's Anti-Corruption Campaign." *The Brookings Institution*. Accessed April 17, 2016. <http://www.brookings.edu/research/opinions/2014/07/17-xi-jinping-anticorruption-misconceptions-li-mcelveen>.
- Liu, Juliana. 2016. "Hong Kong's Missing Booksellers and 'Banned' Xi Jinping Book." *BBC News*. Accessed April 24, 2016. <http://www.bbc.com/news/world-asia-china-35480229>.

- Luijff, E, K Besseling, and Patrick De Graaf. 2013. "Nineteen National Cyber Security Strategies." *International Journal of Critical ...*, no. July 2015: 2–31. <http://inderscience.metapress.com/index/C76007176206246M.pdf>.
- Magnier, Mark. 2016. "China's Economic Growth in 2015 Is Slowest in 25 Years - WSJ." *The Wall Street Journal*. Accessed April 24, 2016. <http://www.wsj.com/articles/china-economic-growth-slows-to-6-9-on-year-in-2015-1453169398>.
- Markowitz, Eric. 2015. "Cuba's Internet Censorship And High Costs Mean Web Access Will Remain Elusive For Most Cubans." *International Business Times*, September 23. And High Costs Mean Web Access Will Remain Elusive For Most Cubans.
- Marsh, Peter. 2008. "China to Overtake US as Largest Manufacturer." *Financial Times*. Accessed April 24, 2016. <http://www.ft.com/intl/cms/s/0/2aa7a12e-6709-11dd-808f-0000779fd18c.html>.
- Martin, Fredrick Thomas. 1999. *Top Secret Intranet : How U.S. Intelligence Built Intelink—the World's Largest, Most Secure Network*. Upper Saddle River, N.J.: Prentice Hall PTR.
- Martin, Gary. 2016. "A Little Knowledge Is a Dangerous Thing - Meaning and Origin." *The Phrase Finder*. Accessed April 24, 2016. <http://www.phrases.org.uk/meanings/a-little-knowledge-is-a-dangerous-thing.html>.
- Masuda, Masayuki. 2006. "Chapter 3 China's Search for a New Foreign Policy Frontier : Concept and Practice of 'Harmonious World.'"
- McFaul, Michael, and Kathryn Stoner-Weiss. 2008. "The Myth of the Authoritarian Model: How Putin's Crackdown Holds Russia Back." *Foreign Affairs VO* - 87, no. 1. Council on Foreign Relations: 68.
- . 1993. "Thwarting the Specter of a Russian Dictator," no. 1. November: 1–17.
- McGraw Hill. 2002. "Little Knowledge Is a Dangerous Thing - Idioms by The Free Dictionary." *McGraw-Hill Dictionary of American Idioms and Phrasal Verbs*. Accessed April 24, 2016. <http://idioms.thefreedictionary.com/little+knowledge+is+a+dangerous+thing>.
- McKirby, Euan. 2015. "China's Net Users Outnumber Entire U.S. Population 2-1." *CNN*. Accessed April 24, 2016. <http://www.cnn.com/2015/02/03/world/china-Internet-growth-2014/>.
- Menn, Joseph. 2015. "Social Media Companies Step up Battle against Militant Propaganda." *Reuters*. Accessed April 24, 2016. <http://www.reuters.com/article/us-california-shooting-socialmedia-insig-idUSKBN0TO0OS20151206>.



- Ministry of Education of The People's Republic of China. 2013. "Educational Policies." *Ministry of Education of the People's Republic of China Online*. Accessed April 24, 2016. [http://www.moe.edu.cn/publicfiles/business/htmlfiles/moe/moe\\_2804/index.html](http://www.moe.edu.cn/publicfiles/business/htmlfiles/moe/moe_2804/index.html).
- Ministry of Foreign Affairs of the Russian Federation. "Information Security Doctrine of the Russian Federation." 2000. Accessed April 27, 2016. <http://archive.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument>.
- Ministry of National Defense the People's Republic of China, and Hua-Chu Kao. 2011. 國防報告書. Edited by 2011 Roc Defense Report Editing Committee. 1st ed. Taipei: Ministry of National Defense.
- Miou, Song. 2015. "Full Text: China's Military Strategy." *Xinhuanet*. Accessed April 24, 2016. [http://news.xinhuanet.com/english/china/2015-05/26/c\\_134271001\\_4.htm](http://news.xinhuanet.com/english/china/2015-05/26/c_134271001_4.htm).
