6-2016

The Rise of China's Hacking Culture: Defining Chinese Hackers

William Howlett IV
California State University - San Bernardino, howlettw@coyote.csusb.edu

THE RISE OF CHINA'S HACKING CULTURE

DEFINING CHINESE HACKERS

A Thesis

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts

in

Social Sciences and Globalization

---

by

William Sedgwick Howlett

June 2016

THE RISE OF CHINA'S HACKING CULTURE

DEFINING CHINESE HACKERS

A Thesis

Presented to the

Faculty of

California State University,

San Bernardino

---

by

William Sedgwick Howlett

June 2016

Approved by:

Cherstin Lyon, Committee Chair, Social Sciences and Globalization

Jeremy Murray, Committee Member, History

Jose Munoz, Committee Member, Sociology

ABSTRACT

China has been home to some of the most prominent hackers and hacker groups of the global community throughout the last decade. In the last ten years, countless attacks globally have been linked to the People's Republic of China (PRC) or those operating within the PRC. This exploration attempts to investigate the story, ideology, institutions, actions, and motivations of the Chinese hackers collectively, as sub-groups, and as individuals. I will do this using sources ranging from basic news coverage, interviews with experts and industry veterans, secondary reportage, leaked documents from government and private sources, government white papers, legal codes, blogs and microblogs, a wide array of materials from the darker corners of the online world, and many other materials. The work will begin to sketch for the reader some of the general and specific aspects of the shadowy world of cybercrime and hacker culture in China in recent years. One of the most prevalent beliefs is that the Chinese government is in fact the one responsible, whether directly or by sponsor, for cyber-attacks on foreign systems. My careful analysis has revealed is not always the case, or at least more complex than simply labeling the group as a state actor. At the root of these attacks is a social movement of "hacktivists," a patriotic sub-culture of Chinese hackers. It is incorrect to allege that all attacks are performed by state-sponsored individuals or groups, because there are many individuals and groups that are motivated by other factors.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

INTRODUCTION

There is an innovative frontier of cyber warfare that is rapidly expanding all over the world, with billions of individuals now united by the internet. Due to the greater opportunities to acquire information, individuals are linked in a way that has never been experienced before. Massive security concerns within online systems are increasing and transforming on a daily basis due to the global access to monetary and government systems, as well as information stored by private institutions. These security issues parallel the creation and growth of a global hacker culture. China has been home to some of the most prominent hackers and hacker groups of the global community throughout the last decade. In the last ten years, countless attacks globally have been linked to the People's Republic of China (PRC) or those operating within the PRC. According to the 2012 State of the Internet Report published by the Akamai group, an online services provider, a third of all cyber-attacks that they were aware of have originated in China in the third quarter of 2012.[1] This report names China as the biggest hacking entity and as the statistical home to the majority of cyber-attacks among all countries.

In the last twenty years China has been in the midst of a type of internet revolution as its peoples are seeking new ways to express themselves as they are further exposed to the greater technology-based globe. Thanks to the establishment of the internet and the liberties that are allowed to its users, the hacking culture in China has grown and advanced in ways that are more dynamic

[1] Akamai. Q1 State If the Internet Report 2013. Rep. N.p.: Akamai, 2013. Print.

and dramatic than any other nation. Although cyber-crimes in Russia, the United States, and countries of the Middle East have garnered much attention over the past few decades, Chinese hackers operate on a scale far greater and vastly different than any other.

Statement of Purpose

This exploration attempts to investigate the story, ideology, institutions, actions, and motivations of the Chinese hackers collectively, as sub-groups, and as individuals. I will do this using sources ranging from basic news coverage, interviews with experts and industry veterans, secondary reportage, leaked documents from government and private sources, government white papers, legal codes, blogs and microblogs, a wide array of materials from the darker corners of the online world, and many other materials. I hope that the work will begin to sketch for the reader some of the general and specific aspects of the shadowy world of cybercrime and hacker culture in China in recent years.

In academic studies and the media, there is a developing fascination in cyber-attacks and cyber-espionage. This includes a particular interest in Chinese hackers infiltrating personal, corporate, and government webpages in a wide variety of countries. One of the most prevalent beliefs is that the Chinese government is in fact the one responsible, whether directly or by sponsor, for cyber-attacks on foreign systems. My careful analysis has revealed is not always the case, or at least more complex than simply labeling the group as a state actor. The People's Liberation Army (PLA) has indeed established one of the

most advanced cyber-capabilities apart from Russia, Iran, and the United States. In some accusations, it is suspected that Chinese authorities are simply intentionally ignoring unlawful behaviors that further the country's economic goals, or which strengthen the Chinese Communist Party's (CCP) agenda.

Yet, there is something truly extraordinary taking place in China that many media outlets tend to gloss over. Hidden at the root of these attacks is a social movement of "hacktivists," a patriotic sub-culture of Chinese hackers. It is too simple and incorrect to allege that all attacks are performed by state-sponsored individuals or groups, because there are many individuals and groups that are motivated by other factors. There are individuals who perform these actions outside of the influence of the government, and there are many distinct motivations involved. This complexity is generally not found in much news coverage and analysis related to the field of global cyber warfare, but this landscape is indeed complex and worth further exploration. In my research, I have found that there are underlying factors related to Chinese cultural identity, nationalism, individual status, and a hacker's personal reputation that can be hidden within the context of this cyber-war.

Recently, there has been a push within China to restore some traditional forms of identity. Today, both Confucianism and Maoism are being revived in China. Whether it is a return to Confucian beliefs, or merely reverting the Communist Party back towards Maoist beliefs, there is indeed cultural change happening. The cultural landscape of China continues to radically transform and shift, even as it did throughout most of the twentieth century. The post-Mao era

has brought not slowing to the cultural changes and the constant reinvention of Chinese identity, and these changes certainly affect China's hacker culture. Within the cyber-attacks that originate in China sometimes there are patriotic motivations even if the group is not employed or directed by the state. There is an attempt to preserve an essential or idealized Chinese identity in the midst of a barrage of foreign ideas and products. Sometimes this is Confucian China that is considered to be under attack by patriotic Chinese people, sometimes it is Marxism and Maoism, and sometimes it is China's sovereign claims to its borders at sea and on land. Interestingly, within these attacks by hackers there can be seen a kind of homegrown effort to enhance or protect Chinese identity and interest. This is a new generation, and it is one that is perhaps less troubled than those before it by painful past events like the Cultural Revolution or Tiananmen Square. These events profoundly alienated and embittered activists and intellectuals, many of whom were silenced, or reluctantly chose silence, or emigrated at their first opportunity. While this new generation of potential activists has grown with perhaps some awareness of these events, online forums and new media have given new intellectuals and activists ways to organize and express themselves that individuals in these earlier eras could not. These platforms, while the state tries to control them in certain ways, still can potentially give voice to patriotism, protest, and frustration of all kinds as articulations of cultural identity, and that cultural continues to be in flux.

The topic of cybercrime and cyberwarfare are extraordinarily important elements in the constantly innovating technical landscape where cyberspace

converges with an individual's more essential daily facets. The occurrence of hacking is a result of the advancement in online networking tools like the Internet. Cyber-espionage has the potential to affect everything from entertainment to financial transactions, social networking, education, and countless other aspects of our lives. In fact, many online systems that comprise of today's global community, including health-care organizations, fiscal systems, and confidential military systems can be potentially destroyed or looted by hackers. From high-profile and far-reaching banking hacks, to the titanic leaks and hacks connected to Edward Snowden and Julian Assange, and the organizations Ashley Madison and Mossack Fonseca, the world is becoming increasingly aware that the risk to our confidential information seems to be growing. It impacts people, and it harms international organizations. Besides the most prominent global hacks noted immediately above, Chinese hackers continue to work at an astounding scale. One Chinese group alone, APT1, has methodically stolen hundreds of terabytes of information from at least one hundred and forty one organizations, and has proven that it has the competence and the intention to pilfer from dozens of organizations at the same time.[2] Hacking activities have led to the loss of billions of dollars worldwide, whether directly and incidentally.

Due to this, the subject of cyber-crime is a hotly deliberated topic by both media and security groups. According to Dmitri Alperovitch, vice president of threat research for the cybersecurity specialists, McAfee Securities, "Today we see pretty much any company that has valuable intellectual property or trade

[2] Mandiant Inc. APT1: Exposing One of China's Espionage Units. Mandiant, 2014. Print.

secrets of any kind being pilfered continually, all day long, every day, relentlessly."[3] It is the pilfering of items like trade secrets and patents that has cost American companies substantial income and has regularly led to the loss of employment opportunities. In an interview that I performed with the Vice President of Cyber Security at Masergy, David Venable, "Chinese cyber efforts have typically been around stealing intellectual property for business. This could be both government backed, or financed independently. But again, sometimes the same individuals will do work for both, so there can be overlap."[4] Estimates of job losses due to cybercrime could be as high as 200,000 American jobs, and as many as 150,000 jobs in Europe.[5] The Chief of the Federal Bureau of Investigation, James Comey, has gone on record stating that the yearly costs to American businesses are "impossible to count," however, extend well into the billions.[6] These losses are a result of lost exclusive markets, lost competitiveness, and other factors as industry secrets are stolen and used by competitors.

From Washington's perspective, Cybersecurity and espionage like this constitutes a topic that the People's Republic of China has commonly avoided or denied. Yet potentially, it has the ability to drastically influence impending political, economic, and military dealings between the U.S. and China. The

---

[3] Gross, Michael Joseph. "Enter the Cyber-dragon." Vanity Fair. Sept, 2011. Accessed October 19, 2015. http://www.vanityfair.com/news/2011/09/chinese-hacking-201109
[4] Venable, David. "Chinese Hackers." E-mail interview by author. April 13, 2016.
[5] MCAffee Securities. *Net Losses: Estimating the Global Cost of Cybercrime*. Report. Santa Clara: Center for Strategic and International Studies, 2014.
[6] "FBI Chief: China Leader in Cyber Crime." Voice of America News. October 5, 2014. Accessed October 19, 2015. http://www.voanews.com/content/fbi-chief-says-china-leader-in-cyber-crime/2473611.html

debate surrounding theft of intellectual property will become vastly more significant as modern societies becomes progressively more technological, and a desire to understand and curb hacking even while hacker groups often defy law enforcement and even identification.

Within the Chinese hacking world there is an ever-changing mix of official, military, and civilian groups. These groups are generally tough to differentiate from each other. Due to this, accusations critical of the Chinese government are common. Security organizations like Mandiant, FireEye, and Trend Micro (all of which are used in this research), in addition to companies like Google have regularly blamed Chinese hackers in the theft of intellectual property from all aspects of society. This research attempt to show that this hacker culture that should be better understood and might be of greatest importance among all of China's hacking groups moving forward, due to the range of motivations and targets.

The issue that is the focal point of my research is unravelling the nature, motivations, and classifications of Chinese hacker groups. The goal is to provide the reader with an understanding of how cultural changes in Chinese identity have allowed individuals the opportunity to explore and expand the landscape of online activism, one dimension of which is hacking. Understanding the cultural foundations of China's hackers today has led me to explore the recent history of the People's Republic of China, and how Chinese identity has transformed so fundamentally in the twentieth century, through the post-Mao era, and into the twentieth century. I will attempt to provide a more detailed look into Chinese

hacker culture, because I feel like the greater story is the hackers themselves instead of the Chinese government. Cyber-attacks by individuals out of China, whether by state-sponsored actors, by independent nationalistic groups, or by profit-seekers who are merely seeking the highest bidder for their services, has turned global cyber-warfare into a severe international threat. Yet in my opinion, the characteristically swift description of these collections by other governments, organizations, and various news outlets is irresponsible and perhaps dangerous. It is true that hackers in China are persistent, and their influence is undeniable. Within the society there are hacker publications, hacker organizations, and online hacker forums. Yet, Chinese hacker culture thrives on an internet driven nationalism. Even the ”Red Hacker Alliance,” which is the most commonly known and one of the oldest hacker groups in China, is just a loose association allowing disparate cells who banded together for nationalistic and political purposes.

The purpose of my research is to distinguish, as clearly as possible, between the various groups of Chinese hackers: state-sponsored, freelance, and independent. There are inherent motivations that distinguish the groups. There is also sometimes a very fine line that separates the government actors from the patriotic actors, and sometimes that line can be blurred beyond discernibility for the observer. In the course of my research, there are a few questions that I will attempt to answer. Why are each of these groups doing engaged in these activities? What are some of the common motivations for each, and how do they differ from one another? How do independent hackers distinguish themselves from their state-sponsored counterparts? How do independent hackers organize?

I hope to demonstrate that it is the disparate motivations to engage in hacking and cyber espionage that most clearly distinguishes each group from one another. The motivations behind independent hackers are very intriguing. Some of the earliest and oldest groups are pro-China activists, but not necessarily or not always pro-government activists. They merely have sought the betterment of China through their activities. Some of the groups within this category came about in response to various political issues in an attempt to push a patriotic agenda. There are others who are fueled by financial gain, or merely to enhance their reputation. There are many historical, political, and social aspects that have not been fully explored in previous analyses, and I take on these daunting and opaque questions directly, using a combination of published and unpublished sources, interviews, and personal online investigation.

Along these same lines, there are other issues worth exploring such as the question of how these motivations affect the actions of these groups. State-sponsored hackers have been known to attack different systems and have a different type of victim than that of their patriotic, non-state-sponsored counterparts. These different things have helped independent activists distinguish themselves from the others, both in the nature of their work as well as in how each group organizes. According to an interview I performed with a former member of Anonymous Serbia, the motives, methods, and goals are what make it possible to distinguish between independent and state-sponsored. He stated “I believe that main method of distinguishing them is by the work they do. Independent groups usually don't achieve a lot, as they are driven by emotion,

while state-sponsored hackers have a specific goal. So, usually I can distinguish them just by looking at the results of their work."[7] I will explore these questions in an attempt to expose the common misconceptions of cyberwarfare in China.

A central issue surrounding a hacker organization when attacks are discovered, is what type of association, if there is one at all, the group might have with any state administration or organization. Is it legitimately sponsored by the government or is it employed as a proxy to implement the Chinese Communist Party's political agenda? The real question is whether there are two factions operating within China, with the first being a collection of private citizens and the other a division of the People's Liberation Army (PLA) or individuals employed as state agents? "Chinese hackers" have littered the media landscape, along with theories about government involvement, along with the growing forms of cyber-crimes they have perpetrated. According to an interview I performed with the founder of HackRead, this misconception is what he believes is a significant issues. He states "The Chinese are very sophisticated in their attacks but accusing everything on them or the Russians sounds like a script of some "Hollywood movie.""[8] What is commonly omitted from most of this reportage and scholarship is a clear background and explanation on just who comprises these secretive organizations.

Despite the fact that research on Chinese hackers is relatively new owing to the modern progress of individual and societal cyber-capabilities. There is some significant work emerging, and the issues concerning cybercrime on a

[7] Uzunovic, Agan. "Chinese Hackers." E-mail interview by author. April 5, 2016
[8] Waqas, Amir. "Chinese Hackers." E-mail interview by author. April 7, 2016.

grander level have been explored from quite a few perspectives. The topic of hacking and cyber-warfare is far older than that of hackers in China. For example, the United Nations General Assembly implemented computer crime law in 1990, which is a full four years before the internet was available in China. In the mid-1990's, nations began to form tactics and shared doctrines to fight cybercrime and safeguard intellectual data, and in this study I will explore these and other policies and laws in various countries. At the beginning of the twenty-first century, numerous regulations and laws were established internationally by the majority of countries throughout the international community. Countless countries have created legislation with protection from, and prosecution of, cybercrimes as the goal. Many researchers and academics had become attracted to the fields of cybercrime, the internet, and cyberespionage as information has become more easily accessible and the topics currency and popularity has exploded in the public sphere.

There are many researchers who explore topics that are peripherally related to my proposed field of research, and some who take on a similar topic directly. *The Dark Sides of the Internet: On Cyber Threats and Information Warfare* (Peter Lang GmbH, 2013), written by the individual in charge of cyber-defense research as well as the Deputy Research Director at the Swedish Defense Research Agency, Roland Heickero, explores several areas related to my field such as theft of data and information, cybercrime and cyber threats, and the consequences of such actions. He explains the importance of the internet as a means for greater freedoms for both criminal organizations and political

activists alike. Another work by Julie Mehan, Associate Professor at the University of Maryland, titled *CyberWar, CyberTerror, CyberCrime: A Guide to the Role of Standards in an Environment of Change and Danger,* (IT Governance Publishing, 2008) attempts to create a greater awareness of changing threats in the cyber landscape. These are just two of the many examples of broad scale perspectives on the field of cybercrime that serve as a technical background to my study of Chinese hackers. There are many other individuals like Heickero and Mehan who provide this type of broad exploration of the topic of cybercrime.

The topic of Chinese cybercrime itself is less clearly defined or even examined in academic circles. I have found that research on the subject of cyber-capabilities in China are usually categorized in two ways: works on global cyberwarfare that include sections on China, and works on the cyber-capabilities of the Chinese military like Elisabette M. Marvel's *China's Cyber Warfare Capability*. (Nova Science Publishers, Incorporated, 2010) Works such as these provide valuable examinations of how China fits into the larger topic of global cybersecurity, but they do not provide a look at the distinctive characteristics of Chinese hacker groups themselves.

Other sources explore the phenomenon and rise of hackers in other broader contexts. RAND Corporation researchers Martin Libicki, David Sentry and Julia Pollack's book *H4acker5 Wanted: An Examination of the Cybersecurity Labor Market* (Rand Corporation, 2014) examines the confrontation between hackers and their targets from the perspective of a cybersecurity professional with examinations into the economic and political factors, as well as the demand

for cybersecurity labor. *Hacker Culture* by Douglas Thomas, Associate Professor at the Annenberg School for Communication at the University of Southern California, (University of Minnesota Press, 2002), provides a look at the rise of global hacker culture in the 1980s and 1990s. Like most sources on hackers, these sources do not examine China and have become somewhat outdated at the time of writing in spring 2016.

In my quest to find sources of research that is unique from the rest of the field, I also incorporate non-fiction sources as well. In 2015, P.W. Singer and August Cole published the novel *Ghost Fleet: A Novel of the Next World War*, which discusses the future of the very topic that my research incorporates: Chinese cyberwarfare. This type of source adds more diversity, and even though it is a work of fiction it is surrounded with well-informed and accurate information. The two authors worked very hard to provide a strong and accurate portrayal of how the next World War would play out between the United States and China, and the narrative is surrounded by actual developments and technology. Some of the projections of the authors have already come true, which shows the true strength of the research behind the novel.

Probably the most relevant source to this study comes from Scott Henderson, and author who spent over twenty years as a mandarin linguist for various intelligence organizations, titled *The Dark Visitor: Inside the World of Chinese Hackers*.(self-published, 2007). Henderson's work is one of the more significant sources that is devoted entirely to Chinese hackers and Chinese cybercrime. Other sources examine Chinese hackers as a whole, and the

damage that they are doing with each attack. It is perhaps telling that this work is self-published and has seems to have enjoyed a relatively small readership in spite of this subject being so crucial to geopolitics. The individuals and groups Henderson explores are motivated primarily by patriotism and nationalism, which looks at the motivations and differences within the Chinese hacker community. There are several things that set my proposed research apart from Henderson. His work is outdated, and my analysis can incorporate close to a decade of further evaluation. He also only deals with independent patriotic hackers, and not state-sponsored groups.

Methodologies

Beginning this project I realized that it was a daunting task to distinguish thousands of Chinese hackers whose motive might include those of the vigilante, the hobbyist, the state actor, the professional for hire, or a blending of these groups. While some hackers may move from one group to another within their career, or even may span more than one simple category in a single days activity, I have aimed to distinguish the categories, at least, in a way that separates their motivations, styles, and gives a background to why they exist in the forms that they do. This study uses a qualitative approach in an attempt to gain an understanding of underlying reasons, motivations, and insights to access the intricacies of Chinese cyber-attacks and the individuals or groups that carry them out.

Due to the controversial and contentious nature of the subject, I have attempted to provide the research with as neutral a stance as possible in an attempt to provide a valuable window onto these groups that goes deeper than hasty news coverage or biased and incomplete government statements. Both news reports and official statements factor in this study, but I have also incorporated interviews with experts and former hackers, as well as the various new media outlets like blogs and microblogs that are usually the most current and cogent analysis of the latest developments in the Chinese political and social landscape. Sites like *China Digital Times* and *The China Media Project*, for example, include both traditional news reporting, and more urgent and current formats like blogs by leading experts and news aggregation from many varied outlets in China and around the world.

These various forms of research were chosen in order to provide personal, group, national, and global perspectives on cyber-attacks emanating from China. Information was also chosen with special attention paid to the validity of the source. Government response and publications, as well as statistical-driven reports by cyber-security organizations are shown to be extremely valid and important to the research. Personal accounts are used to strengthen these other forms of research.

Due to the qualitative approach of the research, I attempted to establish as much focused information collection as possible. The methods of data collection come in the form of existing surveys, questionnaires, government publications, interviews, and secondary research. These existing forms of

information are taken from cyber-security experts and professional organizations with strong insights into global cyber-attacks. Government publications are taken from existing US, Chinese, and UN documents with careful analysis and consideration, in an attempt to provide an overall neutral perspective of the discourse on this subject.

Examples of surveys in sampling include the Center for Social Development Chinese Academy of Social Sciences' "Surveying Internet Usage and its Impact in Seven Chinese Cities." An example of an existing interview includes China Educational Television's interview of Sharp Winner, HackRead's interview of 7zi, and *Time Magazine*'s interview of Wan Tao. All of these individuals and sources will be thoroughly explained below. This study explores the nascent world of existing cyber-crime legislation both at a national level as well as an international level in an attempt to hypothesize the scope, awareness, and possible futures of cyber-attacks and cyber-warfare. Government publications used in this sampling include the UN's *Convention on Cybercrime*, or the European Commission's *Report from the Commission: First Report on the Implementation of the Data Protection Directive*, and more importantly the PLA's *The Science of Military Strategy.*

Also included are new interviews with cyber-security experts and individuals within the hacking world. I conducted these new interviews mainly through digital communications as opposed to phone, which allowed the interview . This new information provides new insights, never before published, on the topics of hacking, cyber-attacks, and the Chinese hacking community.

Individuals were specially chosen based on their previous work and research, which established their authority on the subject. Their work and research are specific to Chinese cyber-attacks, Chinese hackers, or a related field. The interview subjects include a Bosnian journalist who spent significant time working with the hacking group Anonymous Serbia, the founder of HackRead who himself is an expert in the field, and the Vice President of Cyber Security with the organization Masergy. I questioned them on topics pertaining directly to their field, whether that be cyber-attacks, the role of government in perpetrating these attacks, or the types of tools used in common attacks.

This research constitutes both original research into primary resources, government documents, blogs, news reports and others, as well as being an aggregation of many deeply biased primary and secondary sources, taking them each at face value and evaluating their veracity and value. Many previous analyses of Chinese cyber-crime have been agenda-driven works that aim to assign guilt, often in a hasty way, most notably linking all Chinese cybercrime to the Chinese state.

Goal of Research

The goal of the research was to provide a deeper and more even-handed representation of the Chinese hacking world in recent years, to understand the historical roots and antecedents of the movement, and to cut through the propaganda and disingenuous characterizations from nearly all of the loudest voices in this world. The broadest conclusion of this research has been to

delineate various groups in the Chinese hacking world into the categories of independent, state-sponsored, and freelance. The findings of this study indicate that there are distinct differences between the three categories of Chinese hackers, and that these groups have fundamentally differing motivations and goals. I have found that it is possible to distinguish independent actors and state-sponsored groups through the evaluation of targets of attack, types of attack, and means of attack. This study has found that cyber-crime motivations, perpetration, and tools are predictive based on group motivations and trends. The research and information is analyzed from several perspectives (US, China, and each of the three categories of hacker) in order to keep the unbiased nature of the findings intact, but also to provide a top-down and bottom-up perspective of the field.

Limitations of the Study

There are several limitations and challenges that had to be addressed and overcome throughout the course of research accumulation, analysis, and writing. The most significant was the language barrier between English and Chinese. In order to overcome this, a variety of tools were used. Several native Chinese speakers assisted in the project as translators and sometimes simple digital translating tools were used to obtain a rough translations that was later refined with the help of native speakers. Also, news outlets like *China Digital Times*, *China Media Project*, *The People's Daily*, *Xinhua*, and others consistently reprint English translations of prominent Chinese news items. Another issue was that of

western- or US-bias in source material and the author's background, which was overcome through the use of statistic-driven research and careful analysis and parsing of sources. The last issue included that of the secluded and anonymous aspects of Chinese hacking culture, which made individual contact very difficult. Pre-existing and published interviews, as well as a more global search for interviews performed on my behalf, were employed. This provided both a Chinese and a global outlook on the topic.

My proposed field of study also includes Chinese social movements, as hacker groups are naturally founded and fueled by surrounding social and political changes. This field is significantly larger. A few social movements and cultural trends that are particularly relevant to Chinese hackers are the Chinese democracy and activist movements throughout the 1990s, the recent netizen movement (based on freedom of expression), the revivals of Confucianism and Marxism, and Chinese nationalism and patriotism. While each of these have entire fields of research themselves, my research will narrow down these movements to linked motivations and effects that each movement had on China's hackers and hacker culture. There are several works in the field that can greatly aid my research. Kevin O'Brien's *Popular Protest in China* (Harvard University Press, 2008) has chapters outlining student movements and contention in cyberspace. In *China's Future: The Path to Prosperity and Peace* (Enrich Professional Publishing, 2013), Jim Canrong illustrates the changing ideologies that underline Chinese culture. He describes and analyzes the cultural changes over the last two decades, which sheds light on the background of Chinese social

change. Works like these are essential in the understanding of the Chinese individual and their choices to join hacker groups, which is what is missing today from the field.

When one analyzes the research that others have done on the topic of Chinese cybercrime and the culture of hackers within China, there is a single resounding opinion that tends to be misleading. Much of the work published on this subject points toward one category of actor as the root of all illegal actions: the Chinese government or a subsidiary. In reality, the government is just one piece of a very large puzzle. There are many organizations that support the claim of government rooted activities, two of which include the *Washington Times* and Mandiant Inc, both of whom have published articles or reports linking cyber-attacks to the PLA. The *Washington Times* argues that there is a significant correlation between the growth of Chinese cyber-intelligence and the attacks on American corporations. In their article "China Investing in Cyberwarfare Superiority," Bill Geerts writes that "they [the Chinese government] have stolen hundreds of billions of dollars of intellectual property from U.S. businesses and continue to commit this theft. The Chinese have now increased their capability to conduct massive attacks and continue to consider this weapon as a primary tool in their arsenal."[9] This is a great example of western media biases, as publications like the *Washington Times* have a propensity to attribute all cyber-attacks that emanate from Asia to the Chinese government regardless of the

[9] Gertz, Bill. "Cheers to Good Frenemies! China Investing in Cyberwarfare Superiority." *The Washington Times*. April 1, 2015. Accessed March 28, 2016. http://www.washingtontimes.com/news/2015/apr/1/china-invests-cyberwarfare-compete-us-military/?page=all

complexities of the Chinese hacking community.

Many media outlets, like the *Washington Times* for example*,* have a tendency to fuel debate for sensational reasons, and global cybercrime is no different. A simple story of the Chinese government running a nefarious and well-coordinated ring of cybercriminals will perhaps draw in readers for whom this story validates a worldview. In reality, the individuals responsible are not always state-sponsored, but usually have a broad spectrum of motivations. One key element that sets the Chinese hacker culture apart from the stereotypical western hacker is the deep-rooted nationalism of so many Chinese hackers. This can be seen throughout times of political conflict with other countries, as individuals and hacker groups become especially active. This is an aspect that my preliminary research has found is not commonly covered by the media and other academics.

There is support for the research, but finding work that gives a modern collective view of the field is extremely difficult. One of the few academic texts written on the subject of Chinese hackers and nationalism is Henderson's *The Dark Visitor.* It is one of the few and only books devoted exclusively to this topic. Henderson's text was published in 2007, and provides he no follow-up. This is much the case with this field of study. Much of the information becomes outdated quickly because motivations, the relevant technology, and the nature of attacks change dramatically. This can be attributed to the growth and fluidity of the subject base, as well as a language barrier for most western academics.

Since 2006, the spotlight has been increasingly focused on cyberattacks and what some consider an escalating cyberwar. Research that links China to

global attacks has an origin around this time. Some of the first information published was on the Red Hacker Alliance which started as an online protest movement by activists. The research for this study extends to our era, when online activism in China first found its voice.

One of the most common counter-arguments emanating from Chinese sources is that the United States is in fact the greatest perpetrator of cyber-espionage and cyber-attacks. In an interview performed by myself with a former member of Anonymous Serbia, the individual stated that “At this point, it's certain that ALL governments, including USA and China, are using hackers in order to gain an advantage over other countries. This goes not only in intelligence gathering but probably often as part of the effort to destabilise the economy of others.”[10] The most significant agencies within the U.S. are the FBI, the NSA, and the CIA. The United States has multiple agencies that have internet-based resources and cyber capabilities. The Federal Bureau of Investigation (FBI) runs an Internet surveillance program called Carnivore that allows U.S. officials the ability to intercept and collect electronic communications. The National Security Agency (NSA) was established in 1952 to act as a focal point for Signals Intelligence (SIGINT) and Communications Security (COMSEC), with sub-divisions in Communications Intelligence (COMINT) and Electronics Intelligence (ELINT).[11] Communications signals are collected by the NSA around the world, processes, and if deemed necessary, are given to other agencies like the CIA

[10] Uzunovic, Agan. “Chinese Hackers.” E-mail interview by author. April 5, 2016
[11] Janczewski, Lech, and Andrew M. Colarik. *Cyber Warfare and Cyber Terrorism*. Hershey: Information Science Reference, 2008. P. 459

and the DIA (Defense Intelligence Agency).

One of the most proligic government agencies with cyber capabilities in the NSA. Director of the NSA, General Lew Allen, gave a public overview of the responsibilities of the NSA as “directing foreign intelligence, obtained from foreign electrical communications… foreign intelligence derived from these signals is then reported to various agencies of the government in response to their approved requirements for foreign intelligence.”[12] The agency itself is not devoted entirely to cyber-warfare, but it does have sub-divisions that have mastered the cyber-landscape. The TAO unit (Tailored Access Operations) is one of these groups, and is commonly deployed for specific targets, to hack difficult systems, tap cellular phone networks, or to implant surveillance devices.[13] The NSA has another similar group called the Red Team. Its main component was probing for vulnerabilities in new hardware and software that had been designed for the Defense Department. The *People Daily* published an article in response to the cyber-capabilities of the American government and military in which it is proclaimed that:

> Western hostile forces… use the network, and relying on computers, mobile phones and other such information terminals, maliciously attack our Party, … arouse mistaken thinking trends of historical nihilism, with the ultimate goal of using “universal values” to mislead us, using

[12] Janczewski, Lech, and Andrew M. Colarik. *Cyber Warfare and Cyber Terrorism*. Hershey: Information Science Reference, 2008. P. 460

[13] Wexler, Evan, and Elias Mallette. "How the NSA’s Secret Elite Hacking Unit Works." *PBS*. May 29, 2014. Accessed January 19, 2016. http://www.pbs.org/wgbh/frontline/article/how-the-nsas-secret-elite-hacking-unit-works/

> "constitutional democracy" to throw us into turmoil, use "colour revolutions" to overthrow us, use negative public opinion and rumours to oppose us, and use "de-partification and depoliticization of the military" to upset us.[14]

Outside the United States, countries like Russia and Iran also dominate the cyber-landscape. While Russia's cyber-capabilities are far behind the United States, they are a trailblazer in the area of cyberwarfare. In 1999, the Russian nation-state was charged with hacking the American military network in what is now known as Moonlight Maze. Kevin Mandia, who later went on to start the security company Mandiant, was sent by the American government to interview individuals in Moscow. While there he concluded that "the Russian government had been the hacker, working through servers of the academy of sciences."[15] While in Russia, political hackers strongly showed their skill in assaulting and immobilizing the communication of Estonia in 2007, as well as in Georgia in 2008. During a time of armed conflict in 2008, at the precise moment when tanks and planes crossed the South Ossetian Line, fifty-four Georgian websites-related to mass media, finance, government ministries, police, and armed forces-were hacked and, along with the nation's entire internet service rerouted to Russian servers, which shut them down.[16] Speaking to student cadets in September 2010 in Orebburg, the Russian president bluntly stated, "the

---

[14] Cindy. "Re-Defining Cyberspace - China Digital Times (CDT)." China Digital Times (CDT). October 09, 2015. Accessed May 01, 2016. http://chinadigitaltimes.net/2015/10/re-defining-cyberspace/.

15 Kaplan, Fred M. Dark Territory: The Secret History of Cyber War. New York, NY: Simon and Schuster, 2016. P. 87

[16] Kaplan, Fred M. Dark Territory: The Secret History of Cyber War. New York, NY: Simon and Schuster, 2016. P.164

computer today is now no less important of a weapon than an automatic weapon or a tank."[17]

Iranian hackers have also shown significant hacking talent. Google CEP Eric Schmidt indicated that "Iranians are unusually talented in cyber war for some reason we don't fully understand".[18] Iran is now considered an emerging military power in the field. US Secretary of Defense Leon Panetta warned that Iran has "undertaken a concerted effort to use cyberspace to its advantage".[19] Iran was reported in 2013 to have hacked U.S. Navy computers, in one of the most serious infiltrations from the Middle East to date.[20]

Outside of state hacking groups, there has been a rise in independent hacking groups. Anonymous, by far, is the most well-known hacktivist association worldwide. The various individuals that make up the group Anonymous are unified by the conviction that organizations and administrations they deem corrupt should be confronted or even assaulted.[21] One example of this is the 2010 campaign "Operation: Payback" (as seen below), which saw the Anonymous group attack MPAA (Motion Picture Association of America) and RIAA (Recording Industry of America) in retaliation for their attacks on the torrent site ThePirateBay. The group its roots from the online image-based bulletin board 4chan, which started in 2003. The title "Anonymous" was inspired by the

[17] "Speech at opening of the first Presidential Cadet Academy," September 1, 2010, http://eng.kremlin.ru/transctipts/865.
[18] Joshi, Shashank. "Iran, the Mossad and the Power of Cyber-warfare – Telegraph Blogs." *The Telegraph*. October 3, 2013. Accessed December 17, 2016.
[19] Ibid
[20] Ibid
[21] "A History of Anonymous." *InfoSec*. InfoSec Institute, October 24, 2011. Accessed March 30, 2016. http://resources.infosecinstitute.com/a-history-of-anonymous/

perceived anonymity in which users were able to communicate and post on 4chan.[22]

Figure 1: Anonymous Video Screenshot and Logo. The logo commonly associated with the hacking group Anonymous.[23] The second picture is a screenshot of one of Anonymous' videos after an ISIS attack on Brussels.[24]

[22] Stanek, Becca. "How Did Anonymous Start? The History Of The Mysterious "Hacktivist" Group Began Quite Some Time Ago." *Bustle*. February 20, 2015. Accessed March 30, 2016. http://www.bustle.com/articles/65444-how-did-anonymous-start-the-history-of-the-mysterious-hacktivist-group-began-quite-some-time-ago

[23] Casserly, Martyn. "Who Is Anonymous? A Short History of Hacktivism." *PC Advisor*. November 18, 2015. Accessed March 30, 2016. http://www.pcadvisor.co.uk/feature/internet/what-is-hacktivism-short-history-anonymous-lulzsec-arab-spring-3414409/

[24] Makortoff, Kayleena. "Anonymous to Fight IS, Bigotry after Brussels." *CNBC*. March 24, 2016. Accessed March 30, 2016. http://www.cnbc.com/2016/03/24/after-brussels-anonymous-to-tackle-isis-and-bigotry.html

Page 1 September 19, 2010

September 19, 2010

Operation:
Payback is a Bitch.

To whom it may concern;

This is to inform you that we, Anonymous, have for the last few days been involved in an Operation called "Payback is a Bitch".

This was begun in retaliation for denial of service attacks perpetrated by AIPLEX against The Pirate Bay's servers on behalf of the RIAA (Recording Industry Association of America) and the MPAA (Motion Pictures Association of America). Anonymous has successfully engaged in its own DDoS against AIPLEX's servers and has expanded its operations against the MPAA and the RIAA, which at the time of writing were also unreachable.

Anonymous is sick and tired of these corporations seeking to control the internet in their pursuit of profit. Anonymous cannot sit by and do nothing while these organizations stifle the spread of ideas and attack those who wish to exercise their rights to share with others. Anonymous will not just watch while others are attacked. Their servers have been shut down and they will remain so for as long as there is no true freedom of information and data. These successful attacks on MPAA and RIAA's servers shall continue. An injury to one is an injury to all.

Anonymous,

We are legion.
We do not forgive.
We do not forget.

Figure 2: Operation Payback Message. The post left by the hacktivist group Anonymous following attacks on the MPAA and the RIAA in retaliation for their actions on the site ThePirateBay.[25]

[25] Wharton, Michael. "Twittocracy, Interactivism, Hacktivism, and Cyber-Anarchy: Cause." *There Is Always a Theory: Politics, Anarchy, Religion, Atheism, and Science*. October 12, 2010. Accessed January 14, 2016. http://www.michaelwharton.co.uk/2010/10/twittocracy-interactivism-hacktivism-cyber-anarchy-cause/

CHAPTER ONE

SHAPING THE FOUNDATIONS

The cultural identity of China has been in a state of flux and even chaos throughout the twentieth century. From the fall of imperial China in 1911, through the warlord era and the Japanese invasion, civil war, Communist victory, famine and the Cultural Revolution, the political changes in China have had a profound impact on the cultural identity of the diverse population of the PRC. Over the last few decades, since the death of Chinese Communist Party Chairman, Mao Zedong in 1976, the identities and cultures of China have shown no sign of slowing their relentless transformation and reinvention. Social movements have helped create and define new forms of Chinese identity. Movements like the democracy and activist movements throughout the 1980s, the Chinese netizen movements, the revival of Confucianism and Maoism, and the creation of new forms of patriotism and nationalism have come together with the aid of technological adaptations to provide the first hacker groups with a new and potentially powerful means to voice their beliefs. The current movements that have helped establish a Chinese online identity also play a very important role in the lives and actions of online activists who make up the hacker world.

Since 1979, social and economic reforms have led to a radical transformation of Chinese society. Individuals are now free to move from one place to another with the loosening of “household registration” (*hukou*) policies. On the other hand, individualization and the power of self-interest over the group has emerged along with these freedoms. Activism and protests that pertain to

forms of individualization and rising self-interest have become increasingly common recently in contrast to the predominantly collective mentality of the Mao years (1949-1976), and, some would argue, the Confucian collective and familial bonds of pre-revolutionary China. Many observers within China bemoan the rise of a greedy and self-centered generation in China, with the lifting of economic restrictions and the implementation of the “One-Child Policy” also as factors in possibly fostering a generation of self-interested and materialistic young people in China. But individualization can also be a strong and beneficial social force that allows people to identify their specific needs and interests, and then organize socially and politically in a way that favors their sub-group. Examining the *hukou* system, a household registration system that also records social categorizations, and social circles in Beijing, the analysis examines the individualization and in a sense, the atomization, of contemporary Chinese society. Farmers are protesting against local government; migrant workers are fighting for a decent salary; activist organizations are fighting for protection of the environment; and women are fighting for equality. The rise in these sub-groups has fueled a growing culture of individualization where individuals in these groups are fighting for cultural acceptance, concrete economic gain, and social equality.

As China moves further into the twenty-first century, social activism is flourishing, with an increased number of social movements. Many of these social movements in China are still at a nascent stage, and here is something really new: a generation of younger China scholars that are beginning to explore the richness of China’s emerging culture of contention with new tools at their

disposal.

Since the early 1990s, there has been a constant rise in the reporting of social unrest in China. Reported incidents of social unrest rose from 8,700 in 1994, to 90,000 by 2006, and by 2008 to 127,000.[26] Even before the Tiananmen massacre of June 4, 1989, tensions between the Chinese Communist Party and individuals and groups within Chinese society had been escalating for decades. Even now, in the view of many observers, there is a growing divide between a dynamic economy and vibrant society, and a repressive, archaic system of governance and political control. These recent changes in the 1990s have been hopefully labeled by some as the development of "grassroots democracy." According to Huang Weiping and Chen Jiaxi of Shenzhen University, "from village elections, China's grassroots democracy has undergone a multidimensional expansion, i.e. from the village to the city, from grassroots society to grassroots government, from outside of the ruling party to within the party, and from democratic election to democratic governance. This tendency indicates the growth of China's grassroots democracy in terms of width and depth. China's democratization is in steady progress and is gradually realizing the legitimate political rights of citizens and CPC members in the written laws."[27] The optimism of Huang and Chen is considerable, and it is also noteworthy that they are dating these new developments and this social ferment to precisely the era in which the hackers that I am studying are coming of age and taking part in

[26] Baum, *Systematic Stresses and Choices: China's Road to Soft Authoritarian Reform.* 2004
[27] Weiping, Huang, and Chen Jiaxi. "China's Grassroots Democracy: Development and Assessment." *International Journal of China Studies.* 2.2 (2011): 177-211. *ics.um.edu.my/images/ics/IJCSV2N2/IJCSV2N2-huangchen.pdf*

their society as adults.

The individuals that comprise of the “Tiananmen generation” are involved in this new upsurge in political and social action. The knowledge and lessons learned from the events in 1989 have provided a new collective identity as a new political generation. This generation has an awareness of a movement that was repressed and crushed by its own government, and it assists in maintaining an intensity of public involvement even amidst the cynicism, wariness, or fury. These lessons influence modern activist positions as environmentalists and conservationists, human rights campaigners, and advocates of written law. The circumstances that contributed to the ascension to the modern civilian activism help illuminate the importance of the early movement to further a cause for democracy. The rise of the middle class, the advent of the internet and steadily increasing access, globalization, the maturing of a newer generation, and other factors have all combined to shape recent Chinese activism.

The Fight for Democracy

Struggles for democracy in China have taken many divergent forms, and emerge from the twentieth century and tumultuous eras like the May Fourth Movement and the Cultural Revolution. But calls for democracy returned to the forefront of Chinese culture with the events of the 1980s leading to the world-famous Tiananmen Square protests in 1989. This popular movement paradoxically marked both the high-water mark of democratic movements and optimism in modern China but also its low point. The military crackdown on June

4th shattered these democratic ideals.

The reason that the push for democracy and the outlying movements in the 1990s are so significant is that it has led to many of the issues and movements of today, and in turn fuels the actions of Chinese activists. China has quickly revolutionized into a market economy since 1979. In the wave of the blatant repression of 1989, Communist Party leader Deng Xiaoping set in motion the reform agendas of 1992, but at severe costs. The compromise of forestalling political reform for the sake of astounding economic growth has been a bargain many in China have accepted, though not without some opposition. As China sustains impressive amounts of economic development, the country encounters environmental degradation, corruption, and social polarization. For example, in 2010 the price of ecological dilapidation in China was about $230 billion USD, and since taking office in 2012, President Xi has vowed to bring down both "tigers and flies" in his anti-corruption campaign, going after both top administrators as well low-level officials.[28] This purge of corrupt officers and administrators like Shanghai vice mayor Ai Baojun, who supervised an important economic district, as well as a senior CCP official from Beijing named Lu Xiwen.[29] The prevalence of corruption has long been a source of deep frustration among Chinese activists, and indeed this was a major pillar of the Tiananmen protests.

---

[28] Wong, Edward. "Cost of Environmental Damage in China Growing Rapidly Amid Industrialization." *The New York Times*. 2013. Accessed February 1, 2016. http://www.nytimes.com/2013/03/30/world/asia/cost-of-environmental-degradation-in-china-is-growing.html?_r=0

[29] HernÁndez, Javier C. "China Corruption Fight Extends to Top Officials in Beijing and Shanghai." *The New York Times*. 2015. March 28, 2016. http://www.nytimes.com/2015/11/12/world/asia/china-crackdown-corruption-beijing-shanghai-ai-baojun-lu-xiwen.html

Today, an upsurge of protests and social activism is spreading through China. Compared to the incident in 1989, these new protests are more diverse, often more clearly and narrowly defined, and generally more moderate. New problems have moved to the forefront, encompassing everything from the before mentioned environmental protection, to the protection of ostracized social classifies, to legal reform, and anti-discrimination. To this day liberty and equality are still motivating principles, but protesters and advocates are not using the same outright and confrontational tactics of massive and coordinated protest, as was seen in 1989, and also in the Jasmine Revolution that swept across Arab countries in 2011.

Many of these new movements in China use the law in their struggle to protect citizen's rights. They also have adopted non-combative methods of engagement, and make clever manipulation of the internet to construct a solid foundation for their organizations. In January 2013, Hong Kong professor Benny Tai suggested the "Occupy Central with Love and Peace" effort, in an attempt to compel the government to endow unadulterated democracy to Hong Kong in arrangement with quasi-constitution that existed in Hong Kong.[30] In response in June 2014, approximately 800,000 Hong Kong citizens voted in approval of democracy in an unsanctioned vote prepared by the same effort that Benny suggested. The next month, approximately 500,000 individuals paraded for democracy in a movement that continued through the end of the year. This is a unique movement in a unique or "special" autonomous region of China. Hong

[30] "World Report 2015: China." *Human Rights Watch*. 2015. Accessed September 30, 2016. https://www.hrw.org/world-report/2015/country-chapters/china-and-tibet

Kong's urban protests have not spilled into the mainland, but surely they were noticed by many there.[31]

China and the Internet

The greatest form of political action amongst the newest generation in China is almost certainly online activism. In this modern era dominated by the internet, Chinese activists are both structured but also spread out, but there is no question that they comprise a formidable potential force of social change. However, online activism is predominantly conversational and representational, comprising written objections in virtual forums, as well as websites dedicated to protest movements and online petitions. Despite government censorship of cyberspace, the more powerful of these cultural ideals disperse online at incredible speeds, which in turn can become unofficial national media events. The quickness and simplicity of the internet make it an efficient medium for the expression of criticisms, challenging authority, and expressing dissent.

The growth of the internet as well as the explosion of the reliance on mobile devices has helped facilitate popular activism all over the globe. Thanks to the internet and social networks, young Chinese born in the 1990s were born into a culture that has the potential to learn about the values of democracy, freedom, and human rights, even if they do not necessarily share American perspectives on these concepts. In Shifang, a county-level city in Sichuan, China, students testify that they frequently elude government internet restrictions in

[31] "World Report 2015: China." *Human Rights Watch*. 2015. Accessed September 30, 2016. https://www.hrw.org/world-report/2015/country-chapters/china-and-tibet

order to access sites that are barred.[32] They refer to this as “jumping the wall”, and by “jumping the wall” they mean the Great Fire Wall, which is a country wide program used to sensor the internet in China. China established internet connectivity in 1994, and it now boasts the greatest number of internet users on Earth. A critical influence in the growth and expansion of the internet in China is that it fulfills imperative social desires including the need for information and communication.

The writer of *Chinese Hacker History/Looking Back on the Chinese Hacker History,* Chu Tianbi, states that hacking in China commenced in 1994 as the citizens first became users of the internet, even if overall internet use was mainly restricted to “science and technology research personnel” and “rich young people.” [33] Operators functioned on 9,600-bit/second modems and connected straight into Bulletin Board System (BBS) servers.[34] In term of internet access today, the connection speed that these individuals operated on was extremely slow. As Chinese users were introduced to new computer programs, they started to decipher them practically instantaneously due to their enthrallment. It would not be until 1995 that users in China would be able to experience proficient internet service, as some area around mid-sized cities installed their own internet services and connections. Chu explains this opening stage by asserting: “In their

[32] Hook, Leslie. "China’s Post-90 Generation Make Their Mark " *Financial Times*. July 9, 2012. Accessed August 29, 2015. http://www.ft.com/cms/s/0/4fcbab6c-c67d-11e1-963a-00144feabdc0.html#axzz47NCEKi9b
[33] Tianbi, Chu “Chinese Hacker History/Looking Back on Chinese Hacker History,” *Blog China News.* August 9, 2005. http://www.blogchina.com/news/source/310.htm
[34] Ibid

view, moving from BBS to the Internet was an expansion of their stage and allowed them to see a bit more."[35]

Ever since this opening of the internet landscape like Chu describes, internet use in the country has been increasing at a remarkable speed. The expert on data associated with the Internet in China, the China Internet Network Information Center, released a publication in 2009 demonstrating that the country had achieved 298 million online users by the end of the previous year, with an unparalleled 279 million broadband operators.[36] Both of these combined made China at the time, the greatest consumer of the internet.

A publication named "Surveying Internet Usage and Impact in Seven Chinese Cities" created by the Research Center for Social Development, provides an assessment of the internet in China in which research was performed by means of door-to-door interviews throughout the seven most populated cities within the country in an attempt to explore the consumption of the internet.[37] This examination demonstrates that online users in China are extraordinarily young. For example, the percentage of implementation for individuals 24 and younger is over 80 percent. For the adoption rate is between 60 and 80 percent of those users are between the ages of 25 and 29. That means adoption rate for individuals under the age of 30 is extremely high, and that the bulk of people under this age are internet operators. The highest internet

[35] Tianbi, Chu "Chinese Hacker History/Looking Back on Chinese Hacker History," *Blog China News.* August 9, 2005. http://www.blogchina.com/news/source/310.htm
[36] "Chinese Censorship and China's Online Netizens Social Movements." *Visions of Travel*. 2005. Accessed December 21, 2015. http://www.visionsoftravel.org/chinese-censorship-china-online-netizens-social-movement/
[37] Liang, Guo, and Markle Corporation. "Surveying Internet Usage and Its Impact in Seven Chinese Cities." *Center for Social Development Chinese Academy of Social Sciences.* 2007. Accessed January 17, 2016. http://www.policyarchive.org/handle/10207/16013

adoption rate belongs to males (57.2 percent), those who are in secondary education (90 percent), and single (77.2 percent).[38]

In recent years there has also been a push to cure what is called in China as internet addiction. According to the article “Breathing is Also an Addiction” by Hu Yong, this “So-called Internet addition refers to the repeated and excessive use of the Internet to the point that is becomes a kind of mental disorder. It can manifest itself as the intense desire to use the Internet repeatedly, and withdrawal symptoms are often observed when Internet use is decreased.”[39] According to Yong, approximately twenty million individuals in the country suffer from a type of internet addiction.[40] It is even reported that the use of electric shock therapy on children have been employed to combat the effects of addiction.

The Chinese government and the general population have always had a very complex relationship with the internet, yet it is within this culture that individuals have grown very technologically knowledgeable due to the government’s censorship of the web and the “Great Firewall” as will be explored below. With the development of the Internet, this contention and improvisation has taken on some new forms. Popular protest began taking place in cyberspace from the earliest days of the internet in China. The first few years of internet diffusion in China saw only scattered reports of internet protests. It was not until

[38] Liang, Guo, and Markle Corporation. "Surveying Internet Usage and Its Impact in Seven Chinese Cities." *Center for Social Development Chinese Academy of Social Sciences.* 2007. Accessed January 17, 2016. http://www.policyarchive.org/handle/10207/16013
[39] Bandurski, David. "China Soul Searches Its Obsession with Internet Addiction." CMP Newswire. May 14, 2009. Accessed May 01, 2016. http://cmp.hku.hk/2009/05/14/1623/.
[40] Ibid

1996, that the internet became a significant forum for social protest, prompting an unprecedented response from the government.

Golden Shield Project (The Great Firewall of China)

In 1998, the Ministry of Public Security of the PRC introduced a multifaceted project christened “the Golden Shield”. The intent was to encourage “the adoption of advanced information and communication technology to strengthen central police control, responsiveness, and crime combating capacity, so as to improve the efficiency and effectiveness of police work.”[41] The endeavor was initiated fully by 2003, demonstrating the potential to obstruct sensitive or banned material by fundamentally inhibiting entrance to webpages containing these types of materials by instantaneously sorting out sites that contain an amalgamation of pre-prescribed keywords.[42] The idea of “internet sovereignty” was formally introduced legally in June 2010.[43] It expands the Party’s assertion of national sovereignty to cyberspace as well, as the country essentially utilizes the right to regulator the stream of information from the internet as it reaches its citizens. This idea of internet sovereignty was once again brought by China to an international discussion during the World Internet Conference in December 2015, which was held in China’s Zhejiang province. It was during this event that President Xi Jingping gave a speech attempting to promote:

---

[41] Walton, Greg. *China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China*. Montréal: Rights & Democracy, 2001. Print.
[42] "Chinese Censorship and China's Online Netizens Social Movements." *Visions of Travel*. 2005. Accessed December 21, 2015. http://www.visionsoftravel.org/chinese-censorship-china-online-netizens-social-movement/
[43] "Internet Sovereignty." CMP Newswire. 2015. Accessed May 01, 2016. http://cmp.hku.hk/2015/09/30/39279/.

> The transformation of the global system of internet governance… [while] respecting each country's right to choose its own internet development path, its own internet management model, its own public policies on the internet, and to participate on an equal basis in the governance of international cyberspace—avoiding cyber-hegemony, and avoiding interference in the internal affairs of other countries.[44]

The idea of the Chinese modern for internet governance expanding is not so far-fetched. Russia has long been an advocate of expansion. Russian authorities have employed the knowledge of Lu Wei, China's internet authority, and Fang Binxing, known as the founder of the Firewall, in an attempt to "draw up plans for a national internet white list... [of] potential exposure to "'pornography, drugs, paedophiles,' – scary words."[45] This seems to show that Russia is embracing the same "internet sovereignty" model that China has in the past, behind a model similar to China's Great Firewall.

"Golden Shield" is widely known in popular media as the "Great Firewall of China." The project essentially targets the online movements of individual operating online systems within China and the rest of the global internet. Dr Lennon Yao-Chung Chang, Assistant Professor and deputy program leader of the criminology program at the University of Hong Kong, described it as being " built not only for political purposes, such as blocking websites or messages

[44] Bandurski, David. "China's Cyber-diplomacy." CMP Newswire. December 21, 2015. Accessed May 01, 2016. http://cmp.hku.hk/2015/12/21/39527/.
[45] Wade, Samuel. "Chinese Cyberchiefs Preach Internet Sovereignty in Moscow - China Digital Times (CDT)." China Digital Times (CDT). April 27, 2016. Accessed May 01, 2016. http://chinadigitaltimes.net/2016/04/chinese-cyberchiefs-preach-internet-sovereignty-moscow/.

relating to anti-government material or, pro-Taiwan and pro-Tibet matters, it was also used to monitor websites and block out those related to criminal activities."[46] During times of the year that are deemed sensitive by authorities, thousands of websites go offline and web servers are shut down. In this sense, the Chinese government's control over the internet involves not only content but also timing.

The various tools of state monitors of the internet include blocking specific search terms, shutting down specific websites, or slowing down connectivity of a user engaged in activity that is deemed unsavory by government censors. You cannot search for any information involving the Tiananmen massacre like the date June 4 for example.**[47]** Equipped with a blacklist of undesirable IP addresses, routers drop all packets destined to block IPs, which could include the address of a sensitive site like the New York Times.[48] As of April 2016, eight of the top twenty-five most heavily visited websites globally are censored in China, and according to the group at Greatfire.org, almost a quarter of the websites monitored by Chinese authorities end up blocked.[49] Take the picture below for example, which shows that the site hrw.org has been blocked by Chinese censors. The individual is denied access to a certain page, because the site itself or the content on that specific page has triggered government censors.

---

[46] Chang, Lennon Yao-chung. *Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention across the Taiwan Strait*. Cheltenham, Glos, UK: Edward Elgar, 2012.
[47] Lynden, Jacki. "In China, Avoiding The 'Great Firewall' Internet Censors." *NPR*. September 7, 2013. Accessed April 11, 2016. http://www.npr.org/templates/story/story.php?storyId=220106496
[48] Xu, Young. "Deconstructing the Great Firewall of China." *Tech in Asia*. ThousandEyes Inc. 8 March 8, 2016. February 7, 2016. https://blog.thousandeyes.com/deconstructing-great-firewall-china/
[49] Cindy. "China Wants Party's Voice "Strongest in Cyberspace" - China Digital Times (CDT)." China Digital Times (CDT). January 08, 2016. Accessed May 02, 2016. http://chinadigitaltimes.net/2016/01/china-wants-partys-voice-strongest-in-cyberspace/.

Figure 3: HRW.org Censorship. The site *hrw.org* has been blocked by government censors. The page shows a message explaining that the page could not be found because of relevant laws and regulations.[50]

Netizen Movement

The new and rapidly transforming culture that has surrounded the citizens of China has provided them with a unique opportunity, and has also allowed the creation of self-realizing sub-groups within the population. The profound diversity

[50] ""Race to the Bottom": Corporate Complicity in Chinese Internet Censorship." *Human Rights Watch* 18, no. 8 (August 2006). Accessed April 11, 2016.

and complexity of China continues to defy the hasty external prejudiced views of a homogeneous society that is completely and utterly oppressed. The internet has been shown to have had a profound effect on these individuals, yet the government has gone to great lengths to censor the information that is accessible. This culture has bred a new generation of individuals who are more familiar with the inner workings of cyberspace as a consequence of the restrictions placed upon them by their superiors. Firewalls, proxy servers, and backdoors are often a necessity for them to view information that would not otherwise be available. This movement is commonly referred to as the "Netizen movement" due to the fact that its individuals are often referred to as netizens, which is an abridgement for "internet citizen." The term "netizen" was coined in a 1992 article by Michael Hauben titled "The Net and Netizens: The Impact the Net Has on People's Lives." and spread rapidly.[51] It is usually designated to individuals who are extremely immersed in cyber communities. Netizens are distinct from normal internet users in that their emphasis is with manipulating cyberspace as an instrument to participate in social activities, using the internet to increase their scope of social influence, and building more connections outside of their normal social circles. The use of the term netizen has now become nearly indistinguishable with Chinese internet users.

Although government restriction has helped create a very unique internet user collective, the government and internet activists can coexist and even cooperate with each other if the circumstances fulfill both groups' ideologies.

[51] Orlowski, Andrew. "Michael Hauben, Netizen, Dies." *The Register*. June 30, 2001. Web. March 28, 2016. http://www.theregister.co.uk/2001/06/30/michael_hauben_netizen_dies/

This is especially true if netizen action contributes to the Chinese government's agenda in any way. A prominent instance of such confluence was centered around the Olympic torch relay as it crossed France in April of 2008, before the Beijing Summer Games of that year. The global community debated the ethics of hosting the Games under the watchful eye of such an authoritarian regime. Tibetan independence advocates and human rights activists continually made an effort to impede the relay of the Olympic torch as it made its way through Paris. Adding more fuel to the fire, the city hall in Paris flew a Tibetan flag and displayed a banner that proclaimed, "Paris defends human rights throughout the world."[52] Furthermore, members of the French Parliament brought a halt to a National Assembly session to reveal a sigil that declared "Respect for Human Rights in China" while chanting "Freedom for Tibet!"[53] The torch was forcibly extinguished five times amidst scuffles along the route, until the torch relay route was shortened and a town hall ceremony cancelled.[54]

In China there was a resounding response that started in the online community and quickly became physical. A chain of boycotts, protests, and assaults on any person or anything that represented France was implemented by thousands and perhaps millions of Chinese individuals. The hardest hit was the French retailer Carrefour, which had over one hundred shops in China at the time. There were countless cries throughout cyberspace to boycott goods and

[52] Glasius, Marlies. *Global Civil Society Yearbook 2009: Poverty and Activism*. London: SAGE Publications, 2009. Print.
[53] Ibid
[54] L'Express, Flamme olympique: ce qui s'est vraiment passé à Paris (French). April 8, 2008. Accessed October 19, 2015. http://www.lexpress.fr/info/quotidien/actu.asp?id=469562

merchandises from the French retailer.[55] An article published online was even labeled , “Boycott French goods, let’s start with Carrefour.”[56] This led to a congregation of approximately one thousand protesters outside a Carrefour store in the city of Wuhan, and it expanded to encompass the rest of China as well. Amidst the protests were accusations that retailer advocated for Tibetan independence and championed the cause of the Dalai Lama. (To be precise, the Dalai Lama does not currently advocate Tibetan independence, but rather increased autonomy and cultural freedom for the region.) It was contended that the episode turned out a public-relations catastrophe for the Chinese government, while some believed that the concentration of the attention that was placed upon the protestors as primarily upholding and portraying a sense of nationalism. The online campaign surrounding this and other related incidents reflected the confluence of popular netizen activism and the state agenda of promoting patriotism and China’s image abroad.