- Mokyr, Joel. 2000. "Knowledge, Technology, and Economic Growth During the Industrial Revolution." *Productivity, Technology and Economic Growth*, 1–400. Accessed April 24, 2016. <http://www.springer.com/economics/growth/book/978-0-7923-7960-7>.
- Mozur, Paul. 2016. "U.S. Adds China's Internet Controls to List of Trade Barriers." *The New York Times*. Accessed April 27, 2016. <http://www.nytimes.com/2016/04/08/business/international/china-Internet-controls-us.html?ref=collection%2Ftimestopic%2FInternet+Censorship+in+China>.
- Mužiková, Dáša, Tasnim Chaaban, Jacobo Salomon, and Joyce Lee Ching Yan. 2013. "Journalism Self-Censorship." *The Salzburg Academy on Media and Global Change*. Accessed April 27, 2016. <http://www.salzburg.umd.edu/media-innovation/journalism-self-censorship>.
- Myre, Greg. 2014. "The U.S. And Cuba: A Brief History Of A Complicated Relationship : Parallels." *National Public Radio Online*. Accessed March 3, 2016. <http://www.npr.org/sections/parallels/2014/12/17/371405620/the-u-s-and-cuba-a-brief-history-of-a-tortured-relationship>.
- Nakashima, Ellen. 2015. "Chinese Government Has Arrested Hackers It Says Breached OPM Database." *The Washington Post*. Accessed April 28, 2016. [https://www.washingtonpost.com/world/national-security/chinese-government-has-arrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb\\_story.html](https://www.washingtonpost.com/world/national-security/chinese-government-has-arrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html).
- National Bureau of Statistics of China. 2012. "National Bureau of Statistics of China." *National Bureau of Statistics of China Online*. Accessed May 4, 2016. <http://www.stats.gov.cn/english/ClassificationsMethods/Methods/>.

- National Initiative for Cybersecurity Careers and Studies. 2014. "Cyber Glossary." *Department of Homeland Security Sites*. Accessed April 13, 2016. [https://niccs.us-cert.gov/glossary#letter\\_c](https://niccs.us-cert.gov/glossary#letter_c).
- National People's Congress of the People's Republic of China. 2004. "The National People's Congress of the People's Republic of China - Constitution of the People's Republic of China." *Npc.gov*. Accessed April 24, 2016. [http://www.npc.gov.cn/englishnpc/Constitution/node\\_2825.htm](http://www.npc.gov.cn/englishnpc/Constitution/node_2825.htm).
- . 1982. "Constitution of the People's Republic of China." Accessed April 24, 2016. <http://en.people.cn/constitution/constitution.html>.
- NATO CCDCOE. 2008. "Cyber Definitions." *Cooperative Cyber Defence Centre of Excellence Online*. Accessed February 28, 2016. <https://ccdcoe.org/cyber-definitions.html>.
- . "Tallinn Manual Process." *CCDCOE*. Accessed February 28, 2016. <https://ccdcoe.org/tallinn-manual.html>.
- Ortner, Daniel. 2015. "Cybercrime and Punishment: The Russian Mafia and Russian Responsibility to Exercise Due Diligence to Prevent Trans-Boundary Cybercrime," 177–218. Accessed March 20, 2016. <http://papers.ssrn.com/abstract=2576480>.
- Ovide, Shira. 2016. "U.S. Official Releases Details on Prism Program." *The Wall Street Journal*. Accessed February 22, 2016. <http://www.wsj.com/articles/SB10001424127887324299104578533802289432458>.
- País, Ediciones El. 2004. "Atta recibió en Tarragona joyas para que los miembros del 'comando' del 11-S se hiciesen pasar por ricos saudíes." *El País*, March. Ediciones El País. Accessed February 22, 2016. [http://elpais.com/diario/2004/03/21/espana/1079823611\\_850215.html](http://elpais.com/diario/2004/03/21/espana/1079823611_850215.html).
- Peltoniemi, Mirva, and Elisa Vuori. 2004. "Business Ecosystem as the New Approach to Complex Adaptive Business Environments." *Proceedings of eBusiness Research Forum*, 267–81.
- Peralta, Katherine. 2014. "Outsourcing to China Cost U.S. 3.2 Million Jobs Since 2001." *U.S. News and World Report*. Accessed April 24, 2016. <http://www.usnews.com/news/blogs/data-mine/2014/12/11/outourcing-to-china-cost-us-32-million-jobs-since-2001>.