Another form of resistance that is common to the country is online hacktivism and related hacking endeavors, although these are considered highly controversial throughout the rest of the world. A significant example of this that is prevalent in China is government website defacement where a government or state organization’s webpage is hacked and a political message is left for the public’s viewing. In December 2008, the official website for the city’s Bureau of Commerce in Jingzhou was hacked and swapped with a picture of a woman

[55] "China Protests French Retailer Carrefour." *nbcnews.com*. April 19, 2008. Accessed September 2, 2015. http://www.nbcnews.com/id/24218173/ns/world_news-asia_pacific/t/china-protests-french-retailer-carrefour/

[56] "Crisis Management At Carrefour." *EastSouthWestNorth*. April 26, 2008. Accessed September 27, 2015. http://www.zonaeuropa.com/20080428_1.htm

dressed in very revealing attire, with the photograph of the leader of the organization substituted with a statement suggesting immoral behavior on his part. Cases like this have a tendency to be linked to corruption of officials. Various other cases of hackers assaulting webpages in an attempt to stimulate political awareness are very common in media portrayals in today's age. There are other significant examples of this; a Japanese webpage dedicated to the Yasukuni Shrine, where Japanese military personnel that seized China during World War II are being revered, including class A war criminals, was vandalized by a hacker collection out of China.

The People's Republic of China has executed a number of significant suppressions of webpages in China that were purportedly operating contrary to government guidelines. In 2004, two prominent organizations that provide blog services, BlogBus and Blogcn, were restricted to users for the short term due to offensive matter concerning the events in 1989 as well as the 2003 government management of the SARS incident.[57] During 2005, the online crackdown by Chinese authorities escalated as authorities pursued not only the major webpages but, furthermore, the bulletin board systems of significant universities. This suppression led to very aggressive demonstrations in the form of two large student protests against the actions of the authorities.[58][59]

Although it was covered up quickly, one of these demonstrations in 2005

[57] "China Pulls Plug On Internet Blogs." *ChinaTechNews*. Asia Media Network, March 19, 2004. Accessed October 14, 2015. http://www.chinatechnews.com/2004/03/19/1029-china-pulls-plug-on-internet-blogs

[58] "The Great Chinese BBS Crackdown." *EastSouthWestNorth*. Accessed January 14, 2016. http://www.zonaeuropa.com/20050322_2.htm

[59] Pan, Philip P. "Chinese Crack Down On Student Web Sites." *The Washington Post*. March 24, 2005. Accessed September 28, 2015. http://www.washingtonpost.com/wp-dyn/articles/A61334-2005Mar23.html

took place at Tsinghua University and saw over one hundred students come together in protest. The students also requested that the institution resist the government. The school was under pressure by authorities to restrict their internet privileges to only those within the university. This essentially meant that public servers would be shut down. That would have meant that public users, who make important contribution to the conversation, are not able to access these BBS any more.[60] A comparable protest of approximately two hundred individuals took place at Nanjing University. Disapproval of the government's response extended throughout the country with media articles with headings like "Universities Should Not Build Walls Around the Internet."[61]

Nationalism

Nationalism has developed into one of the more significant influences behind group actions, albeit it is a somewhat contemporary trend that followed the birth of the modern countries in Europe in the nineteenth century and then throughout the rest of the world. In *Imagined Communities* by Benedict Anderson, a nation is an "imagined community" that has been socially constructed by individuals who imagine themselves as part of a larger collective.[62] It is this idea of "community" creates a larger sense of nationalism.

---

[60] MacKinnon, Rebecca. "Chinese Protest BBS Crackdown." *RConversation*. March 20, 2005. Accessed March 28, 2016. http://rconversation.blogs.com/rconversation/2005/03/chinese_protest.html

[61] "Chinese Censorship and China's Online Netizens Social Movements." *Visions of Travel*. 2005. Accessed December 21, 2015. http://www.visionsoftravel.org/chinese-censorship-china-online-netizens-social-movement/

[62] Anderson, Benedict R. O'G. *Imagined Communities: Reflections on the Origin and Spread of Nationalism*. London: Verso, 1991. Print.

For some observers, there is much to criticize in China's rush to modernity and global prominence in the past forty years: the crackdown on Tiananmen Square in 1989, the long history of governmental censorship, the brutal eviction of poor residents outside of cities during redevelopment projects, a draconian population policy, cultural chauvinism at China's ethnic frontiers, human rights violations, and much more.

During the first three decades of communist power, Marxist philosophy went hand in hand with nationalism. Since the late 1970s, however, these ideologies have been supplanted by economic principles, and nationalism has become one of the strongest forces that push these ideologies into the more modern era. This was particularly accurate after the 1989 government crackdown on protests in Tiananmen Square and elsewhere. As related to China's youth, nationalism has been a driving force in the developments of both the political and cultural realms of the nation. The internet has provided an entirely new place for individuals to share and build upon nationalist sentiment, especially among the idealistic youth. The summer of 2003 is one example. This was a time that exhibited a rising anti-Japanese sentiment among Chinese youth. Tensions grew out of issues surrounding the disputed Diaoyu or Senkaku islands in the East China Sea, which were a growing tension between the two nations. A popular movement emerged later that year, and escalated into a signed petition of over ten thousand individuals opposing the use of Japanese technology in a high-speed train under development. 2003 also was a significant step forward for online nationalism. Without a doubt, it is this emotion that was replicated to night

precision on a webpage linked to the Red Hacker Alliance (to be examined further below) called *Iron and Blood Union (*tiě ér xuèyè shètuán). The site expressed the standpoint of the group by stating that "The goal of this community: Is to grieve for the prior generation and to never forget the nation's shame; to use history as an example for facing the future."[63]

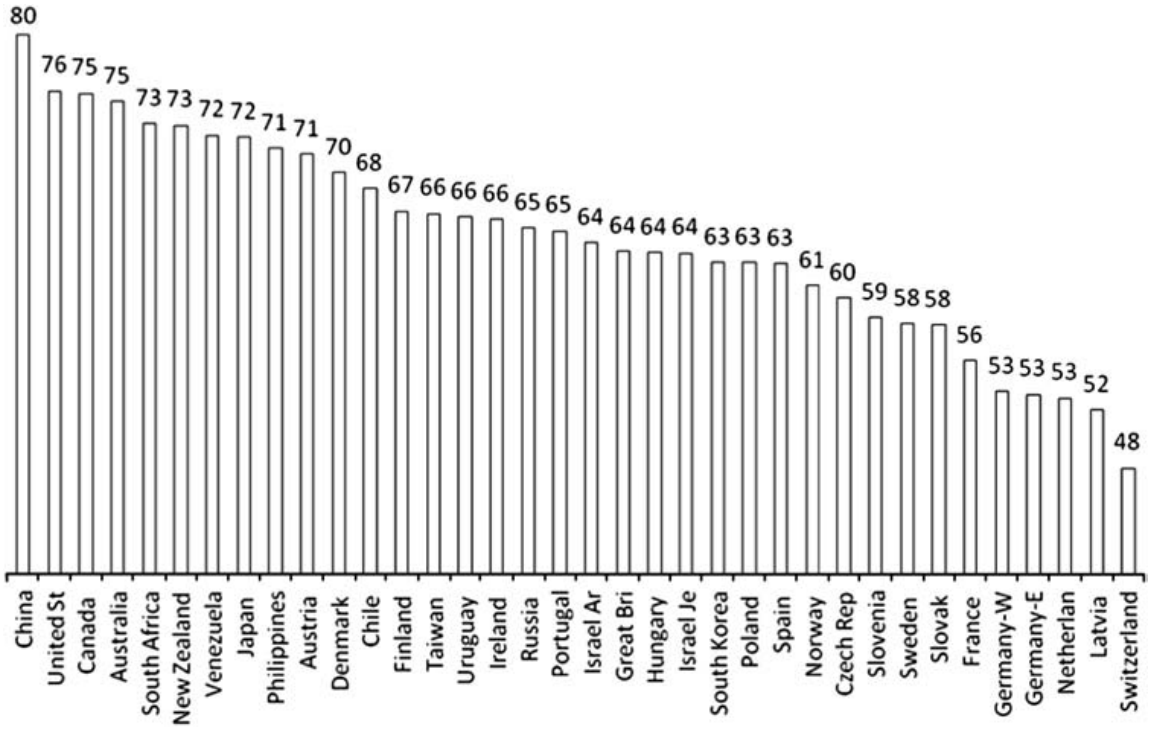

Figure 4: Nationalism: An International Comparison. Note: Nationalism is an imputed factor index of four survey questions. The scale ranges from 0 to 100. Source: National Identity Survey II, International Social Survey Programme, 2003, and 2008 China Survey.

[63] *Iron and Blood* is a military enthusiast site but has links to the Red Hacker Alliance. It is also heavily anti-Japanese. http://www.tiexue.net/

Chinese nationalism and national identity construction have garnered much attention in recent years. Pro-China demonstrations in 2008 during the Olympic torch relay as well as anti-Japanese demonstrations in spring 2005, September 2010, and September 2012, have raised concerns abroad about the nature of Chinese nationalism and national identity. Indeed some observers believe that these protests raise concerns in Beijing about its own ability to control this kind of nationalist sentiment.

Most analysts agree that nationalism is currently a powerful source of legitimacy for the CCP and its hold on power.[64] The figure above represents a National Identity Survey that indexes nationalism of the global community. On a scale from 0 to 100 based on survey questions given to the public, China ranks first with a rating of 80, followed closely by the United States at 76. To further analyze national identity in the country, students at Beijing University (1,346 total) were asked to take part in a survey in spring 2007.[65] This survey found that both Chinese Communist Party supporters and individuals with rural upbringings showed greater levels of nationalism than individuals who did not fall under either category. The Communist party regards students and young people in urban areas as more likely to participate in protest movements over foreign policy issues, which makes this segment of the population “most likely of greatest

[64] Downs and Saunders 1999, 118; Laliberté and Lantegne 2008,
[65] Sinkkonen, Elina. "Nationalism, Patriotism and Foreign Policy Attitudes among Chinese University Students." *The China Quarterly* 216 (2013): 1045-063. Web. http://journals.cambridge.org/action/displayAbstract?fromPage=online&aid=9113316&fileId=S0305741013001094

concern to Chinese leaders."[66] Students have been active in some of the Chinese nationalist movements and other protest movements, but we know little about their unfiltered opinions, perhaps with the exception of those who are active online. It is within recent research like the university survey were it has become evident that Chinese nationalism is a growing phenomenon

This research comes to five conclusions. First, in the Chinese context, nationalism and patriotism are fundamentally distinct, but have a significant effect on those who were interviewed. According to Oxford English dictionary, *nationalism* is defined as a patriotic sentiment; and *patriotism* as a passionate protection of the nation's success and independence from which they identify.[67] Chinese nationalism centers on the idea of returning China to its former greatness prior to the late Qing era and the fall of the imperial system. Patriotism differs from nationalism in China as it usually pertains to individuals with a sense of responsibility to both the nation and the Party. The second conclusion of the research states that nationalism has stronger links with foreign policy predilections than that of patriotism. "Patriots" and "nationalists" differed in their views in all other foreign policy statements except for the statement concerning Taiwan, which indicates that the Taiwan issue seems to unite people with otherwise different views. In the 2007 data, only 6.8 per cent of respondents were against or strongly against the use of force if Taiwan declared

[66] Reilly, James. Strong Society, Smart State: The Rise of Public Opinion in China's Japan Policy. New York: Columbia UP, 2012. P.126.
[67] "Definition of Nationalism in English." Oxford Dictionaries. Web. http://www.oxforddictionaries.com/us/definition/american_english/nationalism

independence.[6869] Third, the answer to the research question of whether Chinese individuals who are more nationalistic differ from less nationalistic Chinese in their foreign policy attitudes is clearly a resounding yes. The political attitudes of Chinese citizens are very much reflective upon their nationalistic qualities. This research has shown that compared to nationalism, patriotism in China is connected with more accommodating and globalized outlooks, whereas the other individuals have a tendency back economic security. Nationalism is usually linked to the idea of a greater "China," while patriotism is linked to the Communist party. It is also true that nationalistic online behavior offers protection in opposition to government enquiry and potential intervention, since it is clearly not undermining the cultural and political authority of the government, at least on the surface. By PRC criteria, this encompasses a significantly sized collection of peoples with shared connections that are hard to supervise and regulate. Within China, a hacking organization could find itself censored, broken up, and even subjected to legal punishment of they become an opposition and do not show support for the PRC or the CCP.

In the world of Chinese hackers, nationalism and patriotism are very similar. Individuals who are labeled "patriotic hackers" usually follow a more nationalistic sense, as in, they are more worried about China as a whole and not so much the Communist party. The term "patriotic" hacker is more common in the

[68] Sinkkonen, Elina. "Nationalism, Patriotism and Foreign Policy Attitudes among Chinese University Students." *The China Quarterly* 216 (2013): 1045-063. Web. http://journals.cambridge.org/action/displayAbstract?fromPage=online&aid=9113316&fileId=S0305741013001094

[69] If Taiwan were to declare independence, 41.2% were strongly in favour of the use of armed force, 35.2% agreed on the use of the army, 16.7% could not decide whether to use armed force or not, 5.3% were against the use of the military, and 1.5% were strongly against the use of armed force.

western work than “nationalistic” hacker. Chinese hackers include both qualities that comprise of nationalism and patriotism.

The growth of the internet as well as the explosion of the reliance on mobile devices has helped facilitate popular activism all over the globe. Thanks to the internet and social networks, young Chinese born in the 1990s were born into a culture that has the potential to learn about the values of democracy, freedom, and human rights. Nationalism has developed into one of the more significant influences behind group actions. In the past, Marxism and government ideologies went hand in hand with nationalism. Even today the government attempts to facilitate nationalistic values. There is a relevant phenomenon called the 50 Cent Party in which the government pays individuals to post fake comments on internet pages to promote the government’s ideologies. These individuals gain their name because these individuals are supposedly paid “50 cents of Renminbi” for every post.[70]

In January 2016, the agency in charge of censorship of the internet in China convened at the National Online Propaganda Work Conference with the focus of specific tasks. According to the People’s Daily, the agency called for a focus on, “deepening online propaganda… so that the theoretical innovations and practical achievements of the Party become the lofty main tone and main theme of the online space,” as well as “fully leveraging websites, online social organisations and internet users, achieving comprehensive [internet]

[70] Sterbenz, Christina. "China Banned The Term '50 Cents' To Stop Discussion Of An Orwellian Propaganda Program." *Business Insider*. October 17, 2014. Accessed April 24, 2016. http://www.businessinsider.com/chinas-50-cent-party-2014-10

management through multiparty execution of policies."[71] This shows that the Party's management of the internet and of its users continue even now, and will continue into the future. Although from a western perspective this sounds incredibly bad, in China and in President Xi Jingping's mind, it is most definitely not. The president calls in "spreading positive energy", and it follows the idea that the country can transform itself it the face of ever-changing public opinion that have been challenged by new technologies.[72] So, there are very good intentions behind the Party's control of the internet as positive energy is intended to contribute the mobilization of the populace behind the party.

[71] Bandurski, David. "A "Year of Innovation" for Internet Controls." CMP Newswire. January 7, 2016. Accessed May 01, 2016. http://cmp.hku.hk/2016/01/07/39575/.
[72] Bandurski, David. "Three Cheers for China's Cyber-Volunteers." CMP Newswire. April 13, 2016. Accessed May 01, 2016. http://cmp.hku.hk/2016/04/13/39684/.

CHAPTER TWO:

WHAT DEFINES THE HACKER CULTURE?

A new culture has developed in China in which some expressions of beliefs can be deemed unacceptable and censored in various forums. These constraints on some kinds of expression on sensitive topics were most obviously apparent in the government's actions in suppressing the 1989 protests, and a powerfully chilling effect has been seen in many forums and venues of public expression. Many who sought to speak their minds on some sensitive topics usually constrained their communication to their immediate social circles. This became the status quo immediately after Tiananmen, and would remain so until the explosion of the internet midway through the 1990s. Then individuals found a new platform and while still circumscribed in some ways, there were efforts to keep the internet as a forum for free expression. This sometimes involved and still involves coded references to sensitive political events (like "May 35" as a reference to June 4, 1989), but creative and savvy efforts have continued to push the limits of expression on the internet within China, beginning in the 1990s. In this regard, one can say that this new Chinese culture led to the creation and growth of a hacker culture, as well as further defining what exactly a hacker culture is on the global scale. Since 1999, online public opinion has gone through three distinct phases: infancy, development, and expansion. These phases begin with the bombing of the Chinese Embassy in Belgrade (more on this later) when the *People's Daily* established forums for public opinion. This phase escalated into yet another in 2003 in what is known as "the year of online public opinion",

where online conviction first swayed government policy. Finally, the country moved into the last phase of independent interpersonal communications, collaboration, and involvement acknowledged as Web 2.0.[73] Throughout these phases a new sub-culture emerged.

The term “hacker” was initially attributed to individuals who can modify computer systems and programs in an attempt to accomplish tasks that were beyond the inherent or intended design of the system.[74] However, as technology advanced and the true power of computer hacking was unleashed, individuals from all walks of life soon discovered the utility of hacking as well as its destructive and criminal capabilities. Hacking now extends to include organized gangs attempting to steal financial information, state-affiliated espionage groups who steal massive amounts of intellectual property, saboteurs and anarchists attempting to destroy critical infrastructures, and other actors. There are also countless small-scale criminals launching attacks for a wide variety of reasons.

Most popular preconceptions about computer hackers reasonably include a criminal view. We should note from the outset, though, that this is no longer the case. Governments and state-sponsored actors, including the United States, China, and many others now employ cybersecurity experts whose duties include not only defense, but also offensive cyber espionage and hacking. There is a large group within the broader hacking community that uses their computer prowess for legal gains.

---

[73] Bandurski, David. "How the Internet Has Changed China." CMP Newswire. October 10, 2010. Accessed May 01, 2016. http://cmp.hku.hk/2010/10/25/8238/.
[74] Hollin, C. “Criminological psychology”. *In The Oxford Handbook of Criminology*, M. Maguire, R. “Morgan, and R. Reiner, Eds. Oxford University Press, Oxford, U.K., 2002.

There is also a youthful shift as new generations are raised in a world where so much of daily life and daily interaction takes place online. Majid Yar, professor of Sociology at the University of Hull, believes that there is a "youth problem" in hacking around the world. Yar attributes two significant factors to the youth movement in hacking, which tends to have an overwhelming male hacker presence as well as being university dropouts in their twenties.[75] Yar points to youth as a stage of unavoidable psychological chaos. This has a tendency to lead to involvement in different types of criminal conduct. He also suggests the "ethical deficit" among these youths that lead them towards illegal behavior. This new generation of computer hackers, raised in a computer-based globalized world, push the boundaries of what is acceptable due to a great variety of motivations. These motivations can potentially make each individual hacker different, but they also help us to broadly classify and understand these individuals.

Hackers are commonly categorized into one of three classes depending on the individual's or group motivations: black hat, white hat, and grey hat hackers. Those who are classified as black hat hackers tend to be the most dangerous. They tend to explore criminal ventures, revenge, sabotage, or illegal financial gain. This financial gain could include the theft of money, products, resources, blueprints or plans, or services. Black hat hackers can vary from beginners just starting to learn their way around systems by distributing malware, which are software programs that are created with the intent to harm or perform

[75] Yar, M. "Computer hacking: Just another case of juvenile delinquency?", *The Howard Journal of Criminal Justice.* 44, 4 (Sept. 2005), 387–399.

further unsolicited activities on a computer system, to skilled professionals with intent to pilfer information.[76] White-hat hackers tend to explore security weaknesses in an attempt to strengthen or develop more secure computer systems, for the sake of industry knowledge and/or for legal financial gain. White hat hackers can be freelancers or employees of businesses as security consultants that are paid to intentionally break into systems to find security issues.[77] Grey hat hackers are the weakest and least dangerous of the three. They explore systems and their weaknesses perhaps out of personal curiosity, to achieve notoriety amongst their immediate social groups, or purely for self-fulfillment. Grey hat hackers usually do not cause harm to their targets, “they’re just looking to get something out of their discoveries for themselves.”[78] According to Peng Yinan, one of China’s most prolific hackers, “Chinese hackers are similar to Western meanings and really nothing more that the three types: black hat hackers (hei maozi), white hat hackers (bai maozi), and grey hat hackers (hui maozi).”[79]

Hackers perform attacks or infiltrate systems for a variety of reasons. These motivations can include testing their skills, gaining recognition, making money, and supporting a political agenda. Some hack alone, and some hack in groups. Modern computer hackers attack or infiltrate systems in a variety of ways. While it is very easy to get lost in the terminology found in the world of

---

[76] Kovacs, Nadia. "What Is the Difference Between Black, White and Grey Hat Hackers?" *What Is the Difference Between Black, White and Grey Hat Hackers?* April 17, 2015. Accessed November 16, 2016. http://www.howtogeek.com/157460/hacker-hat-colors-explained-black-hats-white-hats-and-gray-hats/

[77] Ibid

[78] Ibid

[79] Hagestad, William. *Chinese Cyber Crime: China's Hacking Underworld*. San Bernardino, 2015.

hacking, there are a few significant types of attacks that are common and for the sake of this study, they should be sketched out in brief: phishing/malware, SQL injection, DDOS, insider threat/theft, and vulnerability exploits. The figure below shows the attack cycle that is most common, with cyber-attacks starting with defining the target and ending with covering up tracks.

Figure 5: Advanced Persistent Threat Lifecycle.[80]

[80] Casaretto, John. "Advanced_persistent_threat_lifecycle." *SiliconANGLE*. July 17, 2013. Accessed March 28, 2016. https://conceptdraw.com/a2051c3/preview

Table 1: Common Types of Hacking Attacks

Type of Attack	Definition
Phishing	This is a form of deception where the assailant attempts to gather personal information like login identifications, or identity information through email, instant messages, and other channels. Often times the attacker uses reputable names or fraudulent claims to attract individuals into initiating communication.
Malware	These are software programs designed to damage, freeze, or perform any other unwanted actions without the knowledge of the user. Common examples include viruses, spyware, and "Trojan horses." A Trojan horse program is usually malevolent/destructive in nature and commonly concealed inside another program or downloadable data.
SQL Injection (Structured Query Language)	This is a form of security exploit in which the systems infiltrator adds SQL code in an attempt to obtain entrance to information or resources, or to make system changes. This type of attack allows the attacker to gain access to information systems through automated tools, which increases the scope and overall damage to computer systems.
DDoS (Distributed denial-of-service)	A DDoS strike is when a variety of systems assault a lone objective. Essentially, a flood of messages force the system to shut down, resulting in a rejection of access for the ordinary operators of the besieged system. The types of DDoS attacks are when an attack over encumbers the server by expending all the allotted bandwidth through a network-centric assault, and a program-based strike that overburdens a system by initiating applications.
Insider Threat and Theft	This is a malicious hacker who

	can physically access the information systems of a business, institution, or agency. Insider threats are often disgruntled employees or ex-employees that are seeking revenge or financial gain. A recent example of this is the Edward Snowden NSA case. Snowden physically walked in with a flash drive, and walked out with classified information.
Vulnerability exploit	These also include zero-day exploits, and take advantage of security vulnerability as they are discovered. These include installing malware, spyware, or just allowing unwanted access to information. In the case of zero-day exploits, since the vulnerability is not known in advance, there is no way to guard against the exploitation before it happens. Zero-day vulnerabilities are the holy grail of modern hacking tools.

Responses to Cyber-Attacks

Defense was the predominant approach to internet security during the internet's earliest days. The basic idea was to secure a network with systems that could prevent intrusion, such as firewalls, for example. These systems were created with the ability to keep logs of suspicious codes, as well as the ability to detect suspicious patterns. They would continually be updated so as to keep up with newly emerging threats. One related issue was that this system depended heavily on a user's ability to personally update antivirus software. According to Tom Kellerman, vice-president of the U.S. security firm Trend Micro, "You keep the crown jewels on the inside, and you build electronic walls and a moat around

them."[81] This strategy only works well if the attacks are from small-scale hackers, whose attacks are scattered and random. These individuals are simply attempting to find an easy way in, and as they hit obstructions, they generally move on to the next target.

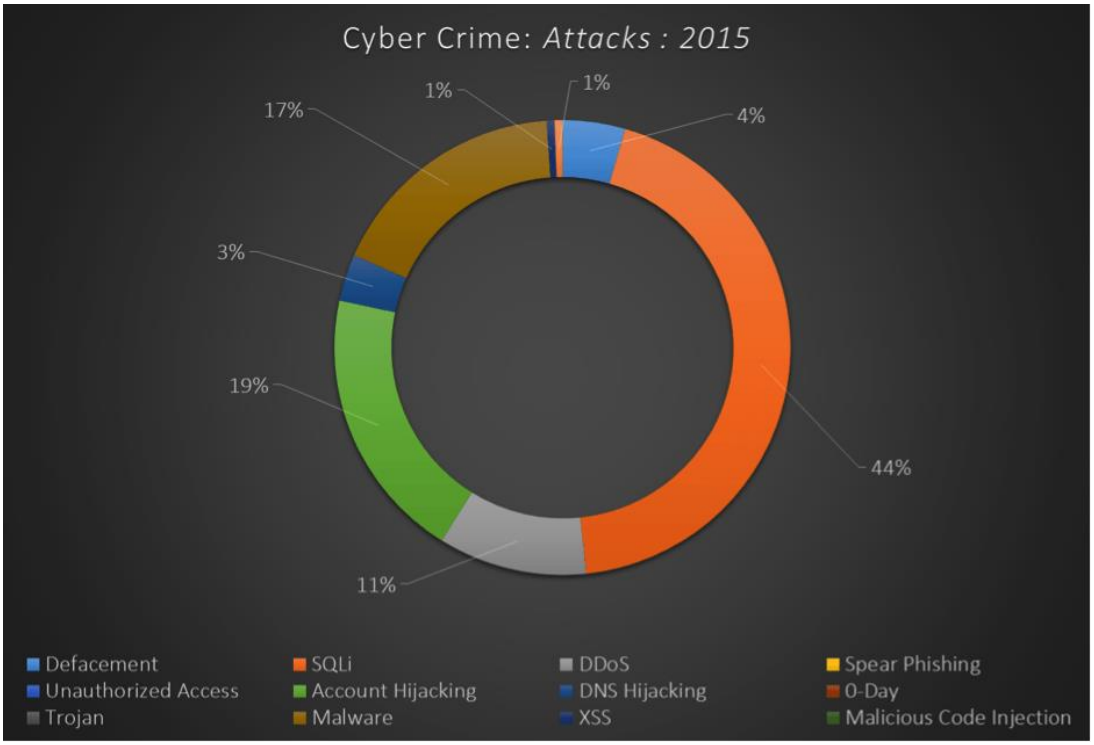

Figure 6: Types of Cyber Crime Attacks in 2015. [82]

[81] Seabrook, John. "Network Insecurity." *The New Yorker*. 20 May 20, 2013. Accessed March 28, 2016. http://www.newyorker.com/magazine/2013/05/20/network-insecurity
[82] "Biggest Data Breaches." *Privacy Risks Advisors*. 2015. Accessed January 2, 2016. http://www.privacyrisksadvisors.com/data-breach-toolkit/worlds-biggest-data-breaches/

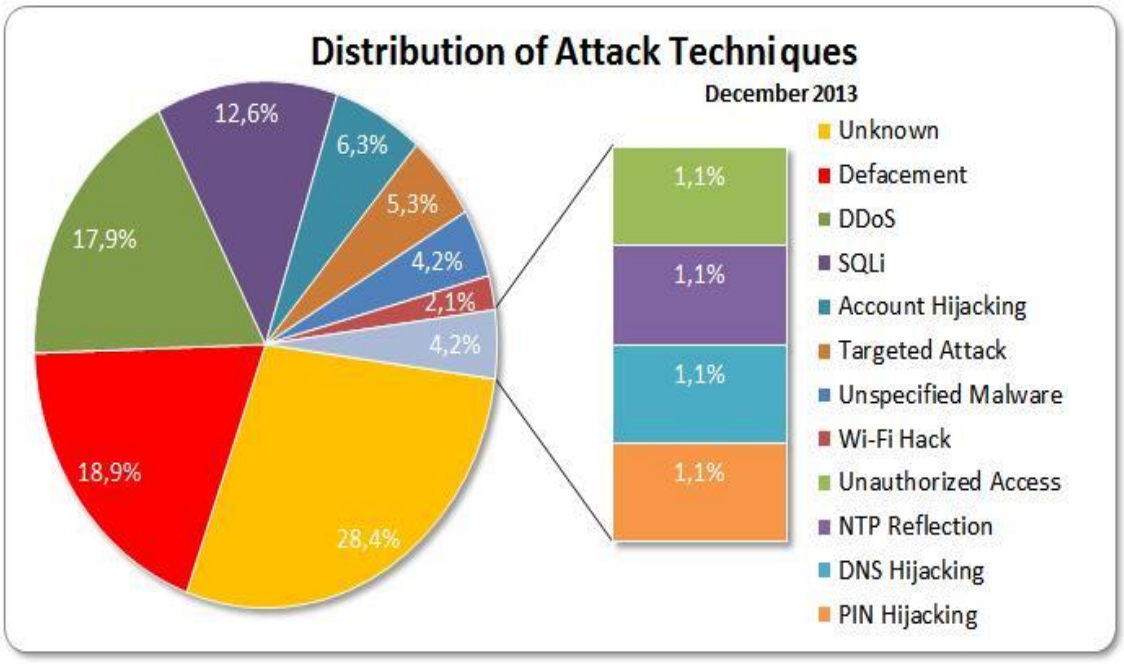

Figure 7: Types of Attacks in December 2013.[83]

However, in recent years these types of security systems are failing to stop the more aggressive actors who are making the most of the technological advancements of the modern era. There has been a rise in what is known as "targeted attacks," where an attacker invades a specific organization, agency, or individual. These individuals or groups usually also have a specific goal or system in mind prior to the attack and are not randomly looking for vulnerabilities. No individual or network is completely safe from these hacks, as has been demonstrated on numerous occasions, and any given person can be the target of a hacker's attack. Any system can be tainted just by merely opening a communication or visiting the incorrect site. "Up until four years ago, we kind of

[83] "Biggest Data Breaches." *Privacy Risks Advisors*. 2015. Accessed January 2, 2016. http://www.privacyrisksadvisors.com/data-breach-toolkit/worlds-biggest-data-breaches/

had a handle on this shit," Tom Kellermann said in 2013. "Virus scanning and encryption and firewalls were doing a pretty good job. But the latest attack kits are bypassing those perimeter defenses, which is why this paradigm has to shift."[84]

The eruption of hacking is a natural outcome of progress in the networking tools that has grown around the internet, as well as by the widespread operation of computers all around the globe. The online systems of the better part of contemporary are all in danger of being destroyed or pillaged from outside threats, and we are frequently reminded of this when news breaks of another high-profile hack or leak. One group alone from China, codenamed APT1 (Advanced Persistent Threat 1), has methodically appropriated hundreds of terabytes of information from at least one hundred and forty one establishments, and have proven that they have the ability and goal of taking from a great amount of individuals and establishments instantaneously.[85]

[84] Seabrook, John. "Network Insecurity." *The New Yorker*. 20 May 20, 2013. Accessed March 28, 2016. http://www.newyorker.com/magazine/2013/05/20/network-insecurity
[85] Kaplan, Fred M. *Dark Territory: The Secret History of Cyber War*. 2016. Print.