- Perlez, Jane. 2015. "In Victory for Philippines, Hague Court to Hear Dispute Over South China Sea - The New York Times." *The New York Times*. Accessed May 4, 2016. <http://www.nytimes.com/2015/10/31/world/asia/south-china-sea-philippines-hague.html>.
- . 2012. "With \$20 Billion Loan Pledge, China Strengthens Its Ties to African Nations." *The New York Times*. <http://www.nytimes.com/2012/07/20/world/asia/china-pledges-20-billion-in-loans-to-african-nations.html>.

- Press, Larry, William Foster, Peter Wolcott, and William McHenry. 2003. "The Internet in India and China." *Information Technologies & International Development* 1, no. 1: 41-60. *Business Source Elite*, EBSCOhost (accessed May 11, 2016).
- Qizhi, He. 1987. "China and International Law." *Grotiana* 8 (1): 37-41. doi:10.1163/016738312X13397477911665.
- Ranganathan, Roshni. 2015. "54483 Cyber-attacks Reported This Year." *Lex Insider*. Accessed January 7, 2016. <http://lexinsider.com/2015/12/03/54483-cyber-attack-reported-this-year-india/>.
- Richardson, Hannah. 2015. "Chinese Schools 'Robbing Young of Individuality' - BBC News." *BBC News*. Accessed May 4, 2016 <http://www.bbc.com/news/education-34605430>.
- Richburg, Keith B. 2011. "Chinese Artist Ai Weiwei Arrested in Ongoing Government Crackdown - The Washington Post." *The Washington Post*. Accessed May 4, 2016. <https://www.washingtonpost.com/world/chinese-artist-ai-wei-wei->
- Riegel, Klaus-Georg. 2005. "Marxism-Leninism as a Political Religion." *Totalitarian Movements and Political Religions* 6 (1): 97-126. doi:10.1080/14690760500099788.
- Risen, Tom. 2014. "Tiananmen Censorship Reflects Crackdown Under Xi Jinping." *US News & World Report Online*. Accessed April 24, 2016. <http://www.usnews.com/news/articles/2014/06/03/tiananmen-censorship-reflects-crackdown-under-xi-jinping>.
- Robinson, Ken. 2010. "Bring on the Learning Revolution!" In *TED*. TED Online. Accessed April 17, 2016. [http://www.ted.com/talks/sir\\_ken\\_robinson\\_bring\\_on\\_the\\_revolution](http://www.ted.com/talks/sir_ken_robinson_bring_on_the_revolution).
- . 2006. "Do Schools Kill Creativity." In *TED*. TED Online. Accessed April 17, 2016. [http://www.ted.com/talks/ken\\_robinson\\_says\\_schools\\_kill\\_creativity](http://www.ted.com/talks/ken_robinson_says_schools_kill_creativity).
- Rogers, Vaughn. 2015. "Comparative Analysis of China and United States Cybersecurity Issues." 1. South Orange. Working paper.
- . 2013. "Chinese Education: Shifting to the West or Business as Usual?" South Orange. Working paper.
- Roscini, Marco. 2015. "Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations." *Texas International Law Journal* 50 (2): 233-73.
- Rothman, Andy. 2008. "Harmonious Society." *China Business Review* 35 (2): 24-28.
- Runciman, David. 2008. *Political Hypocrisy: The Mask of Power, from Hobbes to Orwell and Beyond*. Princeton : Princeton University Press, 2008.

- S.R. 2015. "The Economist Explains: Why China's Economy Is Slowing." *The Economist*. Accessed April 24, 2016. <http://www.economist.com/blogs/economist-explains/2015/03/economist-explains-8>.
- . 2015. "China's Data Doubts: Official Data Say China's Economy Is Barely Slowing. Are They Believable?" *The Economist*. Accessed April 24, 2016. <http://www.economist.com/blogs/freeexchange/2015/10/chinas-data-doubts>.
- Sanger-Katz, Margot. 2014. "Can Cuba Escape Poverty but Stay Healthy?" *The New York Times*. Accessed March 6, 2016. <http://www.nytimes.com/2014/12/19/upshot/can-cuba-escape-poverty-but-stay-healthy.html>.
- Schmid, Alex P. 2011. *The Routledge Handbook of Terrorism Research*. Routledge Handbooks. New York : Routledge, 2011.
- Schuman, Michael. 2011. "Can China's Economy Thrive with a Censored Internet?" *TIME.com*. Accessed April 24, 2016. <http://business.time.com/2011/10/26/can-chinas-economy-thrive-with-a-censored-Internet/>.