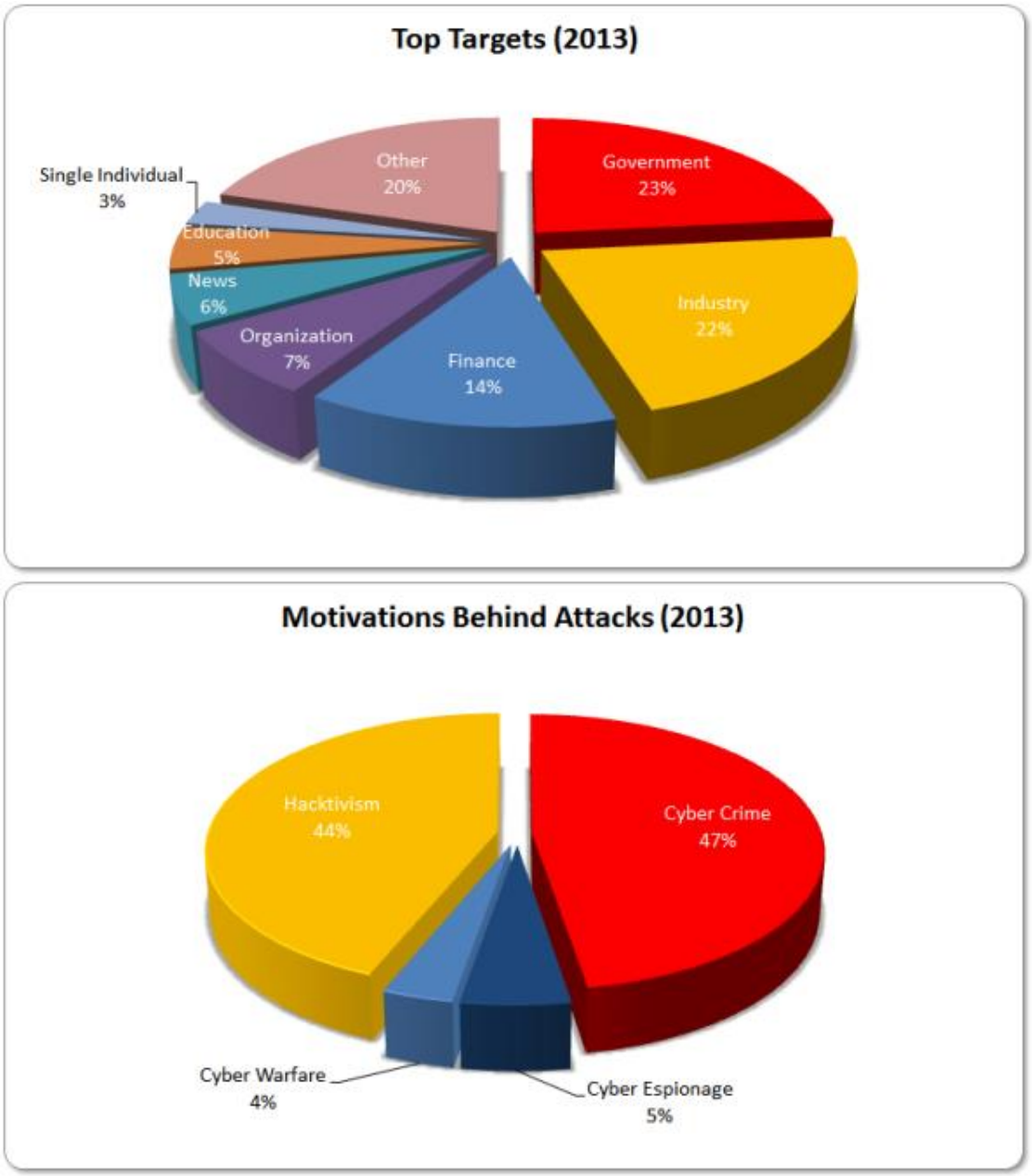

Figure 8: Targeted Systems and Motivations in 2013.[86]

[86] "Biggest Data Breaches." *Privacy Risks Advisors*. 2015. Accessed September 30, 2016. http://www.privacyrisksadvisors.com/data-breach-toolkit/worlds-biggest-data-breaches/

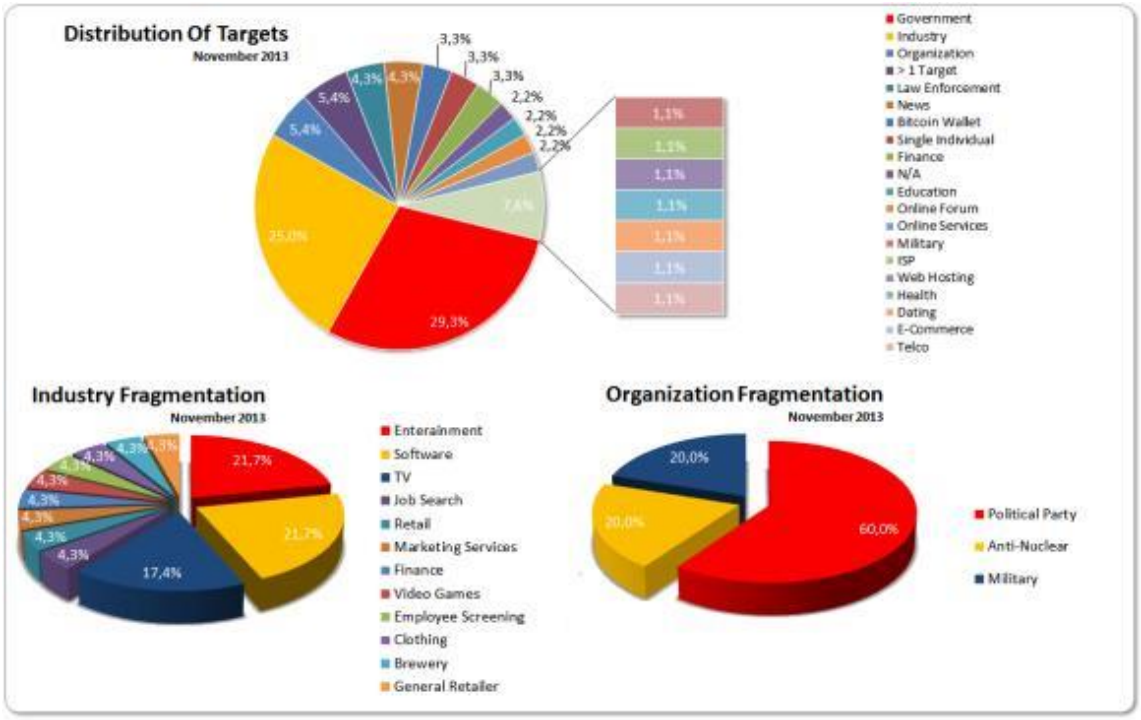

Figure 9: November 2013 Attacks. Distribution of targets, industries attacked, and types of organizations of November 2013[87]

Who Are These Hackers?

Hackers come from all walks of life and from just about every nationality, and the Chinese hacking community is little different in this respect. Active individually as well as in thousands of cyber groups, Chinese hackers represent a community of practitioners that have developed a maturity unmatched at such a large level. Other groups around the world might have more technological

[87] Biggest Data Breaches." *Privacy Risks Advisors*. 2015. Accessed September 30, 2016. http://www.privacyrisksadvisors.com/data-breach-toolkit/worlds-biggest-data-breaches/

knowledge of systems and tools, like the NSA, but Chinese hacking groups are far greater in number. So in reality, due to sheer numbers and the fact that many of these individuals are self-taught, the Chinese hacking community exists on a far grander level than other global hacking groups that are smaller coalitions. They have developed a similar knowledge base to other hackers around the world. Their communities contain many layers of different groups that range from black-hat hackers, malware tool developers, novices and expert computer system explorers, and legitimate legal security analysts and researchers.

There are many publications in China that glorify patriotic hackers. This recent trend helps show that hackers are experiencing a esteemed place in the internet culture in China, and perhaps in the wider society. Books about hackers like Cliff Stoll's 1989 book, *The Cuckoo's Egg,* are common, and are making Chinese citizens familiar with the same ideologies of the individuals who target political enemies around the world.[88] In the face of the recent attempts by the Chinese government to crack down on hacking within the country, it still continues to be a growing business in China, and it is extending its reaches globally. Four significant search engines exist that allowed this community access to the tools and information that it needs: Baidu, Google China, Google US, and Yahoo! China. All four of these engines provide ample links to hacker sites, blogs, and forums with just a simple search of the common Chinese term for hackers, "黑客," *heike*, which sounds something like "hacker" and ominously

[88] Kaplan, Fred M. *Dark Territory: The Secret History of Cyber War*. 2016. Print.

translates as “black guest.”[89] It is within sites where hackers can develop greater social circles in which information on certain networks and tools can be spread. New hackers can learn how, as well as what, is needed to hack based on information found on hacker sites, blogs, and forums. It is not uncommon for homegrown self-taught hackers to be created by these means.

Motivations behind hacking in China can be categorized in one of four ways: nationalism, technical interest, financial gain, and/or fame. For example, when political conflict and personal interest are no longer efficient motivations for hackers, money and fame become the primary motivations keeping Chinese hacking organizations from disbanding. In an interview that I performed with a former member of Anonymous Serbia, the motivation of fame was touched on. He mentioned about making connections with hackers that “once you are in the journalism field people start trusting you and that's how hackers, cyber criminals, and other actors share the inside stories of their work and hey, who don't like fame? So yeah, they love to get into the news and share their stories.”[90] In an interview published by HackRead, the Chinese hacker who uses the name “7zi” explained his initiation into the hacking sphere and how motivations even for one individual are constantly changing. In what started as a fiscal venture with few restrictions, 7zi found that political motivations gradually became more and more important to him. “I did not work and because of shortage of funds, I began to visit hacker circles (online). A brother suggested that I undertake a number of underground transactions... But I hate to attack the government and education

[89] Henderson, Scott J. *The Dark Visitor: Inside the World of Chinese Hackers*. Scott Henderson, 2007. Print.
[90] Uzunovic, Agan. “Chinese Hackers.” E-mail interview by author. April 5, 2016

network [sic], so I did not accept this type of business. I am a patriotic young person, and when the Philippines policeman hijacked the bus full of Chinese, I took part in the back [sic] on the president of the Philippines Department of Communications."[91] This individual's story shows us how difficult it is to track the motivations of hackers in China. Not only is there a broad spectrum of motivations, but even one individual may fluctuate between different motivating forces depending on matters ranging from geopolitics to personal finance.

Many of these individuals also generate income by marketing the culture around them. Besides illegal monetary gains, hackers in China exist in a culture that loves and reveres them. Newspapers clamor to interview them, universities strive to create them, and books and other publications are written based on them. Some thrive openly in the public sector, and even publish their own hacker magazines and webpages. The Chinese hacking culture is nothing like anything found elsewhere around the globe. One example that reflects the popularity of hacking in China, is the Blue Lotus Capture the Flag Competition (CTF). One of the world's largest hacking competitions, the Blue-Lotus competition is held in mainland China where competitors compete at solving individual hacking-based tasks. On April 26, 2015, Jiaotong University held its second annual CTF tournament titled 0CTF 2015, or the Information Security Technology Challenge. Over 654 hacking teams from all over the globe participated, including teams from Shanghai Jiaotong University, Tsinghua University, Fudan University, Beijing University of Posts and Telecommunications, Wuhan University, Fuzhou

[91] Amir, Waqas. "Interview with the Chinese Hacker Who Hacked Microsoft India Store." *HackRead*. February 29, 2012. Accessed December 25, 2015. https://www.hackread.com/interview-with-the-chinese-hacker-who-hacked-microsoft-india-store/

University, and top international hackers.[92]

Another term that revolves around Chinese hacking is hacktivism. The term defines an act of breaching a system based on political and/or social motivations. The individual who performs these acts use similar implements and methods as any other hacker. This kind of attacker may perhaps leave a noticeable comment or note with words or images that reflect a distinct point-of-view on a webpage experiences a significant number of visitors. This type of attack is hidden at the very root of hacking culture in China. In April 2001, Chinese hacktivists posted political homages to Chinese pilot Lieutenant Commander Wang Wei on American sites linked to the government and military. These consisted of the site belonging to the United States Geological Survey administration, as well as an offshoot site of the Federal Emergency Management Agency, and the Naval Surface Force of the U.S. Atlantic Fleet webpage.[93] Wang Wei was killed following a collision with a U.S. Naval surveillance plane over the South China Sea.[94]

Hacker culture in China was largely formed around these types of cultural and political events. One of the earliest, largest and most enduring active hacking groups in China was the Red Hacker Alliance. The alliance was a large coalition of smaller groups that banded together to voice their opinions on political events at the time. Prior to the group's formation hackers worked individually or in very

[92] "第二届 0CTF 信息安全技术挑战赛暨首届 XCTF 上海站选拔赛决赛圆满落幕"SJTU Network & Information Center. May 11, 2015. Accessed May 3, 2016. http://net.sjtu.edu.cn/info/1003/1766.htm
[93] Castello, Sam. "U.S., Chinese Hackers Continue Web Defacements." *CNN*. May 2, 2001. Accessed April 14, 2016. http://www.cnn.com/2001/TECH/internet/05/02/china.hacks.idg/
[94] Martin, Patrick. "US Adopts Aggressive Anti-China Posture in Aftermath of Spy Plane Crisis." *World Socialist Web Site*. April 15, 2001. Accessed December 25, 2015. https://www.wsws.org/en/articles/2001/04/chin-a15.html

small and close-knit groups. Take the more current examples of Edward Snowden and Anonymous for example. Both of these cases outline the individualism or closeness that hackers usually exhibit. Snowden was the sole contributor to the theft and leak of government information and Anonymous is a close-knit group of expert hackers whose reach spans the entire globe.

There are other worldwide incidents where political actions and cyber-warfare combine much like the above 2001 case. The global hacking group Anonymous is perhaps the highest-profile entity in discussions of political hacking groups. Their actions, like the case of the Motion Picture Association of America and Recording Industry Association of America discussed earlier, are a staple of the hacking landscape. Another case that made the media rounds was that of Edward Snowden. The Snowden scandal began in June 2013 when the newspaper, *The Guardian* reported that the NSA (National Security Agency) was gathering information based on the phone records of millions of U.S. citizens. The organization monitored the systems and records of nine internet major companies to trace cyber communications in a program named PRISM (Planning Tool for Resource Integration, Synchronization, and Management).[95] The NSA released a statement, right after the first news stories, calling PRISM "the most significant tool in the NSA's arsenal for the detection, identification, and disruption of terrorist threats to the US and around the world."[96] Since its creation, the NSA has become one of the strongest cyber groups in the world, with cyber-capabilities that far out-strip entire nations.

[95] Kaplan, Fred M. *Dark Territory: The Secret History of Cyber War*. (2016) P. 228-229, 247
[96] Ibid, 247

The Chinese government and the PLA has developed systems much like the NSA in an attempt to match the cyber-capabilities of other leading nations like the U.S., Russia, and Iran. This is evident in the PLA's creation of the Third General Staff Department for Signals Intelligence. Similar to the NSA in that it is a government created group dedicated to and specialized information warfare militia units. In May 2011, the country proclaimed that it had created a "Blue Army" cyber command division of individuals who were recruited from the armed forces, universities, and experts from security organizations.[97]

[97] Lewis, Leo. "China's Blue Army of 30 computer experts could deploy cyber warfare on foreign powers,"
The Australian. May 27, 2011. Accessed February 21, 2016.
http://www.theaustralian.com.au/business/technology/chinas-blue-army-could-conduct-cyber-warfare-on-foreign-powers/story-e6frgakx-1226064132826

CHAPTER THREE:

THE EVOLUTION OF CHINESE HACKERS

Even though the internet was established in China in 1994, there were only seven rudimentary hacker webpages three years later in 1997. The pages available to Chinese individuals were usually reprints and copied information from foreign sites. Most Chinese hackers at the time were very simple in their methodology, and used email-based attacks that were supplied in prepackaged toolkits. Needless to say, the hacker culture was nothing like what exists today. The complexities of modern global or national attacks did not exist.[98]

There would, however, be a significant explosion in hacking activity in 1999, centered around the Indonesian riots of 1998 that came after a financial calamity and saw Chinese individuals in Jakarta targeted by mob violence. A significant amount of the Indonesian populace discriminatorily held responsible the Indonesian Sino-community for the rampant inflation that was occurring within the country, leading to Indonesian civilians targeting their Chinese counterparts with violence, rape, and sometimes murder. This would mark a two-fold evolution that would forever change the Chinese hacking landscape forever. The first change was from simplistic tampering to malicious attackers. The second was in the scope and complexity of the attacks as these groups moved into the twenty-first century. The overall change between the two can be seen as hacker groups moved away from actions like defacing foreign governmental websites to the simultaneous multi-national cyber-attacks that have become

[98] "The Growth of the Chinese Computer Hacker," *KKER Union of China*. November 20, 2004. Accessed March 13, 2016. http://www.kker.cn/book/list.asp?id=1264

common in the last few years. In recent years, it has consistently been the latter forms of attacks causing significant damage to global infrastructures and becoming a hot-button issue for political discussion.

Before the Indonesia riots, few significant hacking organizations existed. Nothing close to an alliance or a group of hackers existed in the years 1995 and 1996. There is nothing at the time that suggests that forms of communication other than rare chat room discussions were taking place between hackers. During this time, Gao Chunhui's webpage was the only forum in China dedicated to anything resembling to hacking as we understand it today, and even Gao's page contained subject matter mainly pertaining to cracking software code.

In 1997, the largest organized hacking group at the time went by the name the Green Army, alternatively known by the name Whampoa (Huangpu) Academy. Both names are historical references, the first to a Qing dynasty (1644-1911) military force, and the second to a famous military academy of the 1920s run by the Nationalist government, but where both Nationalist and Communist future military leaders were first trained. This group is reported to have had a membership of approximately 3000 at its height. Operating in Shanghai, Beijing, and Shijazhuang, the group was established by a cyber expert that went by the pseudonym "Goodwill." The group also drew in further individuals and together they encompassed was is now deemed the country's first group of hackers, such as Cheng Weishan, Peng Quan, Xie Zhaoxia, Huang Lei, and "Little Rong."[99] In 2000. the collection dispersed and is now commonly

[99] Henderson, Scott J. *The Dark Visitor: Inside the World of Chinese Hackers*. Scott Henderson, 2007. Print.

known as a great example of the lasting representations of the Chinese hacker culture.[100] The groups was also one of the first to make successful commercial ventures as well through its Beijing Green Alliance offshoot, which would lead to its collapse. The collective of hackers would invariably split in to two groups, with that former moving into the business of more legalized operations, and the latter (Beijing Green Alliance) continuing the group's illegal hacking efforts. A legal battle insued between the two groups in 2000 leading to a ruling in favor of the Beijing Green Alliance, in which they were granted financial restitution as well as control of the group's web domain (isbase.com).

1998- The Birth of Chinese Hacking

The year of 1998 is considered by most scholars to be the true birth of Chinese hacking. There were two incidents that combined to become the catalyst that produced China's unique hacker culture. The first incident happened outside of China with the release of the "Back Orifice Program" by the American hacking group, "Cult of the Dead Cow."[101] After the program was released, Chinese hackers gained access to its valuable source code and it became a new tool in their repertoire. This program was responsible for the increased use of the now-common Trojan horse virus, which is characterized by its concealment within another program and its malevolent/destructive nature.

The second part of this two-pronged catalyst came with the Indonesian riots of 1998 and subsequent cyber-conflicts. With the exception of the Green

[100] Henderson, Scott J. *The Dark Visitor: Inside the World of Chinese Hackers*. Scott Henderson, 2007. Print.
[101] Ibid

Army, large unified hacker groups did not exist in China as they do now. Tentative communications were developing within the nascent community, and coalitions were starting to form (like the Green Army), but there was not a binding ideology in place to bring these new hackers together. This would all change with the incidents in Jakarta, Indonesia. In May 1998, riots swept through Jakarta after a financial crisis devastated the country. Inquiries by human rights organizations revealed that many of the targets of the hostility were from Jakarta's Chinese community. It was a methodical process of discrimination that included the armed forces and law enforcement.[102] Some ethnic Chinese communities were victimized in a number of atrocities, including rapes, murders, and the destruction of Chinese property and businesses**.**[103]

Stories from Indonesia reached Chinese cyberspace, and spread like wildfire in online communities. The shock brought on by the violence was quickly replaced by outrage.[104] The individual hackers and budding hacker groups that commonly patrolled online communities had found their common cause. A spontaneous gathering of hackers took place in what are known as IRC (Internet Relay Chat) chat rooms.[105] Together, the first Chinese hacktivist groups were formed. In political retaliation, these groups worked together to attack the

---

[102] Komisi Nasional Hak Asasi Manusia Indonesia (Indonesian National Commission on Human Rights), Statement of the National Commission on Human Rights Concerning the Unrest in Jakarta and the Surrounding Areas. June 2, 1998. www.komnas.go.id/english/cases/cs_text02.html

[103] "Anti-Chinese riots continue in Indonesia," *CNN News CNN.com/World*. August 29, 1998. Accessed August 23, 2005. http://www.cnn.com/WORLD/asiapcf/9808/29/indonesia.riot

[104] Long San, "Let's look back on the days of the Red Hacker Alliance," *Juntuan*. October 24, 2005. Accessed November 17, 2005. http://www.juntuan.cn/user1/2334/archives/2005/9612.shtml

[105] "What Is Internet Relay Chat (IRC)?" *SearchExchange*. December 2005. Accessed March 18, 2016. http://searchexchange.techtarget.com/definition/Internet-Relay-Chat

Indonesian government's website by bombarding their e-mail system. It was a primitive attack in comparison to attacks a decade later, but it was the first *collective* demonstration of cyber-force that Chinese hackers showed, and it was a crucial moment in the development of China's hacker community as it exists today.

On August 7, 1998, what had originally started as e-mail-based attacks escalated into website defacement. Chinese hackers obtained access to several web pages from Indonesia, and to show the strength of their attack, the hackers attached the addresses of other defaced web sites.[106] The online publication *China Byte* broke the news of the attacks to individuals with e-mail subscriptions, and soon after, news of the cyber-attacks spread. The email published the same message that the hackers published on the page: "Your site has been hacked by a group of hackers from China. Indonesian thugs, there can be retribution for your atrocities, stop slaughtering the Chinese people [sic]."[107] As the attacks continued, other sites were vandalized with other political statements. One of these statements, on the homepage of the Indonesian National Family Planning Coordinating Board, was supplanted with a statement exclaiming "Warning from Chinese. This page is hacked for your national day. Please keep this page for 48 hours and punish the murderers in May immediately [sic]."[108]

The Indonesian riots also give birth to what would become the "Red

---

[106] Long San, "Let's look back on the days of the Red Hacker Alliance," *Juntuan*. October 24, 2005. Accessed November 17, 2005. http://www.juntuan.cn/user1/2334/archives/2005/9612.shtml

[107] Ibid

[108] Nuttall, Chris. "Chinese Protesters Attack Indonesia through Net." *BBC News*. August 19, 1998. Accessed March 28, 2016. http://news.bbc.co.uk/2/hi/science/nature/154079.stm

Hacker Alliance", one of the most significant cyber-groups in the internet's short history. The political nature of this patriotic campaign led to the creation of something entirely new, and would be the first time the term "red hacker" (红客 *hongke*) would be used. The attacks in the country functioned as the facilitator that brought together individuals who normally operated independently under the guise of nationalism, establishing not only a group but also the notion of red hackers which still exists today.[109] As a present affiliate of the Red Hacker Alliance known as "Sharp Winner" states, it exists as "a group of patriotic youth active on the net engaged in attacks on Indonesian government web sites, under the alias 'China Red hackers.' This patriotic action received a great deal of reporting and praise in the domestic and overseas media. The name China red hackers began here."[110]

A year later, in July of 1999, Chinese hackers would once again have political motivations to perform collective actions. This was the first such event since the attacks on Indonesia. These attacks centered on Taiwanese President Lee Teng-hui's (Li Denghui) "Two-States Theory," which advocated the idea that it was an independent country. This perceived threat to the One China Policy and the nation's sovereignty sparked political attacks by Chinese hackers on Taiwanese targets. On August 7, 1999, hackers attacked ten Taiwanese government pages, leaving statements like "There is only one China in the world

[109] Henderson, Scott J. *The Dark Visitor: Inside the World of Chinese Hackers*. Scott Henderson, 2007. Print.
[110] "The Ever-Changing Red Hacker Sharp Winner," Interview of Sharp Winner by *China Educational Television Satellite Channel (CETV-SD)*, September 13, 2005. Accessed January 14, 2016 http://forum.gd.sina.com.cn/cgibin/viewone.cgi?gid=51&fid=1359&itemid=8191

and the world only needs one China."[111] The same Chinese hackers went on to sabotage state, college, and industrial webpages. The assaults allegedly included more than one hundred and sixty penetrations of the nationwide computer systems of Taiwan.[112]

This event would become what is now known as the First Taiwan-China Hacker War. It played a crucial role in how Chinese hackers would engage in future attacks. This is the point when the first malicious attacks by Chinese hackers took place. Before 1999, hackers merely e-mail bombed, performed denial-of-service attacks, or left political messages on websites. It was during this war that two different malicious programs were developed and used that would change the Chinese cyber-landscape forever.

Tools of the Trade

It would mark the beginning of a new era where programs were created in China instead of being brought in from elsewhere. The first program created in this way was the Glacier Trojan Horse virus, by security programmer Huang Xin. The Trojan horse virus Netspy (inspired by the above-mentioned Cult of the Dead Cow's Back Orifice) followed Glacier, and both would become a hacker staple for years to come. Other hacking tools created in this period included Black Hole, Network Thief, XSan and YAI. Glacier, Black Hole, and Network

---

[111] Li Zi, "The Chinese Hacker Evolution," *People in Focus Weekly*, March 10, 2005. Accessed February 21, 2016. http://net.chinabyte.com/386/1920386.shtml

[112] Hsaio, Russell. "Critical Node: Taiwan's Cyber Defense and Chinese Cyber-Espionage." *The Jamestown Foundation*. December 5, 2013. Accessed February 14, 2016. http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews[tt_news]=41721&cHash=3505e552d9d50d88cfc539af1319e699#.VyWOqnry1_k

Thief are still essential tools for hackers in China, and offshoot versions of each have been developed.[113] These new programs do indeed mark a shift in the Chinese hacking landscape, and as hackers deployed the newly developed "Glacier" and "NetSpy" for the first time they invariably moved away from minor intrusions and into a realm of maliciousness.

In Chu Tianbi's writing *Chinese Hacker History/Looking Back on Chinese Hacker History,* he adds that the Taiwan-China Hacker War led to the formation of hacker classifications (red hackers, blue hackers, and black hackers).

> In addition, it was also in this year that the entirely new concept of 'Blue Hackers' arose. During this time, Chinese hackers could essentially be divided into three categories. One was hackers with a political and nationalistic bent represented by the Chinese Red Hackers. Another was the technical hackers purely interested in Internet security technology and not concerned with other issues, represented by the Blue Hackers. The last type was the original 'Black' Hackers who were entirely concerned with pursuit of the original hacker spirit and did not focus on politics or the frenzied pursuit of technology.[114]

These hacker classifications do not follow the normal categorization of traditional hacker cultures noted above (black, white, and grey hat hackers), but is the best description of Chinese hacker culture due to the deep patriotic and nationalistic beliefs that fueled hackers in China for many years. Even today,

---

[113] Henderson, Scott J. *The Dark Visitor: Inside the World of Chinese Hackers*. Scott Henderson, 2007. Print.

[114] Chu, Tianbi, "Chinese Hacker History/Looking Back on Chinese Hacker History," Accessed August 9, 2015. http://www.blogchina.com/news/source/310.htm

hacker culture is routinely fueled by political events, although these initial groups have largely moved into the "blue hacker" category.

The Chinese hacker community continued to make huge strides after the cyber-feud with Taiwan. Less than a year later, another incident sparked the same nationalistic fervor. On May 7, 1999, the Chinese embassy in Yugoslavia was bombarded by U.S.-led forces during the Kosovo War. The bombing was declared to be a tragic accident by the Americans, and blamed on using old maps of the city of Belgrade. The incident resulted in the deaths of three Chinese. According to Tianbi, "the second day after the bombing of the Chinese embassy, the first Chinese Red Hacker web site appeared, and a new type of hacker was born – the Red Hacker."[115] This attack in consort with the assaults on Taiwan in 1998 aided in solidifying the international position of Chinese hackers as a collective, prepared to partake in politically driven denial-of-service attacks, data destruction, and website defacement. Yet, it was not until 1998-1999 that these individuals banded together in groups like the "Red Hacker Alliance." The group exchanged vandalism and DDoS strikes with their enemies in Taiwan, the United States, Indonesia, Japan, and South Korea and functioned with freedom until disapprovals delivered from the Chinese government and the threat of prosecution basically ended the attacks.[116]

As the world readied for the twenty-first century, so did this ever-growing hacker culture. Between 2000 and 2005, Chinese hackers increased their

[115] Chu, Tianbi, "Chinese Hacker History/Looking Back on Chinese Hacker History," Accessed August 9, 2015. http://www.blogchina.com/news/source/310.htm
[116] Deweese, Steve. *Capability of the People's Republic of China (PRC) to Conduct Cyber Warfare and Computer Network Exploitation*. Rep. Northrop Grumman. Print.

dominance in the Asian world with continued attacks on Japan and Taiwan. The majority of attacks stemmed from political motivations, and the number of hacker groups increased as existing hacker groups grew in size.

Table 2- Chronological Timeline of Significant Hacker Attacks from China.

Year	Name of Attack	Cause
1998	Indonesian Riots	Chinese hackers assault webpages in reaction to anti-Chinese d.emonstrations in Indonesia
1999	Taiwan's "Two-States"	Raids are initiated in opposition to Taiwanese webpages after the country's leader asserts that the country is independent.
1999	Chinese Embassy Bombing	Strikes against the United States' sites commence after the Chinese Embassy is bombarded by U.S. forces.
2000	Nanjing Massacre Incident	Japanese webpages are hit after the Japanese administration is alleged to refute its accountability in the Nanjing Massacre.
2000	Taiwan Voting Episode	Hackers assault webpages after Chen Shui-bian is voted as leader.
2001	Assault on Japan II	Chinese groups attack Japanese webpages for improper treatment of Chinese citizens on an airline, poorly manufactured cars from Japanese company Mitsubishi, and Japanese textbooks.
2001	Sino-U.S. Hacker War	Chinese and American hackers attack one another after an American spy plane crashes into a Chinese fighter jet, forcing the U.S. pilot to land on Hainan.
2004	Diaoyu Island Dispute	Individuals assault Japanese webpages in retaliation to Japanese hacker attacks.
2005	Yasukuni War Memorial Incident	Webpages are vandalizes by Chinese hackers when Japan's Prime Minister journeys to the Yasukuni War Memorial

Hacker War: US-China

Even to this day Chinese hackers have had a fondness for American systems. If the Chinese embassy bombing planted the seeds of anti-American actions, then the events in 2001 would be the sprouting of the tree. Hackers from the U.S. and China conducted mass confrontations; much like the one fought with the Taiwanese after a U.S. spy aircraft crashed into a Chinese military aircraft and then made an emergency landing on the island of Hainan, which is Chinese territory. The crew was detained for several days and then released.

These Sino-American attacks continued to escalate beyond the 2001 incidents. In 2003, hackers from China were able to steal information from various U.S. government agencies. The group conducted wide-ranging assaults in attempts to appropriate delicate intelligence as part of has now been codenamed “Titan Rain.” The sheer scale, speed, and range was remarkable. On November 1st, 2004, at 10:23 p.m. the attackers assaulted the U.S. Army Information Systems Engineering Command in Arizona. Less than an hour later, they used an identical weakness to attack the Defense Information Systems Agency in Virginia. Five hours after the initial attack, the hackers struck again at California’s Naval Ocean Systems Center. The last attack occurred just before 5 a.m. with the United States Army Space and Strategic Defense system.[117] According to Alan Paller, the director of the SANS Institute which specializes in information security and cybersecurity training, “From the Redstone Arsenal,

[117] Thornburgh, Nathan. "Inside the Chinese Hack Attack." *Time*. August 25, 2005. Accessed September 30, 2016. http://content.time.com/time/nation/article/0,8599,1098371,00.html

home to the Army Aviation and Missile Command, the attackers grabbed specs for the aviation mission-planning system for Army helicopters, as well as Falconview 3.2, the flight-planning software used by the Army and Air Force."[118] What makes these attacks more significant than previous ones is that military systems are not connected to the internet directly, so these hackers needed to bypass levels of security that far exceeds the previous actions of Chinese hacker groups. Some of the other attacks on American systems include United Airlines, United States Steel, and more famously, Westinghouse. Chinese targets extended among every significant industry by 2012, when the director of the NSA Keith Alexander designated cyber-espionage out of China as the "greatest transfer of wealth in history."[119]

It is clear from the foundations of the Chinese hacking community, as laid out above, that it did not begin with strict governmental initiatives, but rather from the spontaneous actions of an outraged citizenry, or "netizenry." A coincidence of events in the mid and late 1990s brought about an increasingly coherent community of Chinese hackers with a clear theme of patriotism and nationalism driving much of the community's activity. While today it is very difficult to discern the sources and motives for all Chinese hacks, these early foundations show that Chinese hacking did not begin as the product of explicit governmental directives. Rather, early Chinese "hacktivism" began in the grey area of spontaneous

---

[118] Espiner, Tom. "Security experts lift lid on Chinese hack attacks", November 23, 2005. Accessed December 13, 2015. http://news.zdnet.com/2100-1009_22-145763.html

[119] Rogin, Josh. "NSA Chief: Cybercrime Constitutes the greatest transfer of wealth in history." *Foreign Policy*. July 9, 2012. Accessed February 21, 2016. http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/

nationalist activity in defense of China's international prestige as conceived by China's hackers.

However, the creation of Chinese hacking groups helps to convolute the perception of the Chinese hacking landscape. While the foundations and growth of these groups is indebted to political activism and an independent nature, the rise of China's economic progress during this era owes a great deal to state-sponsored cyber-espionage. Due to a clash of these two ideologies, it can be sometimes difficult to distinguish amongst the two. The question that the next few chapters attempts to answer is just that, how can someone distinguish from what is nationalistic independent action and what are state-sponsored cyber-attacks?

Hacker culture itself seems to be a mirror of the political system that has made China into such a strong economic world power in the realm of manufacturing. Much like a manufacturing system, an individual could write a low-level computer code that is given to or sold to other individuals above them. These secondary individuals might be contracted using these codes or may sell them. These codes could even be placed on hacker webpages where individual can download them or buy them for their own purposes.[120] Because of this it is sometimes very difficult to distinguish between who created the means of attack, and who committed it. The attack might be traced back to the creator, who could very well have no ties to the government, yet the perpetrator of the attack could very well be a state-run organization. This very issue came up during my discussion with the founder of HackRead. This notion also pertains to the idea

[120] Wong, Edward. "Hackers Find China Is Land of Opportunity." *The New York Times*. May 22, 2013. Accessed February 1, 2016. http://www.nytimes.com/2013/05/23/world/asia/in-china-hacking-has-widespread-acceptance.html

that the attack is carried out by one individual and the information stolen is sold to other and reduces the accuracy of recognizing the target. He states “The Independent Chinese and Russian hackers are also sophisticated as they target governments to steal documents and sell them to the government-backed hackers (call them freelancers). I personally think that governments have no problem with independent hackers and they actually like what these guys do, there's always something important coming from these independent groups.”[121] Later on in the same interview, he said “And like I said Chinese hackers don't fear the government because the government knows one day they will get something sensitive from these independent hackers.”[122] This is very important in understanding the way that attacks are carried out, because rarely are the means of attack created by the attackers themselves. More commonly, a program or virus is created by one individual or a small group and acquired by a larger organization.

In the subsequent chapters, the different categorizations of Chinese hackers will be outlined in one of three ways: independent, state-sponsored, and freelance. It has become exceedingly difficult for experts and researchers to separate the different groups because of the intricacies of the hacking culture as well as the anonymity of the internet. There are significant differences between the three classes, and therefore, it is possible to provide a view into the Chinese hacking underworld.

[121] Waqas, Amir. "Chinese Hackers." E-mail interview by author. April 7, 2016.
[122] Ibid

CHAPTER FOUR:

INDEPENDENT ACTORS

In China, there is some blurring of the line between patriotic hackers and criminal hackers. There is also often uncertainty about whether a cyber-attack has been launched by a military or government employee sitting at an office desk, or by sympathetic unaffiliated civilians, or contracted civilians, or even by independent civilians who are attacking for personal motivations such as financial gain or notoriety. Due to the fact that the PRC has its hand in many aspects of the economy entails that hackers have a tendency to come across government jobs in their search for work. “I don’t think the West understands,” a former Chinese hacker said. “China’s government is so big. It’s almost impossible to not have any crossover with the government.”[123] This striking statement is a good point of departure for our examination of the different types of Chinese hackers, starting with independent actors.

Independent hackers are more often than not motivated by money or nationalism, but see themselves as lone sharks in a sea of government-orchestrated agendas. The difference in China is that these individuals for the most part have in mind what is best for their understanding of the Chinese national good, which might involve direct support for the government, or a broader understanding of Chinese national interest. Most often when Chinese hackers are reported on in the world news, they may be an unit in the PLA or a member of an independent nationalistic hacker group. Distinct from the hackers

[123] Wong, Edward. "Hackers Find China Is Land of Opportunity." *The New York Times*. May 22, 2013. Accessed February 1, 2016. http://www.nytimes.com/2013/05/23/world/asia/in-china-hacking-has-widespread-acceptance.html

in the West, who typically are solitary or activists, individuals from China are more concerned about political affairs and establishing the country as superior on a global stage.

Independent, non-state sponsored hackers have deep roots in patriotism and nationalism. These groups date back to the beginning of hacking in China, with groups like ChinaWill, the Red Hacker Alliance, and the Green Army. There is a strong relationship between these types of groups and Chinese identity and Chinese culture and the country's place in the world. According to journalist, Edward Wong writing in the *New York Times* states that "the culture of hacking in China is not confined to top-secret military compounds where hackers carry out orders to pilfer data from foreign governments and corporations." Furthermore, hacking is a fixture of society that is blatantly deliberated about "at trade shows, inside university classrooms and on internet forums."[124]

Honker Union (1999/2001–Present)

Today, China's most famous group of hackers, the Honker Union, illustrates the grey area separating nationalistic actors and the state. The word Honker is similar in nature to the term *hongke,* which literally means 'red visitor'. Founded in 2001, the group grew out of the cyber-warfare centered around the Hainan spy plane incident of that year. Although some scholarship on the subject has asserted that there is a link between the Honker Union and the Chinese government, no specific details have been published. It is true that the hacking

[124] Wong, Edward. "Hackers Find China Is Land of Opportunity." *The New York Times*. May 22, 2013. Accessed February 1, 2016. http://www.nytimes.com/2013/05/23/world/asia/in-china-hacking-has-widespread-acceptance.html

group's actions are similar to the Party's agenda, but in my assessment, this is not enough to categorize a group as state-sponsored. Many patriotic hackers perform actions that follow the same goals as the Communist Party. One of Honker Union's leaders, Lyon, has gone on the record saying, "The Honker Union ... has no interest in getting involved in politics. We work only for the security of Chinese websites."[125] Yet the same article concludes by stating that Lyon is the head of a department in a major state-owned telecommunications firm. The Honker Union has an established set of rules of engagement. To further illustrate the way that the Honker Union operates and how their actions could follow the same ideologies of the Party all one has to do it look at these rules of engagement, which are found on their webpage and state the following:

1. Our offensive and defensive skills are not used to show off!
2. Out technology is to share with all patriotic Honkers!
3. We will continue to learn, and continually research new techniques of attacks and defenses!
4. We must familiar [ourselves] with the C language, and any other language of the target!
5. We must be patriotic!
6. We not only need to know the common exploits of the systems, but also need to know how to discover exploits!
7. We must know how to use search engine, it is a very good tool for learning!

[125] Wong, Edward. "Hackers Find China Is Land of Opportunity." *The New York Times*. May 22, 2013. Accessed February 1, 2016. http://www.nytimes.com/2013/05/23/world/asia/in-china-hacking-has-widespread-acceptance.html

8. We must know how to break the conventional way of thinking! “Nothing is impossible, if we can think of, then we can do it! There is no “room” we cannot enter, if the “room” allows air to go in then we can become “air” and go into the room!
9. We must know how to conduct oneself! – learning skills must first learn how to conduct oneself![126]

After the May 1999 event that say the embassy bombed in Yugoslavia, the word “Honker” emerged within the hacking community. Since then, the individuals whom this term illustrates have bended together within a collective known as the Honker Union. These individuals unite their computer expertise with nationalism. At the group’s inception, a series of attacks on websites in the United States was initiated that illustrate this blending of skills and ideologies. At the time of writing, there is no evidence that the Chinese government has any affiliation with the group. The group mainly teaches and exchanges in counterattack skills, and includes around fifty thousand members.

[126] “Honker Purpose” H.U.C.honkerchina.net. July, 2015. Accessed May 5, 2016 http://www.honker.net.cn/about/zongzhi.html

Figure 10: Honker Union Attacks on Iranian Sites. A Honker Union attack on Iranian web sites due to political motivations in 2010, and on an American web

site.[127]

The *New York Times* indicates that hacking can also be a profitable vocation in China, even if the individual does not work for the government. An individual who has enough technological knowledge can utilize his or her abilities to make one hundred thousand dollars per year in U.S. currency. Along with this, it is the open culture and the view of hackers in China that contribute to such an incredible phenomenon. Young individuals and students in China adore hackers. They want to be them. In a study directed by the Shanghai Academy of Social Sciences, of the five thousand primary school students who were interviewed 43 percent answered that they "adored" hackers and 33 percent said they fantasized of growing to be one in the future.[128] Hacking in China is a lifestyle, an aspiration, and a culture. It presents an autonomous avenue for the possibility of an existence of their own desire, and not one that is controlled or regulated by the government, family expectations, or cultural tradition. In response to the survey, one student named Fan Yi said, "Hackers are very cool. Hackers leave people an impression of high intelligence and are able to do whatever they like and get whatever secrets they want. That is what I lack but dream of."[129]

It is this view of hacker culture and the vast numbers who aspire to the lifestyle and vocation of hacking that creates such a grey area where individuals cannot be easily categorized. In the view of wishful individuals who aspire to

---

[127] Danchev, Dancho. "Baidu DNS Records Hijacked by Iranian Cyber Army" *ZDNet*. January 12, 2010. Accessed March 30, 2016. http://www.zdnet.com/article/baidu-dns-records-hijacked-by-iranian-cyber-army/

[128] Liang, Guo, and Markle Corporation. "Surveying Internet Usage and Its Impact in Seven Chinese Cities." *Center for Social Development Chinese Academy of Social Sciences.* 2007. Accessed January 17, 2016. http://www.policyarchive.org/handle/10207/16013

[129] Zhen, Yan. "Morals lost in cyberspace," *Beijing Time*, December 12, 2005. Accessed January 14, 2016. www.shanghaidaily.com/art/2005/12/12/226181/Morals_lost_in_cyberspace.htm

become hackers, those who already are hackers seem to be able to do whatever they want. They are a beacon of freedom and autonomy.

In 2008, the U.S.-China Economic and Security Review Commission organized an investigation into cyber threats originating from China. The organization collected a wide range of security experts. The Commission's report established that "determining the origin of cyber operations, and attributing them to the Chinese government or any other operator, is difficult. Computer network operations provide a high degree of plausible deniability" to the Chinese government.[130]

Online, an enthusiastic student can purchase all the tools of the trade, from pre-programed Trojan horses to explanations of how to avoid or bypass anti-virus programs. The market for malware in China includes many different types of software, like the program Grey Pigeon. Grey Pigeon was initially conceived to remotely control another user's computer, and provided hackers with an ideal tool. With this tool at their disposal, hackers are quickly able to exploit any opening or system vulnerability. "Malware groups out of China have been very quick to adopt zero-day exploits," said Nart Villeneuve, chief research officer at SecDev.Cyber. "They may be operating independently but there may be some sort of market for selling the information that they get."[131] These zero-day vulnerabilities are system weaknesses that exist without knowledge prior to an

[130]US-China Economic and Security Review Commission, "China's Proliferation Practices, and the Development of its Cyber and Space Warfare Capabilities," May 2008 Accessed February 21, 2016. http://www.uscc.gov/hearings/2008hearings/transcripts/08_05_20_trans/08_05_20_trans.pdf

[131] "Google Attack Puts Spotlight on China's Red Hackers." *Reuters*. Thomson Reuters, January 20, 2010. Accessed January 14, 2016. http://www.reuters.com/article/us-google-china-hackers-idUSTRE60J20820100120

incident; because the group that created it was not aware it existed. In 2008, James Mulvenon, a prominent cyber-security expert, informed a congressional commission that there are some individuals who receive instruction at institutions specifically to become hackers or to learn to acquire confidential information through computer activities, like the Communication Command Academy in Wuhan for example.[132]

Red Hacker Alliance (1998-Present)

In 1998, individual hackers merged into what is known today as the Red Hacker Alliance. This group still exists and has been a strong foundation for Chinese hacking culture for almost twenty years at the time of writing. In 1999, the bombardment of the United States Embassy in Yugoslavia brought together a collection of nationalistic individuals in an attempt to defend their country against what they saw as imperialism. Many of these individuals took the fight to cyberspace in hacking efforts. These 'red hackers', as they were dubbed, attacked any individual or group that they saw as critical of China, and infiltrated other governments, organizations, and companies.

Following the wave of cyber-attacks related to the embassy bombing, the group participated in a sequence of other assaults in opposition to specific countries. They struck Taiwan in 1999 and yet again in 2000, the latter being in connection to political elections. They also struck Japan in 2000 for events

[132] "Google Attack Puts Spotlight on China's Red Hackers." *Reuters*. Thomson Reuters, January 20, 2010. Accessed January 14, 2016. http://www.reuters.com/article/us-google-china-hackers-idUSTRE60J20820100120

regarding the Nanjing Massacre in the Second World War. They assaulted the country yet again in 2004, with strikes associated with the disagreements regarding the Diaoyu Islands. When the U.S.-Sino hacking war broke out in 2001, the 'Red Hackers' sported approximately fifty thousand members. This number can be a little inflated, because there is no telling the levels of expertise that the majority of these members had. Many of these individuals knew little about computer systems and only join based on patriotism and because group membership does not require any technological knowledge. The group maintained that their actions were only in and their only intention was to "defend the national interests."[133] On the "Chinese hacker emergency meeting center" webpage that was created in the midst of an attack, it was declared, "We firmly support the position of the Chinese government and Communist Party of China."[134]

China Eagle and Wan Tao (2000-Dissolved)

The hacking group called China Eagle Union was founded in 2000. Over the course of their short history they penetrated a vast amount of systems ranging from American Government systems to Japanese personal communication systems. Their actions consequently followed the PRC agenda, if in a more aggressive and offensive manifestation than Beijing's more diplomatic language and cautious action. This group comprises of thousands of hackers

[133] Chao, Leon. "The Red Hackers Chinese Youth Infused with Nationalism." *CHINASCOPE*. January 27, 2008. Accessed February 7, 2016. http://chinascope.org/m/content/view/456/148/1/1/
[134] Ibid

whose declared objective is to penetrate western systems.[135] Yet, founder Wan Tao stresses that he on no occasion hacked legitimately for the government and never stole confidential information. Other individuals affiliated with the group maintain that the government has no contribution in their undertakings, and that they are even defying the laws of the state which place them in jeopardy of incarceration.[136]

Today, a lot of these individuals are instead searching for the prospect of developing lawful security companies, or working legally within the security field. Tao has been a fundamental role in this idea of hackers discovering legal means for their skills in transforming the China Eagle Union into a NGO named the Intelligence Defense Friends Laboratory. This organization was formed with the intention to encourage more positive behavior for individuals who usually work illegally for a living. In 2012, Tao also functioned as a managing consultant on IBM's Cloud Tiger Team that markets IBM's cloud-based amenities. He stated that the Chinese hacking population is not one of a well-oiled machine in which gifted individuals are taken by the authorities and quickly incorporated into malevolent operations. Quite the reverse, the community exists as a collection of semi-skilled, self-taught individuals who are sometimes driven by nationalistic spirits. Their intention is to create disorder in the form of cyber activism, while

[135] Chao, Leon. "The Red Hackers Chinese Youth Infused with Nationalism." *CHINASCOPE*. January 27, 2008. Accessed February 7, 2016. http://chinascope.org/m/content/view/456/148/1/1/

[136] Beech, Hannah. "China's Red Hackers: The Tale of One Patriotic Cyberwarrior" *Time*. Febuary 21, 2013. Accessed January 17, 2016. http://world.time.com/2013/02/21/chinas-red-hackers-the-tale-of-one-patriotic-cyberwarrior/

some merely seek to gain from their expertise.[137]

Javaphile *and Coolswallow* (2000-*2008*)

Javaphile was created in September 2000 by two individuals with the online designations of “Coolswallow” and “blhuang”.[138] The entire group is thought to be students enrolled at Jiaotong University in Shanghai. Coolswallow gained prominence during the 2001 EP-3 incident. Coolswallow and blhuang would later reorganize the group into a full-fledged hacker group as well as a creating a web site offering their services. The group gained some notoriety in 2002 for vandalizing a Taiwanese company’s webpage, Lite-On.

Although its more significant members are also members of the Red Hacker Alliance, there is a noteworthy difference between the two groups. Site defacement is very common between the two groups. This can be seen in the attacks on the websites Lite-On and Fox T.V., as the graphics and language is not typical when compared to that of a Red Hacker Alliance attack. The group appears to be more religious-based than that of the common Chinese hacking groups as their homepage displays an image of a Buddha head. Coolswallow came out in the open under his own name in 2008 after publishing several academic articles on cyber-espionage. Peng Yinan, also known as Coolswallow, presently is performing research for the Chinese government. Since his work as

---

[137] Kirk, Jeremy. "Chinese Ex-hacker Says Working for the Government Would Be Too Boring." *Network World*. November 8, 2012. Accessed April 15, 2016. http://www.networkworld.com/article/2161287/data-center/chinese-ex-hacker-says-working-for-the-government-would-be-too-boring.html

[138] Henderson, Scott J. *The Dark Visitor: Inside the World of Chinese Hackers*. Scott Henderson, 2007. Print.

Coolswallow, Peng has worked as a security information consultant for the Shanghai Public Security Bureau, which highlights the relationship that some hackers have in state-run organizations. Public Security Bureaus in the nation are similar to police agencies and act as the principle police and security authority for the People's Republic of China.

Figure 11: Message From Javaphile After Taiwan Attack. A message left by the group Javaphile after an attack on the nation-state of Taiwan.[140]

[140] Hvistendahl, Mara. "Hackers: The China Syndrome." *Popular Science*. April 23, 2009. Accessed March 30, 2016. http://www.popsci.com/scitech/article/2009-04/hackers-china-syndrome

Network Crack Program Hacker (NCPH) *and Wicked Rose*

The Network Crack Program Hacker (NCPH) group is culpable for the creation and distribution of vulnerabilities in Microsoft Word and Mi*crosoft Excel's structure code.* NCPH consists of approximately ten members, including individuals with the usernames "Wicked Rose," "KuNgBiM," "Rodag," and "Charles."[141] Attacks by the group were first published on May 18, 2006. The group became well regarded due to their use of zero-day vulnerabilities. The first sign was discovered when the Internet Storm Center reported a potential zero-day attack on May 18, 2006. The attacks started six days prior on May 12 and were discovered to be attacks on establishments in the U.S. and in Japan, two common cyber-enemies of Chinese hackers.

Wicked Rose is the most significant among the group's members, as well as the one who is most public. An early twenty-year old college student studying at Sichuan University of Science and Engineering, it is through Wicked Rose that the other members can be ascertained.[142] The group is more than likely other students at the university who form a close social circle and support each other's hacking interests. Throughout the summer of 2006, while the school was not in active session, over thirty five zero-day vulnerabilities and assaults on previously undiscovered Microsoft Office vulnerabilities were exposed.[143]

Wicked Rose turned out to be an individual by the name of Tan Dailin. He was arrested by local authorities in Chengdu, China in 2009 due to new Chinese

[141] Dunham, Ken, and Jim Melnick. "Wicked Rose" and the NCPH Hacking Group. Accessed September 30, 2016. fserror.com/pdf/WickedRose_andNCPH.doc
[142] Dunham, Ken, and Jim Melnick. "Wicked Rose" and the NCPH Hacking Group. Accessed September 30, 2016. fserror.com/pdf/WickedRose_andNCPH.doc
[143] Ibid

cybercrime laws that were passed that same year. Tan was allegedly detailed after a discovered DDOS attack in which his victims went to the authorities with proof of his actions.[144] There are significant dangers in hacking independently, especially now that cyber-attacks originating from Asia are gaining and international audience. China itself has passed legislation protecting public systems, which is a contrast to past legislation that merely protected government systems. In 2011, the PRC revised its Regulations on the Protection of Computer Information System Security of the PRC, and in 2012 the Decision of the National People's Congress Standing Committee on Strengthening the Protection of Internet Information was passed.[145] Both of these allowed for the crack down on cyber-attacks within the country. Individuals like Tan would find that the watchful eyes of the Chinese government would no longer turn a blind eye to the actions of hackers and hacktivists. Hackers would now face harsher punishment for their actions, especially if Chinese systems were the victims.

[144] McMillan, Robert. "As Hacking Hits Home, China Strengthens Cyber Laws." *PCWorld*. May 11, 2009. Accessed March 18, 2016.
[145] Ventre, Daniel. *Chinese Cybersecurity and Defense*. London: ISTE, 2014. Print.

Figure 12: Wicked Rose, Leader of NCPH. Wicked Rose turned out to be a college student named Tan Dailin.[146]

[146] Dunham, Ken, and Jim Melnick. "Wicked Rose" and the NCPH Hacking Group. Accessed September 30, 2016. fserror.com/pdf/WickedRose_andNCPH.doc

Figure 13: The Hacker Studio. Members of NCPH operating in their “Hacker studio”. [147]

[147] Dunham, Ken, and Jim Melnick. "Wicked Rose" and the NCPH Hacking Group. Accessed September 30, 2016. fserror.com/pdf/WickedRose_andNCPH.doc

CHAPTER FIVE:

STATE-SPONSORED GROUPS

Efforts by individuals or groups from China to pilfer vital information from western organizations and businesses have been well- documented. These successful or foiled attacks have caused frequent hostilities amongst the United States and China in recent years. Cyber-security authorities and prominent organizations whose services exist online, like Google and Microsoft, have upheld that Chinese individuals employ cyber-attacks to take vital information from many significant sectors of society. In the face of these accusations, Chinese representatives have routinely rejected assertions that the PRC and PLA are sponsors to cyber-attacks on western establishments. Representatives also reject the allegations that the PLA has the competency and abilities to assault the infrastructure and systems of other nations. In a proclamation in 2015, Chinese President Xi Jinping stated, “the Chinese government does not engage in theft of commercial secrets in any form, nor does it encourage or support Chinese companies to engage in such practices in any way.” He also asserted, “Cybertheft of commercial secrets and hacking attacks against government networks are both illegal; such acts are criminal offenses and should be punished according to law and relevant international conventions.”[148] There are specific laws created by the PRC to battle cybercrime in the nation:

[148] Tweed, David. "U.S.-China Hacking Deal Seen on Civilian, Not Company Hits." *Bloomberg.com*. September 22, 2015. Accessed December 17, 2015. U.S.-China Hacking Deal Seen on Civilian, Not Company HitsU.S.-China Hacking Deal Seen on Civilian, Not Company HitsU.S.-China Hacking Deal Seen on Civilian, Not Company Hits

Table 3: Criminal Procedure Law of the People's Republic of China

Article Number	Definition[149]
285	Whoever violates state regulations and intrudes into computer systems within formation concerning state affairs, construction of defense facilities, and sophisticated science and technology is be sentenced to not more than three years of fixed-term imprisonment or criminal detention.
286	Whoever violates states regulations and deletes, alters, adds, and interferes in computer information systems, causing abnormal operations of the systems and grave consequences, is to be sentenced to not more than five years of fixed-term imprisonment or criminal detention; when the consequences are particularly serious, the sentence is to be not less than five years of fixed-term imprisonment. Whoever violates state regulations and deletes, alters, or adds the data or application programs installed in or processed and transmitted by the computer systems, and causes grave consequences, is to be punished according to the preceding paragraph. Whoever deliberately creates and propagates computer virus and other programs which sabotage the normal operation of the computer system and cause grave consequences is to be punished according to the first paragraph.
287	Whoever uses a computer for financial fraud, theft, corruption, misappropriation of public funds, stealing state secrets, or other crimes is to be convicted and punished according to relevant regulations of this law.