- Segal, Adam. 2013. "The Code Not Taken: China, the United States, and the Future of Cyber Espionage." *Bulletin of the Atomic Scientists* 69 (5): 38–45. doi:10.1177/0096340213501344.
- Shih, Gary, and Paul Carsten. 2015. "Out of the Shadows, China Hackers Turn Cyber Gatekeepers." *Reuters*. Accessed April 24, 2016. <http://www.reuters.com/article/us-china-cybersecurity-idUSKCN0P813N20150629>.
- Simpson, John. 2016. "Critics Fear Beijing's Sharp Turn to Authoritarianism." *BBC News*. Accessed April 24, 2016. <http://www.bbc.com/news/world-35714031>.
- Sleuwaegen, Leo, and Priscilla Boiardi. 2014. "Creativity and Regional Innovation: Evidence from EU Regions." *Research Policy* 43 (9). Elsevier B.V.: 1508–22. doi:10.1016/j.respol.2014.03.014.
- Stahl, Lesley. 2016. "The Great Brain Robbery." *CBS News*. Accessed April 27, 2016. <http://www.cbsnews.com/news/60-minutes-great-brain-robbery-china-cyber-espionage/>.
- . 2016. "How China's Spies Can Watch You at Your Desk." *CBS News*. Accessed April 27, 2016. <http://www.cbsnews.com/news/60-minutes-overtime-how-chinas-spies-can-watch-you-at-your-desk/>.
- Stevens, Mark. 2012. "Is Ai Weiwei China's Most Dangerous Man?" *Smithsonian*. Accessed April 24, 2016. <http://www.smithsonianmag.com/arts-culture/is-ai-weiwei-chinas-most-dangerous-man-17989316/?no-ist>.

- Stiennon, Richard. 2011. "A Brief History Of Chinese Cyberspying." *Forbes*. Accessed January 10, 2016. <http://www.forbes.com/sites/firewall/2011/02/11/a-brief-history-of-chinese-cyberspying/#fbd405fff3c7>.
- Taibi, Catherine. 2015. "These Are The Most Censored Countries In The World." *Huffington Post*. Accessed March 20, 2016. [http://www.huffingtonpost.com/2015/04/21/most-censored-countries-cpj-top-ten\\_n\\_7109932.html](http://www.huffingtonpost.com/2015/04/21/most-censored-countries-cpj-top-ten_n_7109932.html).
- Tao, Liqing, Maragaret Berci, and Wayne He. 2006. "Historical Background: Expansion of Public Education." *The New York Times*. Accessed April 3, 2016. <http://www.nytimes.com/ref/college/coll-china-education-001.html>.
- The Associated Press. 2016. "A Glance at China's Latest Economic Numbers." *U.S. News and World Report*. Accessed April 3, 2016. <http://www.usnews.com/news/business/articles/2016-04-15/a-glance-at-chinas-latest-economic-numbers>.
- The Department of Economic and Social Affairs of the United Nations Secretariat. 2012. "Statistical Annex." *Review Literature And Arts Of The Americas*. Accessed May 11, 2016. [http://www.un.org/en/development/desa/policy/wesp/wesp\\_current/2012country\\_class.pdf](http://www.un.org/en/development/desa/policy/wesp/wesp_current/2012country_class.pdf).
- The Economist Intelligence Unit. 2014. "Creative Productivity Index: Analysing Creativity and Innovation in Asia," no. 1. August: 88.
- The Economist Staff. 2013. "What Is the Difference between Common and Civil Law?" *The Economist*. Accessed March 13, 2016. <http://www.economist.com/blogs/economist-explains/2013/07/economist-explains-10>.
- The Global Times Staff. 2016. "Why Does the Western Media Hate the GFW so Much? - Global Times." *The Global Times*. Accessed April 24, 2016. <http://www.globaltimes.cn/content/977979.shtml#.VwsGseOTqGY>.
- The History.com Staff. 2011. "Invention of the P.C." *A+E Networks*. Accessed February 22, 2016. <http://www.history.com/topics/inventions/invention-of-the-pc>.
- . 2010. "The Invention of the Internet." *A+E Networks*. Accessed November 27, 2015. <http://www.history.com/topics/inventions/invention-of-the-Internet>.
- The White House. 2008. "The Comprehensive National Cybersecurity Initiative." *Washington, DC: White House*, 1–5. Accessed April 24, 2016. <http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf> \n<http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:The+Comprehensive+National+Cybersecurity+Initiative#0>.
- The United States Congress. "National Institute of Standards and Technology Act" 1 (1).

- Tong, Bao. 2015. "How Deng Xiaoping Helped Create a Corrupt China." *The New York Times*. Accessed April 24, 2016. <http://www.nytimes.com/2015/06/04/opinion/bao-tong-how-deng-xiaoping-helped-create-a-corrupt-china.html>.
- Toxen, Bob. 2014. "The NSA and Snowden." *Communications of the ACM* 57 (5): 44–51. doi:10.1145/2594502.
- United Nations. 1945. "Charter Of The United Nations And Statute Of The Charter Of The International Court Of Justice," 55. ISBN: 9789210020251.
- Vandergraft, Kay E. 1997. "Censorship, the Internet, Intellectual Freedom and Youth." *Rutgers University Online*. Accessed March 20, 2016. <http://comminfo.rutgers.edu/professional-development/childlit/censorship.html>.
- Ventre, Daniel, Dean Cheng, Alan Chong, Alice Ekman, Thomas Flichy de La Neuville, Longdi Xu, and Samuel Cherian. 2014. *Chinese Cybersecurity and Cyberdefense (Information Systems, Web and Pervasive Computing)*. Edited by Daniel Ventre. 1st ed. Hoboken: John Wiley & Sons, Inc.
- . 2013. *Cyber Conflict: Competing National Perspectives*. John Wiley & Sons, Inc.
- Vicens, A.J. 2015. "The Shocking Truth About Wednesday's Apocalypse Involving Wall Street, China, ISIS, and United Airlines." *Mother Jones*. Accessed March 13, 2016. <http://www.motherjones.com/politics/2015/07/nyse-glitch-hack-china-cia-cyber-isis>.
- Vogel, Ezra F. 2011. *Deng Xiaoping and the Transformation of China*. 1st ed. Cambridge, Mass: Harvard University Press.
- Warner, Michael. 2014. *The Rise and Fall of Intelligence : An International Security History*. Washington: Georgetown University Press.
- Watson, Dale L. 2002. "FBI — The Terrorist Threat Confronting the United States." *Federal Bureau of Investigation*. Accessed March 20, 2016. <https://www.fbi.gov/news/testimony/the-terrorist-threat-confronting-the-united-states>.
- Wen, Philip. 2016. "Party Pressure: Chinese Journalists in Hot Water over 'Subversive' Headline." *Sydney Morning Herald*. Accessed April 27, 2016. <http://www.smh.com.au/world/party-pressure-chinese-journalists-in-hot-water-over-subversive-headline-20160303-gn9hdi.html>.
- Wertime, David. 2015. "This Chart Explains Everything You Need to Know About Chinese Internet Censorship." *Foreign Policy Magazine*. March 20, 2016. <http://foreignpolicy.com/2015/04/20/this-chart-explains-everything-you-need-to-know-about-chinese-Internet-censorship/>.

- Whittaker, David J. 2007. *The Terrorism Reader*. Routledge Readers in History. London ; New York : Routledge, 2007.
- Williamson, Myra. 2009. *Terrorism, War and International Law. [Electronic Resource] : The Legality of the Use of Force against Afghanistan in 2001*. The Ashgate International Law Series. Farnham, England ; Burlington, VT : Ashgate, ©2009.
- Wilshusen, Gregory C. 2015. "U.S. G.A.O. - Key Issues: Cybersecurity." *United States Government Accountability Office*. Accessed March 20, 2016. [http://gao.gov/key\\_issues/cybersecurity/issue\\_summary](http://gao.gov/key_issues/cybersecurity/issue_summary).
- Wu, Guo. 2014. "Recalling Bitterness: Historiography, Memory, and Myth in Maoist China." *Twentieth-Century China* 39 (3): 245–68. doi:10.1179/1521538514Z.00000000047.
- Xinyu, Yang, Zhengshou Qi, Zeng Ming, Hengyi Wei, and Li Zhu. 2001. "CAINONET 业务流设计系统的通信模型描述." *Xi'an Jiao Yong University Online* 22 (April). Xi An: 426–29. ISSN: 1000-1220.
- Xu, Benia. 2015. "Media Censorship in China." *Council on Foreign Relations*. Accessed April 27, 2016. <http://www.cfr.org/china/media-censorship-china/p11515>.
- Zhang, Jian. 2012. "China's Defense White Papers: A Critical Appraisal." *Journal of Contemporary China* 21 (77): 881–98.
- Zhao, Jinqiu. 2008. "A Snapshot of Internet Regulation in Contemporary China: Censorship, Profitability and Responsibility." *China Media Research* 4 (3): 37–43.