However, there are hacker collections that exhibit connections to the PRC and/or government-run organizations, and individuals from China's hacking underworld have publically affirmed that they or a group that they were members of are now or at one point were sponsored by the state. United States security

[149] China. National People's Congress. *Criminal Procedure Law of the People's Republic of China*. Beijing: China Procuratorial, 1997. Print.

firms have also published research on hacking groups that that link them to the Chinese government, like Mandiant and FireEye for example.[150] On top of all this, there also exists official government documents issued by the Chinese government that confirms that the People's Liberation Army has cyber-defense and warfare divisions.

While many media sources, like the *Washington Times*, continuously accuse the Chinese Communist Party for the bulk of attacks emanating from Asia, the party adamantly renounces these assertions. For example, hundreds of executive officers in Great Britain received messages from the chief of the British Secret Service informing them that they had fallen victim to cyber-attacks from the Chinese government.[151] Party representatives allege that these assailants are either other governments feigning to be China, non-governmental sanctioned hackers, or the attacks themselves are fabrications created by anti-Chinese factions in the United States and Western Europe.

The Science of Military Strategy and the Role of the Party

There has been acknowledgement from the Chinese government itself that it has been developing and plans to further its cyber-capabilities. According to Joe McReynolds at the Center for Intelligence Research and Analysis, the newest issue of *The Science of Military Strategy* is confirmation of these cyber-capabilities. Because it is disseminated by the PLA itself, the publication is

[150] Mandiant Inc. APT1: Exposing One of China's Cyber Espionage Units. Rep. N.p.: Mandiant, 2014. Print. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.
[151] Finch, Amanda, and Julian Wadley. "Waking up to the Realities of the Cyber Threat." *IISP Pulse* Summer 11.6 (2011). Accessed January 14, 2016.

meticulously studied by many western experts.[152] It provides the leading examination of the function of the Chinese government in cyber-crime, as well as the Communist party's position on hacking. *The Science of Military Strategy* is produced "once in a generation," McReynolds said, and "is the first time we've seen an explicit acknowledgement of the existence of China's secretive cyber-warfare forces from the Chinese side".[153]

There is a fundamental cultural difference that might significantly contribute to both the direct and indirect relationship between the Chinese Communist Party (CCP) and Chinese hackers. According to the interview performed with the member of Anonymous Serbia, he believes that foreign policy and hacking can be related. According to him, "countries like China don't have to be worried about answering to their own public, so they tend to lead, on the surface, at least, more offensive foreign policy. Nowadays, hacking is part of that foreign policy."[154] Normally, Western nations do not require its non-governmental citizens to attempt to collect information of any kind on the government's behalf while in peacetime. Most other nations do not seem to participate in the types of actions that Chinese hackers are involved in. These activities, according to some observers, move far past intelligence-gathering, and into a much more malicious territory. The CCP does not make a differentiation between these two responsibilities, because its citizens are supposed to openly participate in actions

[152] Kulacki, Gregory. *The Chinese Military Updates China's Nuclear Strategy*. Rep. Union of Concerned Scientists, 2015. Accessed September 30, 2015. http://www.ucsusa.org/nuclear-weapons/us-china-relations/chinas-nuclear-weapons-strategy#.VyWUlHry1_k
[153] Rudolph, Josh. "China Reveals Its Cyberwar Secrets." *China Digital Times (CDT)*. March 19, 2015. Accessed March 28, 2016. http://chinadigitaltimes.net/2015/03/china-reveals-its-cyberwar-secrets/
[154] Uzunovic, Agan. "Chinese Hackers." E-mail interview by author. April 5, 2016

that further the growth of the nation. McReynolds wrote that the publication has a tendency to "focus heavily on the central role of peacetime 'network reconnaissance' — that is, the technical penetration and monitoring of an adversary's networks — in developing the PLA's ability to engage in wartime network operations."[155] According to McReynolds, the People's Liberation Army does not see the same types of distinctions as its Western counterparts in military and civilian roles, and their philosophy for future conflicts even muddles these views further:

> In the high-tech local war which we will face in the future, the role of the masses as the main body of the war is embodied by the country. The great power of the people's war is released through comprehensive national power, the combination of peace time and war time, the combinations of the military and the civilian, and the combination of war actions and non-war actions. Besides the direct participation and cooperation with the army's operations in the region where war happens, the masses will support the war mainly by political, economic, technical, cultural and moral means.[156]

There is another arena where the Chinese system differs from Western practices and that is corporate espionage. Much like the PLA's ideologies in intelligence gathering, gathering trade secrets falls under the same umbrella of intelligence gathering for the sake of national-growth. Due to its nominally

---

[155] Aftergood, Steven. "China's Science of Military Strategy (2013)." *Federation Of American Scientists*. August 3, 2015. Accessed March 28, 2016. https://fas.org/blogs/secrecy/2015/08/china-sms/

[156] Guangqian, Peng. Youzhi, Yao. The Science of Military Strategy, *Military Publishing House, Academy of Military Science of the Chinese People's Liberation Army*, 2005, p. 455

communist nature, the PRC does not make the distinguishment from the nation's domestic production, and all of the country's possessions and resources are regarded as property of the Chinese people. Money, banking, and other financial organization usually comprise one of the pillars of society and are vital for the maintaining stability. This ranks even higher than that of the development of military capabilities, as a weak financial base makes military growth futile. For a growing society like the PRC, which seeks to enhance its military might, the PRC must first develop a strong financial base. So with this in mind, hacking attempts that support the promotion of government initiatives, whether state-sponsored or independent, would be seen as beneficial and more likely to be allowed to continue by officials. In a 2002 official warning from Taiwanese police for example, it stated that "some 300,000-plus hackers in China who break into high-tech companies around the world and steal confidential information and programs, with the tacit consent of the Chinese government."[157] Also evaluating this topic, iSight Chief Executive, John Watters has said "Nothing suggests that Chinese authorities are vigilantly prosecuting those who are attacking foreign interests. They turn a blind eye to it as long as it doesn't oppose national interests."[158] One reason for these types of actions by the government revolves around the country's increasing energy requirements, as the Chinese government finds itself under greater pressures to sustain its economic momentum as it moves into the future, they must acquire stability in their energy

[157] "Taiwan: Hacker Working for PRC Firm Arrested," *Taipei Times*. June 26, 2002. Accessed December 21, 2015.
[158] Vardi, Nathan. "Chinese Takeout," *Forbes*. July 25, 2005. Accessed October 13, 2015. http://www.forbes.com/forbes/2005/0725/054.html

resources. Chinese hackers, whether working for personal gain or as state operatives, are finding that the exchange of information associated with the petroleum and energy industries are extremely profitable and/or extremely important to the growth of the Chinese state. So out of either a nationalistic viewpoint or financial gain, Chinese hackers are finding that the government is more apt to turn a blind eye to these types of practices or even facilitating the hacks themselves.

These types of attacks span more than a decade and are not only easily recognized but can also be readily researched. Much like many media outlets, researchers find the prospect of state-sponsored hacker groups very interesting. In 2004, Shawn Carpenter, an expert at Sandia National Laboratories managed to uncover a sizable cyber-espionage organization with links to known state-sponsored hackers in China's Guangdong Province. These hackers were given the alias "Titan Rain" by the Federal Bureau of Investigation. Like stated before, the attackers behind Titan Rain assaulted hundreds of systems in a single night.

PLA Unit 61398: Advanced Persistent Threat 1

A recent publication issued by the American cyber-security firm Mandiant exposes a group based out of Shanghai and the shocking history of hacking and cyber-theft linked to it. Mandiant argues that this group of hackers is Chinese military-based, with specific connections to the PLA. Since 2004, Mandiant (which has since been purchased by FireEye) has researched cyber-security penetrations at organizations globally. They dub this individual group APT1, and

proclaim that it is one of more than 20 “advanced persistent threat” or APT groups that originate from China. The firm witnessed the Chinese group break into over a hundred computer systems belonging to Western government institutions and corporations. According to the publication, “though our visibility of APT1’s activities is incomplete, we have analyzed the group’s intrusions against nearly 150 victims over seven years.”[159] This group is believed to be the Second Bureau of the PLA’s General Staff Department’s Third Department, which is usually recognized by the military label “Unit 61398.”

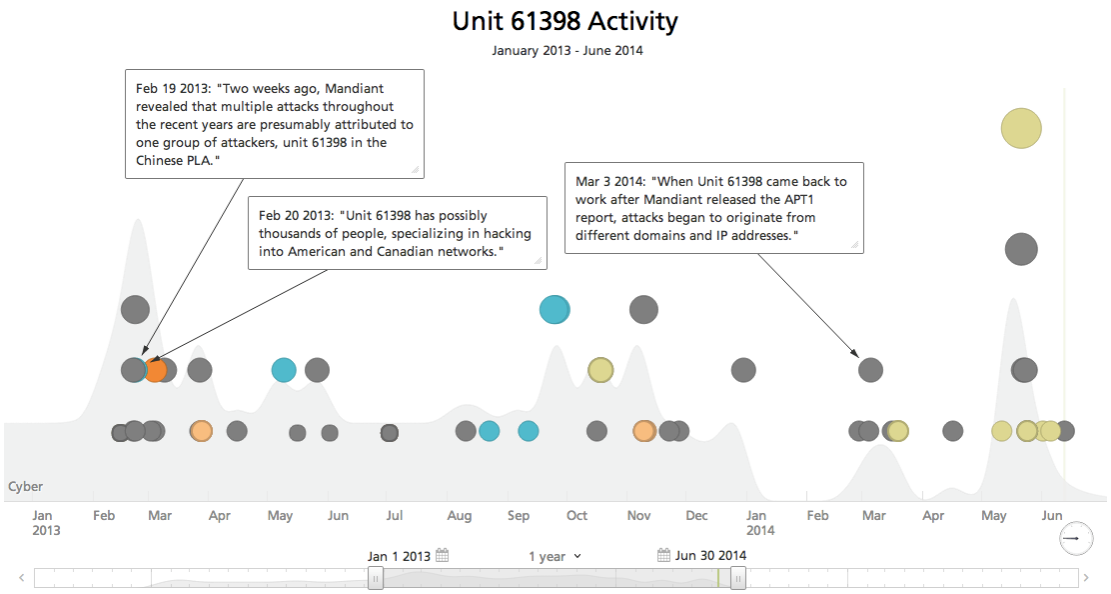

Figure 14: Unit 61398 Activity. The first shows the activity of the PLA group that is accused of attacking American systems.

[159] Mandiant Inc. APT1: Exposing One of China's Cyber Espionage Units. Rep. N.p.: Mandiant, 2014. Print. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

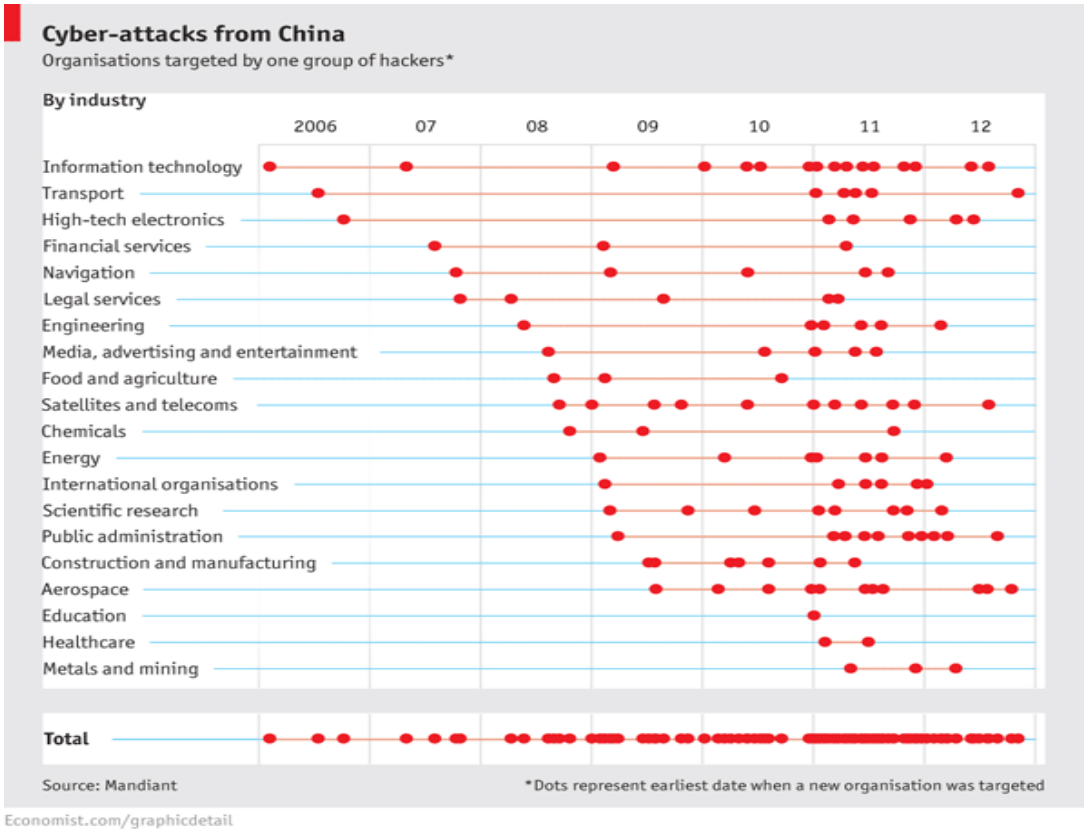

Figure 15: Cyber-Attacks Performed by APT1.[160]

Throughout Mandiant's investigation, APT1 besieged almost two dozen industries, paying special consideration to areas that could be deemed as crucial to the Chinese government and state, like technology and military for example. The evidence that Mandiant has compiled linking this hacker group to the Chinese military is extraordinary. The key is in the location of Unit 61398's headquarters. Military Unit 61398 is located in the Shanghai's Pudong New Area, and their station itself is a facility twelve floors high built in 2007. The group's undertakings have been traced by the security organization to Shanghai

[160] "Hack-attack." *The Economist*. The Economist Newspaper. February 20, 2013. Accessed March 30, 2016. http://www.economist.com/blogs/graphicdetail/2013/02/daily-chart-12

networks, with two of the four found being located in the same area as Unit 61398 base of operations. Ninety-eight percent of the IP (Internet Protocol) addresses used by APT1 were traced back to China, and 99.8 percent of the HTRAN communication IP addresses were registered to the Shanghai networks.[161] IP addresses are used to identify a device while on a network like the internet. Through the use of IP addresses, three individual hackers ("UglyGorilla," "DOTA," and "SuperHard") were traced both to APT1 and the Pudong area, each with very detailed links.[162] HTRAN communication IP addresses are proxy server addresses used to mask a host's address. Even after the report's publication, the Chinese government denied any wrongdoing. In response, a government webpage asserted that many of these attacks were performed using commandeered IP addresses and that IP addresses are very misleading.[163]

In 2013, The U.S. Department of Defense openly accused Chinese state-sponsored hacking groups of attacking and extracting information from United States civilians, government, military, and businesses. The founder of security firm Ivincea, Anup Ghosh, added "the acknowledgement by the Pentagon is a first step in publicly declaring the threat." This comes more than a year after the United States Justice Department officially indicted five military officials from

[161] Marcus, Jonathan. "China Condemns Hacking Report by US Firm Mandiant" *BBC News*. February 20, 2013. Accessed October 31, 2015. http://www.bbc.com/news/world-us-canada-21515259

[162] Mandiant Inc. APT1: Exposing One of China's Cyber Espionage Units. Rep. N.p.: Mandiant, 2014. Print. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

[163] Vijayan, Jaikumarcc. "Chinese Hackers Master the Art of Lying in Wait." *Computerworld*. May 8, 2013. Accessed March 28, 2016. http://www.computerworld.com/article/2497171/cyberwarfare/chinese-hackers-master-the-art-of-lying-in-wait.html

China for breaking into the systems of American corporations and pilfering exclusive records and documents. American prosecutors revealed that the group had stolen trade secrets from five businesses as well as a labor union. “The alleged hacking appears to have been conducted for no reason other than to advantage state-owned companies and other interests in China, at the expense of businesses here in the United States,” attorney general Eric Holder said in a dramatic press conference that included posters of the five individuals.[164] In response, Qin Gang of the foreign ministry replied that the accusations were “made up” and could very much “damage Sino-American co-operation and mutual trust” if the charges stood. He would go on to state that “China is a staunch defender of network security, and the Chinese government, military and associated personnel have never engaged in online theft of trade secrets.”[165] The alleged conspirators were all known members of the PLA’s Unit 61398. Speaking on behalf of the PRC, Qin Gang of the Ministry of Foreign Affairs proclaimed the the arrests are “based on fabricated facts,” and that “China is steadfast in upholding cyber security. The Chinese government, the Chinese military and their relevant personnel have never engaged or participated in cyber theft or trade secrets.”[166]

While if the previously mentioned PLA unit indeed is in operation, it

[164] Caponi, Steven. "United States v. China: The Battle over Cyber-Espionage Results in Criminal Charges." *Cybersecurity Law Watch*. May 19, 2014. Accessed October 17, 2015. https://cybersecuritylawwatch.com/2014/05/19/united-states-v-china-the-battle-over-cyber-espionage-results-in-criminal-charges/

[165] Carsten, Paul. "China: U.S. Cyber Spying Accusations 'made Up' and Will Damage Trust." *Reuters*. May 19, 2014. Accessed November 15, 2015. http://www.reuters.com/article/us-cybercrime-usa-china-response-idUSBREA4I0GL20140519

[166] Rudolph, Josh. "China Dismisses U.S. Cyber-Spying Charges - China Digital Times (CDT)." China Digital Times (CDT). May 19, 2014. Accessed May 01, 2016. http://chinadigitaltimes.net/2014/05/chinese-govt-netizens-angry-u-s-cyber-spying-charges/.

performs its tasks in the shadows, that does not mean that there are no other cyber divisions within the PLA or the government. Quite the contrary, in February 2014, President Xi Jingpin announced the establishment of a group named the Central Internet Security and Informatization Leading Group.[167] The group exists as an information security organization, and is led prominent individuals like Lu Wei (who also heads the Party's Cyberspace Administration).[168] Both the military unit within the PLA and the group led by Lu Wei show that both the Party and the military are very concerned about the country's cyber-capabilities, and are beginning to move within sight of the international community.

Operation Shady Rat (2006-2010)

In 2005 and 2006 a group attacked a total of seventy-two organizations, corporations, and governments, as well as the International Olympic Committee. Over fourteen different countries were victims, and it was one of the largest hacking operations ever at that time. Having been blamed for attacks on the IMF and Sony, the media and many experts pointed the finger at the Chinese government. Dmitri Aplerovich, vice president of McAfee securities said that "This is the biggest transfer of wealth in terms of intellectual property in history. The scale at which this is occurring is really, really frightening, we were surprised by the enormous diversity of the victim organizations and were taken aback by the audacity of the perpetrators." The operation gained its name from the tools used in the attack: remote access tools (RAT).

[167] Bandurski, David. "What's up with the PLA?" CMP Newswire. May 21, 2015. Accessed May 01, 2016. http://cmp.hku.hk/2015/05/21/38822/.
[168] Ibid

Recognized as one of the biggest chains of cyber-attacks since the rise of hackers, McAfee securities unraveled in 2014 what they dubbed “Operation Shady Rat.” Using common spear-phishing tactics, systems that are attacked are bombarded with personal communications (usually emails) that are sent to people within. Once the file is opened malware is downloaded onto the victims computer and the file is opened. Once opened a program will initiate and exploit whatever the hackers are trying to do. The targets are found in many locations globally. McAfee revealed that the systems are penetrated using “obfuscated or encrypted HTML comments embedded in otherwise benign websites, in order to indirectly control compromised endpoints,” FireEye securities added that this type of method is linked to a collection identified as “Comment Group”, who is assumed to be connected to either the PRC or the PLA.[169]

[169] Pidathala, Vinay, Zheng Bu, Thoufique Haq, and Darien Kindlund. "Operation Beebus." *FireEye*. February 1, 2013. Accessed December 25, 2015. https://www.fireeye.com/blog/threat-research/2013/02/operation-beebus.html

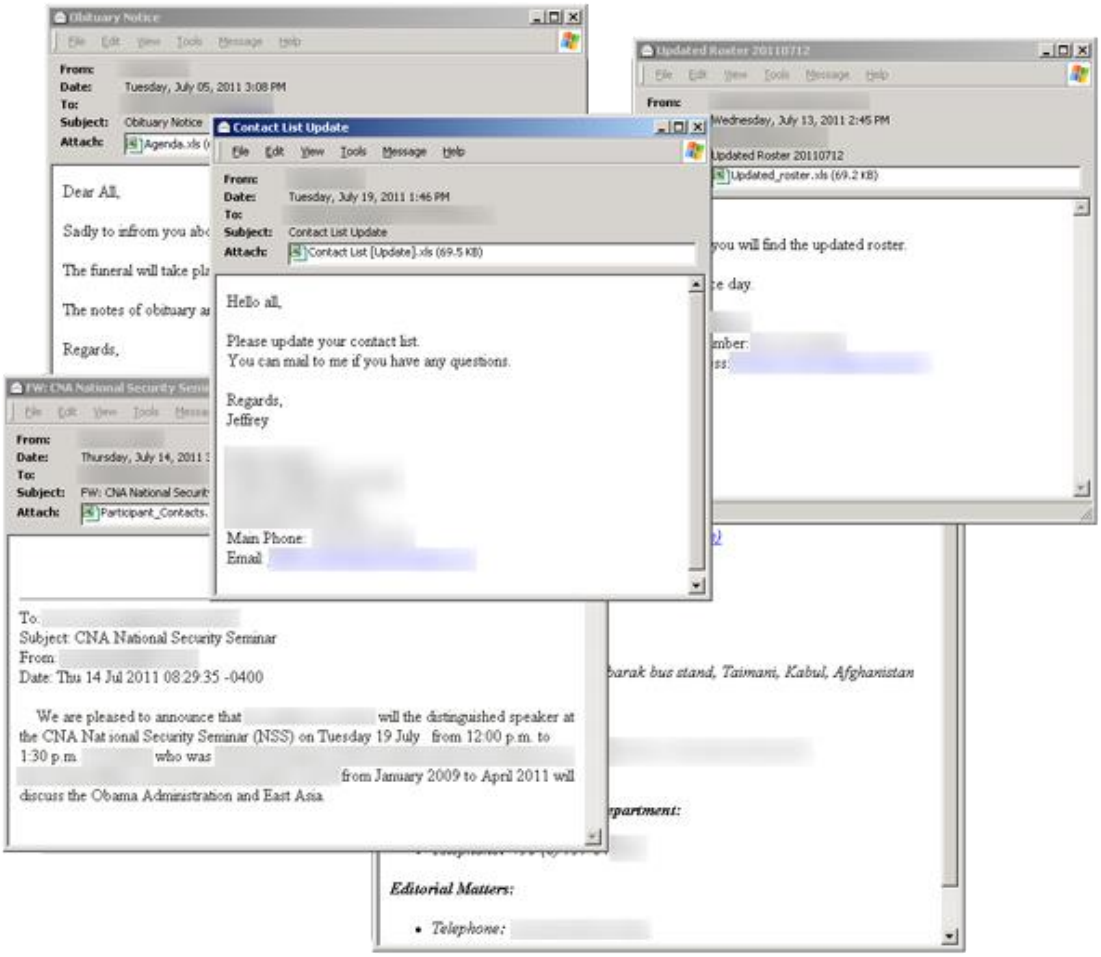

Figure 16: Shady Rat Phishing Attack.[170]

Operation Aurora (2009-2010)

Discovered in late 2009, this operation was a high-profile attack against Google and linked directly by security expert Brian Krebs to the Chinese government.[171] Operation Aurora takes its name due to the fact that attackers

[170] Lau, Hon. "The Truth Behind the Shady RAT." *Symantec Security Response*. August 4, 2011. Accessed March 30, 2016. http://www.symantec.com/connect/blogs/truth-behind-shady-rat

[171] Krebs, Brian. "New Clues Draw Stronger Chinese Ties to 'Aurora' Attacks." *Krebs on Security*. January 20, 2010. Accessed April 15, 2016. http://krebsonsecurity.com/2010/01/new-clues-suggest-stronger-chinese-role-in-aurora-attacks/

utilized the Aurora Trojan horse program. Attackers used a database of Gmail accounts accumulated by the Federal Bureau of Investigation and law enforcement agencies. “In mid-December [2009], we detected a highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual property from Google,” said an online message by Google’s chief legal officer, David Drummond. Nevertheless, Google stated that the incident affected “at least twenty other large companies from a wide range of businesses – including the Internet, finance, technology, media and chemical sectors – have been similarly targeted.”[172] Chinese IP addresses were uncovered as the main servers in the attacks as the source servers in the attacks, and Symantec securities linked the Chinese hacker group Hidden Lynx to the attacks. Another reason the attacks are believed to be Chinese in origin is because much of the programing in the attacks is written using Chinese tools and with Chinese code.[173] Because the region of origin for the attacks was traced back to Chinese servers and the code itself was created using distinct Chinese computer code, it is not uncalled for for these security experts to blame Chinese individuals or groups for these attacks.

Experts believe that the attacks from Aurora originated from Shanghai Jiaotong University and the Lanxiang Vocational School in the Shandong

[172] Naone, Erica. "Google Reveals Chinese Espionage Efforts." *MIT Technology Review*. January 13, 2010. Accessed December 17, 2015. https://www.technologyreview.com/s/417087/google-reveals-chinese-espionage-efforts/
[173] Stewert, Joe. "Operation Aurora: Clues in the Code." *Dell SecureWorks*. January 19, 2010. Accessed Setpember 30, 2015. https://www.secureworks.com/blog/research-20913

province.[174] On the other hand, Chinese authorities both within the government as well as with the universities have denied any wrongdoing. Li Zixiang with the Lanxiang school even formally stated that "investigations …found no trace the attacks originated from our school."[175] Rong Lanxiang, the founder of the Lanxiang School made a public statement in which he said "The report (by *The New York Times*) is merely a fabrication. We do have students joining the PLA, but it is part of the national policy of military recruitment. Our computing center has more than 2000 computers, but this fact has nothing to do with Baidu. [The report] said we have a military background, this is a joke."[176]

Deep Panda (2011-2015)

Between 2011 and 2015, a group that went by many different names attacked various high profile organizations in one of the greatest acts of cyber-espionage ever. Also known as Shell Crew," the group has been linked to attacks on the health care providers Anthem, and Premera, in addition to the U.S. Office of Personnel Management. The penetration of data on the health care providers resulted in the theft of the financial and medical records of approximately eleven million individuals. The group's activities were first seen in 2011 with smaller attacks on the American and Japanese organizations related to infrastructure. It was named "Deep Panda" due to its links to China.

---

[174] Areddy, James T. "People's Republic of Hacking." The Wall Street Journal. February 18, 2010. Accessed May 1, 2016. http://www.wsj.com/articles/SB10001424052748704140104575057490343183782.
[175] Beach, Sophie. "People's Republic of Hacking (Updated) - China Digital Times (CDT)." China Digital Times (CDT). February 20, 2010. Accessed May 02, 2016. http://chinadigitaltimes.net/2010/02/chinese-school-denies-cyber-attack-on-google/.
[176] Ibid

Figure 17: A FBI Alert for Deep Panda. A email alert sent to all members of the Federal Bureau of Investigation about the security issues brought forth by the Deep Panda attacks.[177]

[177] A Little Sunshine. "China To Blame in Anthem Hack?" *Krebs on Security RSS*. February 6, 2015. Accessed March 30, 2016. http://krebsonsecurity.com/2015/02/china-to-blame-in-anthem-hack/

Figure 18: Logo and Calling Card for Deep Panda. The logo for Deep Panda as it left on sites as a calling card on websites after an attack.[178]

Operation Poisoned Hurricane (2014)

First discovered in early 2014, this group targeted several internet service providers, government organizations, an American media company, and a financial institution. The hackers used malware that was connected to websites like adobe.com and outlook.com, but individuals were re-routed to pages that hackers had set up to look legitimate. Security firm FireEye identified twenty-one websites that were hijacked this way.

All twenty-one websites were configured using the same internet service,

[178] A Little Sunshine. "China To Blame in Anthem Hack?" *Krebs on Security RSS*. February 6, 2015. Accessed March 30, 2016. http://krebsonsecurity.com/2015/02/china-to-blame-in-anthem-hack/

Hurricane Electric's public DNS (domain name service) service, meaning that all twenty-one sites were run by the same organization. FireEye believes that the targets were involved in the Hong Kong democracy protests. The People's Republic of China is the being in all likelihood to be concerned with attaining this goal.[179] The attack was given its name because the system attacked belonged to a corporation called Hurricane Electric. The cyber-security firm FireEye tracked the operation and published their findings. In their conclusions they state that they observed "the use of Hurricane Electrics public DNS resolvers to redirect command and control traffic." They also state that "the fact that the malware appears to beacon to legitimate domains may lull defenders into a false sense of security."[180]

Emissary Panda (2015-Present)

In 2015, the Emissary Panda group targeted a wide range of organizations involved in defense manufacturing and international relations. Also known as TG-3390, the websites compromised by the group were connected with five diverse establishments, which industrial firms, predominantly those providing to the sector of defense; U.S. embassies involved in international relations; government organizations; energy enterprises; and several non-government organizations (NGOs). Based on this information, researchers with Dell SecureWorks Counter

[179] Kovacs, Eduard. "APT Group Hijacks Popular Domains to Mask C&C Communications: FireEye." *Security Week*. August 6, 2014. Accessed March 28, 2016. http://www.securityweek.com/apt-group-hijacks-popular-domains-mask-cc-communications-fireeye

[180] Homan, Joshua, Mike Scott, and Ned Moran. "Operation Poisoned Hurricane." *Threat Research Blog*. FireEye, August 6, 2014. Accessed April 23, 2016. https://www.fireeye.com/blog/threat-research/2014/08/operation-poisoned-hurricane.html

Threat Unit believe that the group's objective was to gather information pertaining to defense, manufacturing data and blueprints, and vital information found in government and NGO systems.[181]

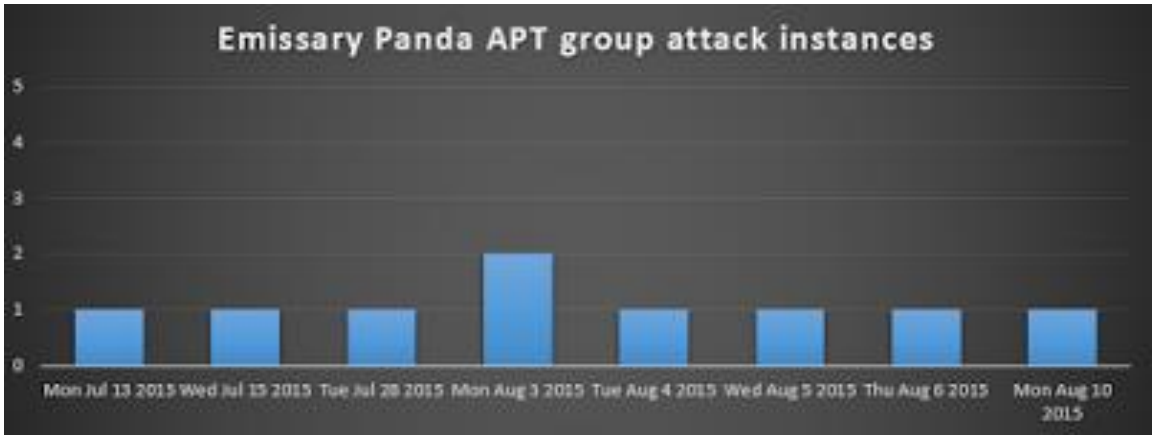

Figure 19: Emissary Panda Attacks 2015. Amount of attacks per week by the Emissary Panda group between July 13 and August 10, 2015.[182]

Wekby (2015)

Also known as APT 18, Dynamite Panda, and TG-0416, this group stole four and a half million patient records from Community Health Systems in 2015. Using a method that is shown to be very familiar to Chinese hackers, spear-phishing emails were sent that were titled "Important: Flash Update" to company

[181] Dell SecureWorks Counter Threat Unit Threat Intelligence. "Threat Group-3390 Targets Organizations for Cyberespionage." *Dell Secure Works*. August 5, 2005. Accessed January 14, 2016. https://www.secureworks.com/research/threat-group-3390-targets-organizations-for-cyberespionage

[182] Desai, Deepen. "Chinese Cyber Espionage APT Group 'Emissary Panda' Activity Update." *Chinese Cyber Espionage APT Group 'Emissary Panda' Activity Update*. August 8, 2015. Accessed September 9, 2015. https://www.zscaler.com/blogs/research/chinese-cyber-espionage-apt-group-%E2%80%98emissary-panda%E2%80%99-activity-update

personnel. The hackers used a zero-day attack using Adobe Flash Player code. The emails contained a link that led the readers to an apparently official download page. Those who clicked on the link downloaded a malicious file containing malware. “This group typically targets companies in the aerospace and defense, construction and engineering, technology, financial services, and healthcare industry verticals,” said Charles Carmakal, managing director at Mandiant securities “The attacker has been known to steal intellectual property related to medical technology and pharmaceutical manufacturing processes.”[183]

[183] Mimoso, Michael. "APT Gang Branches Out to Medical Espionage in Community Health Breach." *Threatpost The First Stop for Security News*. August 19, 2014. November 17, 2015. https://threatpost.com/apt-gang-branches-out-to-medical-espionage-in-community-health-breach/107828/

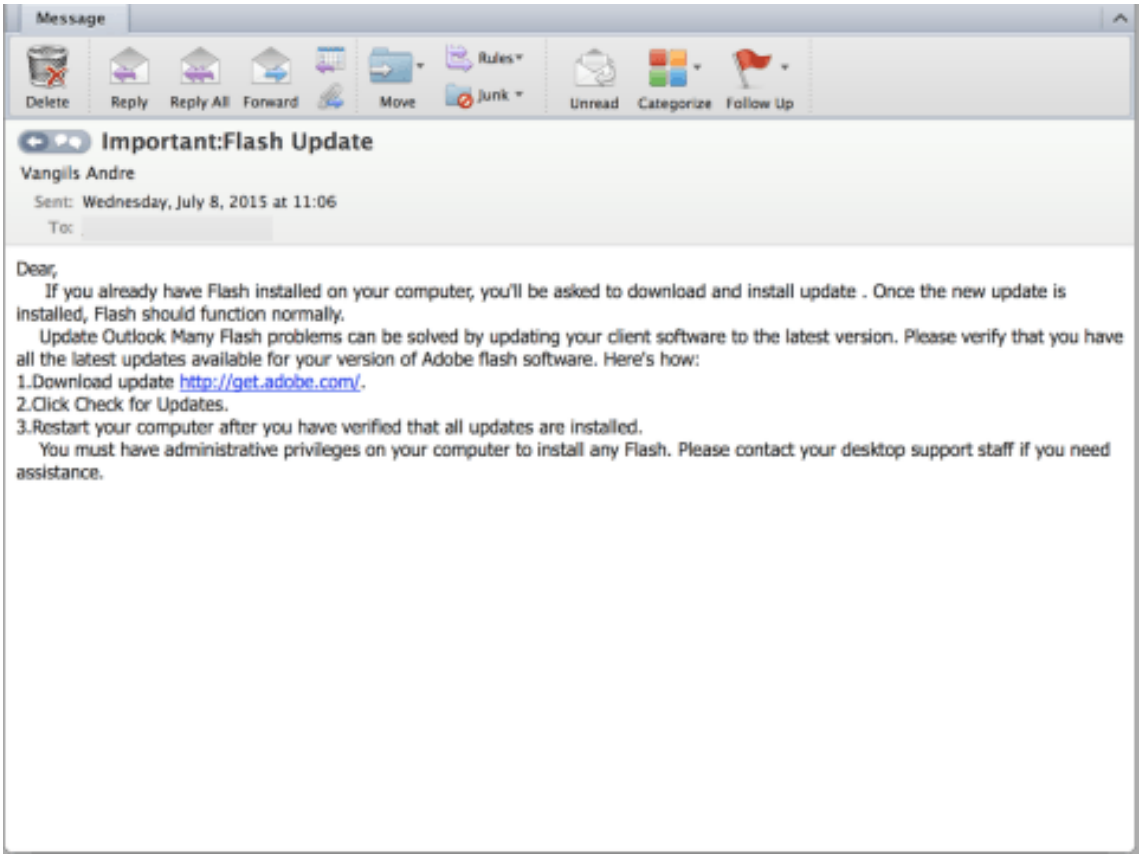

Figure 20: Wekby Phishing Attack[184]

[184] Paganini, Pierluigi. "Wekby APT Attacks Leverage Hacking Team Exploits." Security Affairs. July 11, 2015. Accessed October 1, 2015. http://securityaffairs.co/wordpress/38500/cyber-crime/wekby-apt-ht-exploits.html

CHAPTER SIX:

FREELANCE ACTORS, THE GREY AREA

As with everything in this world, hackers in China do not exist in a world of simple black and white. There are grey areas between that cannot be defined in such polarized categories. In the world of Chinese hacking, there are groups and individuals that move between the lines separating independent actors and state-sponsored agents. These individuals are best described as freelance actors. They are those who render their services to the highest bidder, even if that bidder is the Chinese government. There are groups that at one moment carry out attacks that are significantly linked to the Chinese government, and then performing attacks with no link at all to the government. Due to the fluid allegiances of these groups, it is sometimes difficult to unravel the motivations for their attacks.

Wan Tao, one of China's first nationalistic hackers believes that there is another separate group of hackers that he labeled "underground hackers." They are best described as black-market operatives who peddle their unique abilities or act on their own volition in order to increase their reputation in hopes of expanding their business opportunities. "Their business model is to sell,"[185] Wan declares. He provides his own experiences as a prominent hacker as proof. As a member of the prominent hacking group, the "Green Army," he e-mail bombed the Japanese prime minister in 1997 and conducted many attacks on U.S. webpages after the 2001 EP-3 incident. He acted on his own initiative and not as

[185] "Masters of the Cyber-universe." *The Economist*. April 6, 2013. December 13, 2015. http://www.economist.com/news/special-report/21574636-chinas-state-sponsored-hackers-are-ubiquitousand-totally-unabashed-masters

an agent of the Communist party. Yet, as his reputation grew he was solicited to offer his skills.

While attending a security conference in Guangzhou in 1998, Wan was approached by law enforcement seeking his assistance. He designed a software system in order for law enforcement to ascertain the authors of anonymous postings on webpage bulletin boards. "I'm a security expert," he explains. "They had the need." He was later approached by the PLA for assistance, but he declined to help. He did instead help recruit other hackers into their services. When anti-Japanese riots shook China in 2005, the Communist Party worked to mute the same nationalistic attitude it had nurtured for so many years. Wan Tao was at one time free to attack non-nationals online, and then he was commanded by the powers that be to remove seditious substance from his personal website. "I thought I had freedom online," says Wan. "But I was wrong."[186]

Wan's story did in fact come full circle. In 2011 and 2012, cyber-crime skyrocketed in China. According to official statistics, approximately 260 million Chinese were victims of cyber-attacks during this time.[187] Those who were once motivated by nationalistic and patriotic causes where lured into illegality by financial motivations. In response, Chinese authorities fought back against cyber-crime within their borders. The man who was once approached by the PLA for assistance was jailed. No longer in jail and working as a cybersecurity consultant, he stresses that at no time provided he provide hacking services to the Chinese

[186] Beech, Hannah. "China's Red Hackers: The Tale of One Patriotic Cyberwarrior" *Time*. Febuary 21, 2013. Accessed January 17, 2016. http://world.time.com/2013/02/21/chinas-red-hackers-the-tale-of-one-patriotic-cyberwarrior/
[187] Ibid

government.

Wan Tao's story is the perfect example of the fluidity of hacking culture in China. At any point, many Chinese hackers could be classified under any of the three categorizations (independent, state-sponsored, freelance). Much like every other job, hacking can be all about profit. This is not always the case, but it is a strong motivation nonetheless. During a speech, the Guangdong Province governor Lu Ruihua, stated "as long as they [Chinese hackers] do not break the law, there is no loss, regarding the master hacker; we can send them a thousand dollars a month to support them! Some sectors of the system are not easy to find vulnerabilities; why cannot I use the hacker's knowledge and skills."[188] It is under these circumstances where normally independent actors can become agents of the state, either on a short-term or long-term basis.

Much like that of an independent actor, nationalism can be a large motivation for why Chinese hackers blur the line between independent and state-sponsored. Over the past few generations, China has been battling to regain its power on the global stage. When examining freelance Chinese hackers, it is important to know that Chinese nationalism, in the view of many, is especially concerned with returning the nation to its previous glory. It is not entirely about conflict with the west or the US, though this is a part of that impetus. As stated before, the majority of Chinese hackers are young (many are of college age) and can be fanatical about topics that affect their nation's global image and standing. From the earliest days of the Chinese hacking scene, many attacks emanating

[188] "广东：高薪请黑客堵"漏洞" Jingan Times cia China.com.cn. May 24, 2002. Accessed May 3, 2016. http://www.china.com.cn/chinese/difang/150045.htm

from China have been politically fueled and are commonly a means to protest against actions or perceived stances of foreign countries. However, as significant as nationalistic motivations are, monetary motivations seem to be becoming almost as important. Many companies and organizations are taking advantage of this, including the Chinese government. There are a significant number of patriotic hackers that steal commercial secrets with the intention of selling them to the highest bidder, which in some cases could be the government.

Yujun Yumin

Recently, as a segment of its effort to improve and develop the PLA, the government has wanted to extract its assets located in the citizen populace. In 2003, the PLA declared the program of *yujun yumin*, or in discovering military aptitude within its population.[189] Consequently, ascertaining where the government concludes and the public commences is becoming a progressively difficult task, as has been an ongoing challenge throughout this study. Exploiting enemy weakness to overcome relative deficits in strength has been central to Chinese military planning as far back as the early Han dynasty, and was central to Mao Zedong's theory of guerrilla warfare. *Unrestricted Warfare*, a book published in 1999 by the People's Liberation Army, applies this longstanding approach to modern informational and cyber warfare, suggesting that the blurred

[189] Mulvenon, James. and Tyroler-Cooper, Rebecca Samm "China's Defense Industry on the Path to Reform" *U.S.-China Economic and Security Review Commission,* (Ithaca: Cornell University Press, 2009) *dtic.mil/dtic/tr/.../u2/a523026.pdf*

lines examined throughout this paper are there by design.[190]

Sometimes the Chinese government calls upon its people to act for the government. Other times hackers aid in fulfilling or completing the government's agenda purely by following their own nationalistic ideals. A member of the Chinese hacking group "Honker Union," codenamed "Prince," also provides a good example of this and the experiences of a freelance hacker. "Prince" has gone on record saying that the group's actions, as well as the individuals themselves, are strictly based on nationalistic agendas. "We never proactively launch attacks for no reason. We only do it when China's national interest is harmed," he said. "In most of the cases, we just fight back."[191]

He says the hackers act on their own but that occasionally they are called on by the government to help track those believed to be working against the state. "I independently have some cooperation with the Chinese government but it's all off the record," he said. "The government normally asks me to follow the electronic footprint of different hackers, gather information on hackers, and ultimately submit official reports."[192]

We should note that this kind of activity is certainly not restricted to China. There are examples of this within the United States. In 1997, the Federal Bureau of Investigation sought to test how vulnerable America's networks were by hiring outside hackers to attack their own systems. They employed "a team of eccentric

---

[190] Summers, Timothy C. "Here's What Chinese Hackers Really Want." *MarketWatch*. October 1, 2015. Accessed February 14, 2016. http://www.marketwatch.com/story/heres-what-chinese-hackers-really-want-2015-10-01

[191] Yoon, Eunice. "Hacker Weighs in on US-China Cyber Spat." *CNBC*. September 23, 2015. Accessed September 30, 2015. http://www.cnbc.com/2015/09/23/hacker-weighs-in-on-us-china-cyber-spat.html

[192] Ibid

computer geniuses who occasionally helped out with law enforcement investigations and who called themselves 'The L0pht.'"[193] They could break passwords stored in any operating system. They could decrypt any satellite communications. They even created software that could hack into someone's computer and control it remotely, spying on the user's every keystroke, changing the user's files, kick the user off the internet, or send the user to any site of their choosing.[194] The group was even brought to Capitol Hill on May 19, 1998 to testify about the status of the internet. This group operated in whatever capacity suited them best, and in this case just so happened to work in concert with a government agency to do what they did best, and that was hack.

GhostNet (2006–2009)

GhostNet was a cyber-espionage operation that penetrated computers and stole records from many international governments and public organizations. The system used by the attackers corrupted systems with a Trojan horse branded "gh0st RAT", which granted them comprehensive, instantaneous command of the system. The gh0st RAT malware has been linked to China's Hainan Province. Ultimately, there existed a network of approximately 1,300 contaminated systems in over 100 nations. In addition, approximately 30 percent of these systems were deemed as highly importance victims . These systems encompassed several departments of international affairs, international businesses, embassies, and media outlets. Christened GhostNet, this cluster of

[193] Kaplan, Fred M. *Dark Territory: The Secret History of Cyber War*. New York, NY: Simon and Schuster, 2016. P.91
[194] Ibid. 93

systems was centered on Asian governments.

Gh0st RAT was capable of seizing complete influence of contaminated systems, and was able to explore and take particular documents, as well as secretly controlling devices like cameras. When asked about the government of China's involvement, Wenqi Gao a spokeman for the Chinese Consulate in New York rejected the notion that it was implicated. "These are old stories and they are nonsense," Gao said. "The Chinese government is opposed to and strictly forbids any cybercrime."[195]

Hidden Lynx (2009–2012?)

In February 2013, a security company named Bit9 which is now known as Carbon Black Inc, issued a proclamation divulging that a recognized collection titled "Hidden Lynx" was able to breach the company's system. The group is an expert group of assailants with sophisticated skills. The group has existed ever since 2009, and is almost certainly a group that its skills in exchange for financial gain. Many of the attacks linked to this group involve the retrieval of information, and the targets are a significant arrangement of businesses and governments. The collection utilizes innovative methods, separating them from other hacking organizations. According to security firm Symantec, Hidden Lynx is a good-sized group consisting of between at most 100 people.

[195] Beardson, Timothy. *Stumbling Giant: The Threats to China's Future*. Yale UP, 2013. Print.

Black Vine (2012–2014)

In early 2014, the biggest healthcare data breach ever occurred on one of the largest health insurers in the United States, Anthem. The Anthem breach began in May 2014 when the company was contaminated with a malicious program called Mivast. The breach was not discovered until February of 2015, almost a year after it had commenced. The invaders stole the records and confidential information of millions of individuals. Symantec's report on Operation Aurora also offered evidence linking the same group to a China-based IT security company known as Topsec, which also happens to be funded by the government. [196]

Like I stated earlier, the world of Chinese hacking does not exist purely in blacks and whites. There are groups like Hidden Lynx and individuals like Wan Tao that move between the classifications of independent and state-sponsored agents. They are those who are likely to be motivated by financial means and are the most likely to sell their services to the highest bidder. Wan Tao, for example, has gone on record stating that independently he has helped the government track individuals and do other services. Black Vine, on the other hand, has been directly linked to the organization TopSec, which is a state-run group. These hackers are the ones that make it most difficult to make classifications of the Chinese hacking culture.

---

[196] Goodin, Dan. "Group That Hacked Anthem Shared Weaponized 0-days with Rival Attackers." *Arstechnica*. July 28, 2015. Accessed September 9, 2015. http://arstechnica.com/security/2015/07/group-that-hacked-anthem-shared-weaponized-0-days-with-rival-attackers/

CHAPTER SEVEN:

CYBER-CRIME AND THE GLOBAL COMMUNITY

The topic of cyber-crime is extraordinarily important in a world where online activities encompass the most essential facets of our lives. U.S. officials even alerted President Barack Obama that China had hacked into his campaign computer systems, gaining access to position papers, finances, and emails. Obama had decided later to confront the Chinese directly on their rampant penetrations of U.S. computer networks. On March 11, 2013, President Obama's National Security Consultant Thomas Donilon, presented at the New York Asia Society. At the event he said that American corporations were more and more apprehensive "about sophisticated, targeted theft of confidential business information and proprietary technologies through cyber intrusions emanating from China on an unprecedented scale."[197]

The subject of Chinese cyber-attacks is a moderately new field owing to the modern expansion of the phenomenon. However, international concerns about hacking as a whole are not. In 1990, the United Nations General Assembly approved computer crime laws. Key nations began forming approaches and doctrines to battle online crime and defend information as early as 1997. At the turn of the century, regulations and procedures were established internationally throughout the global community. Countless countries have created legislation with defense and prosecution of cybercrimes in mind. Many researchers and

[197] Kaplan, Fred M. *Dark Territory: The Secret History of Cyber War*. New York, NY: Simon and Schuster, 2016. P. 221

academics had become attracted to the fields of cybercrime, the internet, and cyberespionage as information was easily accessible.

A Borderless Crime

Many computer crimes are transnational, meaning that they cross borders and jurisdictions. A cybercrime can be committed in one country with a victim in another country, thousands of miles away. Because every nation is connected to the Internet, cybercriminals can commit offenses from anywhere, and victims can be anywhere. Moreover, offenders can be very mobile, moving from one place to the next very quickly if needed. Hackers can physically operate in one country, easily access data on computers located in a different continent, and then move to another location to evade law enforcement. The borderless nature of cybercrime also means that any nation can be targeted and its citizens victimized from anywhere in the world. This makes it very difficult, if not impossible, for law enforcement to determine the country in which the crime was actually committed and then to locate the specific offender. If an offender is found, it may be unclear what agency should have jurisdiction to adjudicate the offense. To fix this issue, the United Nations has developed legislature to combat cybercrime. In 2000, the organization passed Resolution 55/64, which includes:

> (a) States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies.
> (d) Legal systems should protect the confidentiality, integrity, and

availability of data and computer systems from unauthorized impairment and ensure that criminal abuse is penalized.[198]

In order for transnational crimes to be prosecuted, there has to be two kinds of jurisdiction: substantive and investigative. Both of these are required for cases of transnational cyber-crimes. States must be able to uphold that their systems of criminal law utilized be applied to the case in question. It is important that a nation's laws can be applied to cases that take place partly within its territories, or even outside their territory. In the case of cybercrime and internet crimes, this can be tricky because these forms are global in scope. Additionally, it needs to be seen if these nations have the legal ability to carry out investigative actions that concern the territories of other states. In many of these cases, international cooperation is required. In order to provide for cases such as cyber-crime, multilateral and bilateral levels of international treaty laws are created, as well as national laws that form the basis for an individual nation's cooperation.

Creation of International Laws

As a result of the mounting danger of worldwide cybercrime and the political and legal complications in organizing law enforcement that can traverse international lines, numerous endeavors have been created to enable and assist collaboration amongst nations. One of the earliest and more important attempts

[198] United Nation General Assemby. *Combating the Criminal Misuse of Information Technologies: Resolution*. New York: UN, 2001. Print.

the Council of Europe's Convention on Cybercrime.[199] The treaty has remained an issue of considerable deliberation by the European Union since as early as 1997. The objective of the convention was seen as an effort to "harmonize laws against malicious hacking, virus writing, fraud and child pornography on the net. It also aims to ensure that police forces in separate countries gather the same standard of evidence to help track and catch criminals across borders."[200] Since cybercrime often has a tendency to transcend an individual nation's borders, the measures to combat it must also of course be of an international nature.

The treaty's contents are a great example of international legislation that pertains to computer-based crimes. Articles 2 through 11 of the Treaty accomplish the goal of prohibiting specific types of conduct.[201] Each nation that endorses the treaty is expected to agree upon specified criminal offenses and the associated consequences for crimes perpetrated within that nation, the territories in their possession, on a state's vessel or aircraft, or by their citizens when they are in a foreign country. The offenses are categorized in four areas of crime: scam and counterfeiting, child pornography, intellectual property, and computer system intrusion or hacking. Other articles in the treaty establish a legal procedure for each state, incorporating human rights protections, legal processes, and the apparatuses and actions for criminal investigations.[202]

---

[199] *Convention on Cybercrime = Convention Sur La Cybercriminalité*. Strasbourg: Council of Europe, 2002. Print.
[200] Ward, Mark. "Cybercrime Treaty Condemned." *BBC News*. December 18, 2000. Accessed March 17, 2016. http://news.bbc.co.uk/2/hi/science/nature/1072580.stm
[201] Robel, Dan. *International Cybercrime Treaty: Looking Beyond Ratification*. SANS Institute. 2006. Accessed March 28, 2016. *https://www.sans.org/.../**international-cybercrime-treaty-rat***
[202] Ibid

Most major countries have created national legislation related to cybercrime extradition and have provided for legal assistance concerning other nations in cases where these nations call for assistance in matters that extend across borders. Almost all countries in Europe have reported that such legislation exists within their countries. The United Kingdom was the first country to create national legislation in the subject of cybercrime. The legislation in question was "The Computer Misuse Act of 1990," which contained punishments for computer-related crimes.[203] Many nations soon followed suit. China promulgated the "Computer Information Network and Internet Security Protection and Management Regulations, 1997" to police internet activities. However, the Chinese legislation dealt mainly with national security within China instead of the deterrence of cybercrime. Chinese President Xi Jingping connected cybersecurity with national security as well as with the country's growth, remarking that "there is no national security without cybersecurity, and no modernization without informatization."[204] In China, internet security has been a focal point of public opinion and government policy. In a survey conducted by the Chinese publication *Global Times,* 98.1 percent of individuals support the government's initiative of creating specialized laws to protect internet security.[205] To this day, the U.S. has the widest range of legal conditions regarding

[203] Great Britain. *Computer Misuse Act 1990: Elizabeth II. 1990. Chapter 18*. London: H.M.S.O., 1990. Print.
[204] Cindy. "China Wants Party's Voice "Strongest in Cyberspace" - China Digital Times (CDT)." *China Digital Times (CDT)*. 08 Jan. 2016. Web. 02 May 2016.
[205] Rudolph, Josh. "Documents Show How Weibo Filters Sensitive News - China Digital Times (CDT)." China Digital Times (CDT). March 03, 2016. Accessed May 01, 2016. http://chinadigitaltimes.net/2016/03/documents-show-how-weibo-filters-sensitive-news/.

cybercrime, incorporating provisions concerning violations, investigation, as well as punishment.

There are also international coalitions and groups that have legislation pertaining to the subject. The European Commission, the executive board that administers the European Union, announced in 1995 a data protection directive.[206] It concentrated on the online security of personal data. The directive was amended again in 2011 to combat new technology and circumstances. NATO, the North America Treaty Organization, created cyber-defense responsibilities for its controlled websites by establishing the NATO Computer Incident Response Capability (NCIRC).

Along the same lines, the Council of Europe implemented significant proposals to its member states regarding criminal procedural law on cybercrime in 1995. The group's recommendations formed the basis of the Convention on Cybercrime on 2001. The international treaty contained policies to ease the gathering of evidence, as well as the prosecution and punishment of criminals, for the nations involved. By agreeing to the treaty, the country agreed to create a minimum set of national laws to mirror the treaty's laws on particular computer-based crimes.

More modernly, because of the hacking efforts of the US actors on China and the efforts of Chinese hackers on US systems, the United States and Chinese governments have made some serious breakthroughs in international cooperation to combat cybercrime. According to *New York Times* writer David E.

[206] European Commission. *Report from the Commission: First Report on the Implementation of the Data Protection Directive (95/46/EC)*. Luxembourg: Office for Official Publications of the European Communities, 2003. Print.

Sanger, “The United States and China are negotiating what could become the first arms control accord for cyberspace, embracing a commitment by each country that it will not be the first to use cyberweapons to cripple the other’s critical infrastructure during peacetime.” To counter Sanger’s statement about the international accord, *People’s Daily* writer Liu Xin proclaimed that the agreement “is expected to halt all disputes” and “could serve as a role model for other countries”.[207] From both sides, there is definitely mutual cooperation. There are other countries with incredible cyber-capabilities like Russia that would be the next logical addition to any international accords, like for two nations with significant cyber-power to come together and form even a shaky alliance is a step in the right direction.

The cyberwarfare capabilities of the three nations is indeed moving into the forefront of the minds of everyday citizens, as well as in popular culture. The novel *Ghost Fleet* by Singer and Cole, portrays the increasing fears of cyber-attacks and cyber warfare on a global scale. Chinese cyber warfare lays the groundwork for war in the narrative on the story. They prey on real fears of today in an attempt to predict tomorrow. For example, American equipment and systems manufactured in China are infiltrated without the knowledge of the American public. Hackers are active, public, and a military force in China as well, even well equipped with the fictitious tools needed to create an army of red hackers as the unthinking arm of the government. The authors romanticize the topic making it very popular, especially in the cyber-defense circles. It expresses

[207] Wade, Samuel. "Xi Pledges Cooperation vs. Hacking as Sanctions Loom - China Digital Times (CDT)." China Digital Times (CDT). September 22, 2015. Accessed May 02, 2016. http://chinadigitaltimes.net/2015/09/hacking-sanctions-threat-hangs-over-xis-u-s-visit/.

the anxiety of the American public, and what makes it even more significant is that it is not entirely wrong.

Some of the themes of the novel are very much a reality. In 2012 Microsoft researchers found that computers that had never before turned on were already compromised by malware.[208] In 2015, Lenovo, one of the world's biggest computer manufacturers, was found selling systems with malware and other malicious software pre-installed. The software was named the "Superfish Malware", and it was found with the ability to analyze the users internet usage in an attempt to interject advertisements into the computers web browser.[209]

Behind President Xi Jingping, China has indeed made progress in halting the efforts of hackers in the mainland. In 2014, the Cyberspace Administration of China (CAC) was founded. It is now the group responsible for the governance of the internet within the PRC. During the group's first meeting, President Xi stressed that the lack of network security throughout the country is indeed negatively affecting the whole. According to Bill Hagestad, in his book *Chinese Cyber Crime*, the President called for "unified planning, unified deployment, unified effort, and unified implementation."[210] The President offered this, "in today's world, the ever-changing information technology revolution of the international political, economic, cultural, social, military and other areas of development had a profound impact… China is in this tide, it affected more and

[208] Jeffers, David. "Your PC May Come with Malware Pre-installed." *PCWorld*. 14 Sept. 2012. Web. 12 May 2016.
[209] Khandelwal, Swati. "Lenovo Shipping PCs with Pre-Installed 'Superfish Malware' That Kills HTTPS." *The Hacker News*. 19 Feb. 2015. Web. 12 May 2016.
[210] Hagestad, William. *Chinese Cyber Crime: China's Hacking Underworld*. San Bernardino, 2015.

more… we must also realize that we are relatively backward in terms of innovation."[211] It are instances like this that makes *Ghost Fleet* such a strong portrayal. It takes subjects that strike fear in the present, and magnify them in the context of war.

The current landscape of cybercrime legislation involves ongoing legal reform, yet it is fairly new in terms of international law. States are increasingly aware that it requires legal responses across multiple platforms and across borders. These have a tendency to include criminal, civil, and administrative laws. Traditional laws can sometimes provide nations with the ability to prosecute cybercrime cases, but these cases usually have both the target and attacker within the country's borders and do not require the aid of investigation of other nations. Although cybercrime law does date back several decades, it has only been in the past decade that cybercrime has become a significant global issue. In order to combat such a dynamic field and the ever-changing nature of computer-based concepts, the introduction of shared definitions and agreement on specific offenses have been created in an attempt to prosecute new crimes.

[211] Hagestad, William. *Chinese Cyber Crime: China's Hacking Underworld*. San Bernardino, 2015.

REFERENCES

"A History of Anonymous." *InfoSec*. InfoSec Institute, October 24, 2011. Accessed March 30, 2016. http://resources.infosecinstitute.com/a-history-of-anonymous/

A Little Sunshine. "China To Blame in Anthem Hack?" *Krebs on Security RSS*. February 6, 2015. Accessed March 30, 2016. http://krebsonsecurity.com/2015/02/china-to-blame-in-anthem-hack/

Aftergood, Steven. "China's Science of Military Strategy (2013)." *Federation Of American Scientists*. August 3, 2015. Accessed March 28, 2016. https://fas.org/blogs/secrecy/2015/08/china-sms/

Anderson, Benedict R. O'G. *Imagined Communities: Reflections on the Origin and Spread of Nationalism*. London: Verso, 1991. Print.

“Anti-Chinese riots continue in Indonesia,” *CNN News CNN.com/World*. August 29, 1998. Accessed August 23, 2005. http://www.cnn.com/WORLD/asiapcf/9808/29/indonesia.riot

Areddy, James T. "People's Republic of Hacking." The Wall Street Journal. February 18, 2010. Accessed May 1, 2016. http://www.wsj.com/articles/SB10001424052748704140104575057490343183782.

Bandurski, David. "A “Year of Innovation” for Internet Controls." CMP Newswire. January 7, 2016. Accessed May 01, 2016. http://cmp.hku.hk/2016/01/07/39575/.

Bandurski, David. "China's Cyber-diplomacy." CMP Newswire. December 21, 2015. Accessed May 01, 2016. http://cmp.hku.hk/2015/12/21/39527/.

Bandurski, David. "China Soul Searches Its Obsession with Internet Addiction." CMP Newswire. May 14, 2009. Accessed May 01, 2016. http://cmp.hku.hk/2009/05/14/1623/.

Bandurski, David. "How the Internet Has Changed China." CMP Newswire. October 10, 2010. Accessed May 01, 2016. http://cmp.hku.hk/2010/10/25/8238/.

Bandurski, David. "Three Cheers for China's Cyber-Volunteers." CMP Newswire. April 13, 2016. Accessed May 01, 2016. http://cmp.hku.hk/2016/04/13/39684/.

Bandurski, David. "What's up with the PLA?" CMP Newswire. May 21, 2015. Accessed May 01, 2016. http://cmp.hku.hk/2015/05/21/38822/.

Baum, Richard. *Systematic Stresses and Choices: China's Road to Soft Authoritarian Reform.* 2004

Beach, Sophie. "People's Republic of Hacking (Updated) - China Digital Times (CDT)." China Digital Times (CDT). February 20, 2010. Accessed May 02, 2016. http://chinadigitaltimes.net/2010/02/chinese-school-denies-cyber-attack-on-google/.

Beardson, Timothy. *Stumbling Giant: The Threats to China's Future*. Yale UP, 2013. Print.

Beech, Hannah. "China's Red Hackers: The Tale of One Patriotic Cyberwarrior" *Time*. Febuary 21, 2013. Accessed January 17, 2016. http://world.time.com/2013/02/21/chinas-red-hackers-the-tale-of-one-patriotic-cyberwarrior/

"Biggest Data Breaches." *Privacy Risks Advisors*. 2015. Accessed January 2, 2016. http://www.privacyrisksadvisors.com/data-breach-toolkit/worlds-biggest-data-breaches/

Caponi, Steven. "United States v. China: The Battle over Cyber-Espionage Results in Criminal Charges." *Cybersecurity Law Watch*. May 19, 2014. Accessed October 17, 2015. https://cybersecuritylawwatch.com/2014/05/19/united-states-v-china-the-battle-over-cyber-espionage-results-in-criminal-charges/

Carsten, Paul. "China: U.S. Cyber Spying Accusations 'made Up' and Will Damage Trust." *Reuters*. May 19, 2014. Accessed November 15, 2015. http://www.reuters.com/article/us-cybercrime-usa-china-response-idUSBREA4I0GL20140519

Casaretto, John. "Advanced_persistent_threat_lifecycle." *SiliconANGLE*. July 17, 2013. Accessed March 28, 2016. https://conceptdraw.com/a2051c3/preview

Casserly, Martyn. "Who Is Anonymous? A Short History of Hacktivism." *PC Advisor*. November 18, 2015. Accessed March 30, 2016. http://www.pcadvisor.co.uk/feature/internet/what-is-hacktivism-short-history-anonymous-lulzsec-arab-spring-3414409/

Castello, Sam. "U.S., Chinese Hackers Continue Web Defacements." *CNN*. May 2, 2001. Accessed April 14, 2016. http://www.cnn.com/2001/TECH/internet/05/02/china.hacks.idg/

Chang, Lennon Yao-chung. *Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention across the Taiwan Strait*. Cheltenham, Glos, UK: Edward Elgar, 2012.

Chao, Leon. "The Red Hackers Chinese Youth Infused with Nationalism." *CHINASCOPE*. January 27, 2008. Accessed February 7, 2016. http://chinascope.org/m/content/view/456/148/1/1/

"China Protests French Retailer Carrefour." *nbcnews.com*. April 19, 2008. Accessed September 2, 2015. http://www.nbcnews.com/id/24218173/ns/world_news-asia_pacific/t/china-protests-french-retailer-carrefour/

"China Pulls Plug On Internet Blogs." *ChinaTechNews*. Asia Media Network, March 19, 2004. Accessed October 14, 2015. http://www.chinatechnews.com/2004/03/19/1029-china-pulls-plug-on-internet-blogs

"China Wants Party's Voice "Strongest in Cyberspace" - China Digital Times (CDT)." China Digital Times (CDT). January 08, 2016. Accessed May 02, 2016. http://chinadigitaltimes.net/2016/01/china-wants-partys-voice-strongest-in-cyberspace/.

"Chinese Censorship and China's Online Netizens Social Movements." *Visions of Travel*. 2005. Accessed December 21, 2015. http://www.visionsoftravel.org/chinese-censorship-china-online-netizens-social-movement/

Chu, Tianbi, "Chåinese Hacker History/Looking Back on Chinese Hacker History," Accessed August 9, 2015. http://www.blogchina.com/news/source/310.htm

Convention on Cybercrime = Convention Sur La Cybercriminalité. Strasbourg: Council of Europe, 2002. Print.

"Crisis Management At Carrefour." *EastSouthWestNorth*. April 26, 2008. Accessed September 27, 2015. http://www.zonaeuropa.com/20080428_1.htm

Danchev, Dancho. "Baidu DNS Records Hijacked by Iranian Cyber Army" *ZDNet*. January 12, 2010. Accessed March 30, 2016. http://www.zdnet.com/article/baidu-dns-records-hijacked-by-iranian-cyber-army/

Dell SecureWorks Counter Threat Unit Threat Intelligence. "Threat Group-3390 Targets Organizations for Cyberespionage." *Dell Secure Works*. August 5, 2005. Accessed January 14, 2016. https://www.secureworks.com/research/threat-group-3390-targets-organizations-for-cyberespionage

Desai, Deepen. "Chinese Cyber Espionage APT Group 'Emissary Panda' Activity Update." *Chinese Cyber Espionage APT Group 'Emissary Panda' Activity Update*. August 8, 2015. Accessed September 9, 2015. https://www.zscaler.com/blogs/research/chinese-cyber-espionage-apt-group-%E2%80%98emissary-panda%E2%80%99-activity-update

Deweese, Steve. *Capability of the People's Republic of China (PRC) to Conduct Cyber Warfare and Computer Network Exploitation*. Rep. Northrop Grumman. Print.

Downs, Erica Strecker, and Phillip C. Saunders. "Legitimacy and the Limits of Nationalism: China and the Diaoyu Islands." *International Security* 23, no. 3 (1998): 114. Accessed March 21, 2016. doi:10.2307/2539340.

Espiner, Tom. "Security experts lift lid on Chinese hack attacks", November 23, 2005. Accessed December 13, 2015. http://news.zdnet.com/2100-1009_22-145763.html

European Commission. *Report from the Commission: First Report on the Implementation of the Data Protection Directive (95/46/EC)*. Luxembourg: Office for Official Publications of the European Communities, 2003. Print.

Finch, Amanda, and Julian Wadley. "Waking up to the Realities of the Cyber Threat." *IISP Pulse* Summer 11.6 (2011). Accessed January 14, 2016.

Gertz, Bill. "Cheers to Good Frenemies! China Investing in Cyberwarfare Superiority." *The Washington Times*. April 1, 2015. Accessed March 28, 2016. http://www.washingtontimes.com/news/2015/apr/1/china-invests-cyberwarfare-compete-us-military/?page=all

Glasius, Marlies. *Global Civil Society Yearbook 2009: Poverty and Activism*. London: SAGE Publications, 2009. Print.

Goodin, Dan. "Group That Hacked Anthem Shared Weaponized 0-days with Rival Attackers." *Arstechnica*. July 28, 2015. Accessed September 9, 2015. http://arstechnica.com/security/2015/07/group-that-hacked-anthem-shared-weaponized-0-days-with-rival-attackers/

"Google Attack Puts Spotlight on China's Red Hackers." *Reuters*. Thomson Reuters, January 20, 2010. Accessed January 14, 2016.

http://www.reuters.com/article/us-google-china-hackers-idUSTRE60J20820100120

Great Britain. *Computer Misuse Act 1990: Elizabeth II. 1990. Chapter 18*. London: H.M.S.O., 1990. Print.

Guangqian, Peng. Youzhi, Yao. The Science of Military Strategy, *Military Publishing House, Academy of Military Science of the Chinese People's Liberation Army*, 2005, p. 455

"Hack-attack." *The Economist*. The Economist Newspaper. February 20, 2013. Accessed March 30, 2016. http://www.economist.com/blogs/graphicdetail/2013/02/daily-chart-12

Hagestad, William. *Chinese Cyber Crime: China's Hacking Underworld*. San Bernardino, 2015.

Henderson, Scott J. *The Dark Visitor: Inside the World of Chinese Hackers*. Scott Henderson, 2007. Print.

Hernandez, Javier C. "China Corruption Fight Extends to Top Officials in Beijing and Shanghai." *The New York Times*. 2015. March 28, 2016. http://www.nytimes.com/2015/11/12/world/asia/china-crackdown-corruption-beijing-shanghai-ai-baojun-lu-xiwen.html

Hollin, C. "Criminological psychology". *In The Oxford Handbook of Criminology*, M. Maguire, R. "Morgan, and R. Reiner, Eds. Oxford University Press, Oxford, U.K., 2002.

Homan, Joshua, Mike Scott, and Ned Moran. "Operation Poisoned Hurricane." *Threat Research Blog*. FireEye, August 6, 2014. Accessed April 23, 2016. https://www.fireeye.com/blog/threat-research/2014/08/operation-poisoned-hurricane.html

"Honker Purpose" H.U.C.honkerchina.net. July, 2015. Accessed May 5, 2016 http://www.honker.net.cn/about/zongzhi.html

Hook, Leslie. "China's Post-90 Generation Make Their Mark " *Financial Times*. July 9, 2012. Accessed August 29, 2015. http://www.ft.com/cms/s/0/4fcbab6c-c67d-11e1-963a-00144feabdc0.html#axzz47NCEKi9b

Hsaio, Russell. "Critical Node: Taiwan's Cyber Defense and Chinese Cyber-Espionage." *The Jamestown Foundation*. December 5, 2013. Accessed February 14, 2016.

http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews[tt_news]=41721&cHash=3505e552d9d50d88cfc539af1319e699#.VyWOqnry1_k

Hvistendahl, Mara. "Hackers: The China Syndrome." *Popular Science*. April 23, 2009. Accessed March 30, 2016. http://www.popsci.com/scitech/article/2009-04/hackers-china-syndrome

"Internet Sovereignty." CMP Newswire. 2015. Accessed May 01, 2016. http://cmp.hku.hk/2015/09/30/39279/.

Janczewski, Lech, and Andrew M. Colarik. *Cyber Warfare and Cyber Terrorism*. Hershey: Information Science Reference, 2008.

Jeffers, David. "Your PC May Come with Malware Pre-installed." *PCWorld*. 14 Sept. 2012. Web. 12 May 2016. http://www.pcworld.com/article/262325/your_pc_may_come_with_malware_pre_installed.html

Joshi, Shashank. "Iran, the Mossad and the Power of Cyber-warfare – Telegraph Blogs." *The Telegraph*. October 3, 2013. Accessed December 17, 2016.

Kaplan, Fred M. *Dark Territory: The Secret History of Cyber War*. New York, NY: Simon and Schuster, 2016.

Khandelwal, Swati. "Lenovo Shipping PCs with Pre-Installed 'Superfish Malware' That Kills HTTPS." *The Hacker News*. 19 Feb. 2015. Web. 12 May 2016. http://thehackernews.com/2015/02/lenovo-superfish-malware.html

Kirk, Jeremy. "Chinese Ex-hacker Says Working for the Government Would Be Too Boring." *Network World*. November 8, 2012. Accessed April 15, 2016. http://www.networkworld.com/article/2161287/data-center/chinese-ex-hacker-says-working-for-the-government-would-be-too-boring.html

Komisi Nasional Hak Asasi Manusia Indonesia (Indonesian National Commission on Human Rights), Statement of the National Commission on Human Rights Concerning the Unrest in Jakarta and the Surrounding Areas. June 2, 1998. www.komnas.go.id/english/cases/cs_text02.html

Kovacs, Eduard. "APT Group Hijacks Popular Domains to Mask C&C Communications: FireEye." *Security Week*. August 6, 2014. Accessed March 28, 2016. http://www.securityweek.com/apt-group-hijacks-popular-domains-mask-cc-communications-fireeye

Kovacs, Nadia. "What Is the Difference Between Black, White and Grey Hat Hackers?" *What Is the Difference Between Black, White and Grey Hat Hackers?* April 17, 2015. Accessed November 16, 2016.

http://www.howtogeek.com/157460/hacker-hat-colors-explained-black-hats-white-hats-and-gray-hats/

Krebs, Brian. "New Clues Draw Stronger Chinese Ties to 'Aurora' Attacks." *Krebs on Security*. January 20, 2010. Accessed April 15, 2016. http://krebsonsecurity.com/2010/01/new-clues-suggest-stronger-chinese-role-in-aurora-attacks/

Kulacki, Gregory. *The Chinese Military Updates China's Nuclear Strategy*. Rep. Union of Concerned Scientists, 2015. Accessed September 30, 2015. http://www.ucsusa.org/nuclear-weapons/us-china-relations/chinas-nuclear-weapons-strategy#.VyWUlHry1_k

L'Express, Flamme olympique: ce qui s'est vraiment passé à Paris (French). April 8, 2008. Accessed October 19, 2015. http://www.lexpress.fr/info/quotidien/actu.asp?id=469562

Laliberte, Andre, and Marc Lanteigne. *The Chinese Party-state in the 21st Century: Adaptation and the Reinvention of Legitimacy*. London: Routledge, 2008.

Lau, Hon. "The Truth Behind the Shady RAT." *Symantec Security Response*. August 4, 2011. Accessed March 30, 2016. http://www.symantec.com/connect/blogs/truth-behind-shady-rat

Lewis, Leo. "China's Blue Army of 30 computer experts could deploy cyber warfare on foreign powers," *The Australian*. May 27, 2011. Accessed February 21, 2016. http://www.theaustralian.com.au/business/technology/chinas-blue-army-could-conduct-cyber-warfare-on-foreign-powers/story-e6frgakx-1226064132826

Li Zi, "The Chinese Hacker Evolution," *People in Focus Weekly*, March 10, 2005. Accessed February 21, 2016. http://net.chinabyte.com/386/1920386.shtml

Liang, Guo, and Markle Corporation. "Surveying Internet Usage and Its Impact in Seven Chinese Cities." *Center for Social Development Chinese Academy of Social Sciences.* 2007. Accessed January 17, 2016. http://www.policyarchive.org/handle/10207/16013

Long San, "Let's look back on the days of the Red Hacker Alliance," *Juntuan*. October 24, 2005. Accessed November 17, 2005. http://www.juntuan.cn/user1/2334/archives/2005/9612.shtml

Lynden, Jacki. "In China, Avoiding The 'Great Firewall' Internet Censors." *NPR*. September 7, 2013. Accessed April 11, 2016. http://www.npr.org/templates/story/story.php?storyId=220106496

MacKinnon, Rebecca. "Chinese Protest BBS Crackdown." *RConversation*. March 20, 2005. Accessed March 28, 2016. http://rconversation.blogs.com/rconversation/2005/03/chinese_protest.html

Makortoff, Kayleena. "Anonymous to Fight IS, Bigotry after Brussels." *CNBC*. March 24, 2016. Accessed March 30, 2016. http://www.cnbc.com/2016/03/24/after-brussels-anonymous-to-tackle-isis-and-bigotry.html

Mandiant Inc. APT1: Exposing One of China's Cyber Espionage Units. Rep. N.p.: Mandiant, 2014. Print. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

Marcus, Jonathan. "China Condemns Hacking Report by US Firm Mandiant" *BBC News*. February 20, 2013. Accessed October 31, 2015. http://www.bbc.com/news/world-us-canada-21515259

Martin, Patrick. "US Adopts Aggressive Anti-China Posture in Aftermath of Spy Plane Crisis." *World Socialist Web Site*. April 15, 2001. Accessed December 25, 2015. https://www.wsws.org/en/articles/2001/04/chin-a15.html

"Masters of the Cyber-universe." *The Economist*. April 6, 2013. December 13, 2015. http://www.economist.com/news/special-report/21574636-chinas-state-sponsored-hackers-are-ubiquitousand-totally-unabashed-masters

McAffee Securities. *Net Losses: Estimating the Global Cost of Cybercrime*. Report. Santa Clara: Center for Strategic and International Studies, 2014.

McMillan, Robert. "As Hacking Hits Home, China Strengthens Cyber Laws." *PCWorld*. May 11, 2009. Accessed March 18, 2016.

Mimoso, Michael. "APT Gang Branches Out to Medical Espionage in Community Health Breach." *Threatpost The First Stop for Security News*. August 19, 2014. November 17, 2015. https://threatpost.com/apt-gang-branches-out-to-medical-espionage-in-community-health-breach/107828/

Mulvenon, James. and Tyroler-Cooper, Rebecca Samm “China’s Defense Industry on the Path to Reform” *U.S.-China Economic and Security*

Review Commission, (Ithaca: Cornell University Press, 2009) dtic.mil/dtic/tr/.../u2/a523026.pdf

Naone, Erica. "Google Reveals Chinese Espionage Efforts." *MIT Technology Review*. January 13, 2010. Accessed December 17, 2015. https://www.technologyreview.com/s/417087/google-reveals-chinese-espionage-efforts/

Nuttall, Chris. "Chinese Protesters Attack Indonesia through Net." *BBC News*. August 19, 1998. Accessed March 28, 2016. http://news.bbc.co.uk/2/hi/science/nature/154079.stm

Orlowski, Andrew. "Michael Hauben, Netizen, Dies." *The Register*. June 30, 2001. Web. March 28, 2016. http://www.theregister.co.uk/2001/06/30/michael_hauben_netizen_dies/

Paganini, Pierluigi. "Wekby APT Attacks Leverage Hacking Team Exploits." Security Affairs. July 11, 2015. Accessed May 03, 2016. http://securityaffairs.co/wordpress/38500/cyber-crime/wekby-apt-ht-exploits.html.

Pan, Philip P. "Chinese Crack Down On Student Web Sites." *The Washington Post*. March 24, 2005. Accessed September 28, 2015. http://www.washingtonpost.com/wp-dyn/articles/A61334-2005Mar23.html

Pidathala, Vinay, Zheng Bu, Thoufique Haq, and Darien Kindlund. "Operation Beebus." *FireEye*. February 1, 2013. Accessed December 25, 2015. https://www.fireeye.com/blog/threat-research/2013/02/operation-beebus.html

"Race to the Bottom": Corporate Complicity in Chinese Internet Censorship." *Human Rights Watch* 18, no. 8 (August 2006). Accessed April 11, 2016.

"Re-Defining Cyberspace - China Digital Times (CDT)." China Digital Times (CDT). October 09, 2015. Accessed May 01, 2016. http://chinadigitaltimes.net/2015/10/re-defining-cyberspace/.

Reilly, James. Strong Society, Smart State: The Rise of Public Opinion in China's Japan Policy. New York: Columbia UP, 2012. 126.

Robel, Dan. *International Cybercrime Treaty: Looking Beyond Ratification*. SANS Institute. 2006. Accessed March 28, 2016. https://www.sans.org/.../***international-cybercrime-treaty-rat***

Rogin, Josh. "NSA Chief: Cybercrime Constitutes the greatest transfer of wealth in history." *Foreign Policy*. July 9, 2012. Accessed February 21, 2016.

http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/

Rudolph, Josh. "China Dismisses U.S. Cyber-Spying Charges - China Digital Times (CDT)." China Digital Times (CDT). May 19, 2014. Accessed May 01, 2016. http://chinadigitaltimes.net/2014/05/chinese-govt-netizens-angry-u-s-cyber-spying-charges/.

Rudolph, Josh. "China Reveals Its Cyberwar Secrets." *China Digital Times (CDT)*. March 19, 2015. Accessed March 28, 2016. http://chinadigitaltimes.net/2015/03/china-reveals-its-cyberwar-secrets/

Rudolph, Josh. "Documents Show How Weibo Filters Sensitive News - China Digital Times (CDT)." China Digital Times (CDT). March 03, 2016. Accessed May 01, 2016. http://chinadigitaltimes.net/2016/03/documents-show-how-weibo-filters-sensitive-news/.

Seabrook, John. "Network Insecurity." *The New Yorker*. 20 May 20, 2013. Accessed March 28, 2016. http://www.newyorker.com/magazine/2013/05/20/network-insecurity

Sinkkonen, Elina. "Nationalism, Patriotism and Foreign Policy Attitudes among Chinese University Students." *The China Quarterly* 216 (2013): 1045-063. Web. http://journals.cambridge.org/action/displayAbstract?fromPage=online&aid=9113316&fileId=S0305741013001094

“Speech at opening of the first Presidential Cadet Academy,” September 1, 2010, http://eng.kremlin.ru/transctipts/865.

Stanek, Becca. "How Did Anonymous Start? The History Of The Mysterious "Hacktivist" Group Began Quite Some Time Ago." *Bustle*. February 20, 2015. Accessed March 30, 2016. http://www.bustle.com/articles/65444-how-did-anonymous-start-the-history-of-the-mysterious-hacktivist-group-began-quite-some-time-ago

Sterbenz, Christina. "China Banned The Term '50 Cents' To Stop Discussion Of An Orwellian Propaganda Program." *Business Insider*. October 17, 2014. Accessed April 24, 2016. http://www.businessinsider.com/chinas-50-cent-party-2014-10

Stewert, Joe. "Operation Aurora: Clues in the Code." *Dell SecureWorks*. January 19, 2010. Accessed Setpember 30, 2015. https://www.secureworks.com/blog/research-20913

Summers, Timothy C. "Here's What Chinese Hackers Really Want." *MarketWatch*. October 1, 2015. Accessed February 14, 2016. http://www.marketwatch.com/story/heres-what-chinese-hackers-really-want-2015-10-01

"Taiwan: Hacker Working for PRC Firm Arrested," *Taipei Times*. June 26, 2002. Accessed December 21, 2015.

"The Ever-Changing Red Hacker Sharp Winner," Interview of Sharp Winner by *China Educational Television Satellite Channel (CETV-SD)*, September 13, 2005. Accessed January 14, 2016 http://forum.gd.sina.com.cn/cgibin/viewone.cgi?gid=51&fid=1359&itemid=8191

"The Great Chinese BBS Crackdown." *EastSouthWestNorth*. Accessed January 14, 2016. http://www.zonaeuropa.com/20050322_2.htm

"The Growth of the Chinese Computer Hacker," *KKER Union of China*. November 20, 2004. Accessed March 13, 2016. http://www.kker.cn/book/list.asp?id=1264

Thornburgh, Nathan. "Inside the Chinese Hack Attack." *Time*. August 25, 2005. Accessed September 30, 2016. http://content.time.com/time/nation/article/0,8599,1098371,00.html

Tweed, David. "U.S.-China Hacking Deal Seen on Civilian, Not Company Hits." *Bloomberg.com*. September 22, 2015. Accessed December 17, 2015.

Uzunovic, Agan. "Chinese Hackers." E-mail interview by author. April 5, 2016.

United Nation General Assemby. *Combating the Criminal Misuse of Information Technologies: Resolution*. New York: UN, 2001. Print.

US-China Economic and Security Review Commission, "China's Proliferation Practices, and the Development of its Cyber and Space Warfare Capabilities," May 2008 Accessed February 21, 2016. http://www.uscc.gov/hearings/2008hearings/transcripts/08_05_20_trans/08_05_20_trans.pdf

Vardi, Nathan. "Chinese Takeout," *Forbes*. July 25, 2005. Accessed October 13, 2015. http://www.forbes.com/forbes/2005/0725/054.html

Venable, David. "Chinese Hackers." E-mail interview by author. April 13, 2016.

Ventre, Daniel. *Chinese Cybersecurity and Defense*. London: ISTE, 2014. Print.

Vijayan, Jaikumarcc. "Chinese Hackers Master the Art of Lying in Wait." *Computerworld*. May 8, 2013. Accessed March 28, 2016. http://www.computerworld.com/article/2497171/cyberwarfare/chinese-hackers-master-the-art-of-lying-in-wait.html

Wade, Samuel. "Chinese Cyberchiefs Preach Internet Sovereignty in Moscow - China Digital Times (CDT)." China Digital Times (CDT). April 27, 2016. Accessed May 01, 2016. http://chinadigitaltimes.net/2016/04/chinese-cyberchiefs-preach-internet-sovereignty-moscow/.

Wade, Samuel. "Xi Pledges Cooperation vs. Hacking as Sanctions Loom - China Digital Times (CDT)." China Digital Times (CDT). September 22, 2015. Accessed May 02, 2016. http://chinadigitaltimes.net/2015/09/hacking-sanctions-threat-hangs-over-xis-u-s-visit/.

Walton, Greg. *China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China*. Montréal: Rights & Democracy, 2001. Print.

Ward, Mark. "Cybercrime Treaty Condemned." *BBC News*. December 18, 2000. Accessed March 17, 2016. http://news.bbc.co.uk/2/hi/science/nature/1072580.stm

Waqas, Amir. "Chinese Hackers." E-mail interview by author. April 7, 2016.

Waqas, Amir. "Interview with the Chinese Hacker Who Hacked Microsoft India Store." *HackRead*. February 29, 2012. Accessed December 25, 2015. https://www.hackread.com/interview-with-the-chinese-hacker-who-hacked-microsoft-india-store/

Weiping, Huang, and Chen Jiaxi. “China’s Grassroots Democracy: Development and Assessment.” *International Journal of China Studies.* 2.2 (2011): 177-211. ics.um.edu.my/images/ics/IJCSV2N2/IJCSV2N2-huangchen.pdf

Wexler, Evan, and Elias Mallette. "How the NSA’s Secret Elite Hacking Unit Works." *PBS*. May 29, 2014. Accessed January 19, 2016. http://www.pbs.org/wgbh/frontline/article/how-the-nsas-secret-elite-hacking-unit-works/

Wharton, Michael. "Twittocracy, Interactivism, Hacktivism, and Cyber-Anarchy: Cause." *There Is Always a Theory: Politics, Anarchy, Religion, Atheism, and Science*. October 12, 2010. Accessed January 14, 2016. http://www.michaelwharton.co.uk/2010/10/twittocracy-interactivism-hacktivism-cyber-anarchy-cause/

"What Is Internet Relay Chat (IRC)?" *SearchExchange*. December 2005. Accessed March 18, 2016. http://searchexchange.techtarget.com/definition/Internet-Relay-Chat

Wong, Edward. "Cost of Environmental Damage in China Growing Rapidly Amid Industrialization." *The New York Times*. 2013. Accessed February 1, 2016. http://www.nytimes.com/2013/03/30/world/asia/cost-of-environmental-degradation-in-china-is-growing.html?_r=0

Wong, Edward. "Hackers Find China Is Land of Opportunity." *The New York Times*. May 22, 2013. Accessed February 1, 2016. http://www.nytimes.com/2013/05/23/world/asia/in-china-hacking-has-widespread-acceptance.html

"World Report 2015: China." *Human Rights Watch*. 2015. Accessed September 30, 2016. https://www.hrw.org/world-report/2015/country-chapters/china-and-tibet

Xu, Young. "Deconstructing the Great Firewall of China." *Tech in Asia*. ThousandEyes Inc. 8 March 8, 2016. February 7, 2016. https://blog.thousandeyes.com/deconstructing-great-firewall-china/

Yar, M. "Computer hacking: Just another case of juvenile delinquency?", *The Howard Journal of Criminal Justice.* 44, 4 (Sept. 2005), 387–399.

Yoon, Eunice. "Hacker Weighs in on US-China Cyber Spat." *CNBC*. September 23, 2015. Accessed September 30, 2015. http://www.cnbc.com/2015/09/23/hacker-weighs-in-on-us-china-cyber-spat.html

Zhen, Yan. "Morals lost in cyberspace," *Beijing Time*, December 12, 2005. Accessed January 14, 2016. www.shanghaidaily.com/art/2005/12/12/226181/Morals_lost_in_cyberspace.htm

"第二届 0CTF 信息安全技术挑战赛暨首届 XCTF 上海站选拔赛决赛圆满落幕 "SJTU Network & Information Center. May 11, 2015. Accessed May 3, 2016. http://net.sjtu.edu.cn/info/1003/1766.htm

"广东：高薪请黑客堵"漏洞" Jingan Times cia China.com.cn. May 24, 2002. Accessed May 3, 2016. http://www.china.com.cn/chinese/difang/150045.htm