ON THE ETHICS OF CYBER WARFARE AND INTERNATIONAL RELATIONS

by

Brenna Fitzpatrick
A Thesis
Submitted to the
Graduate Faculty
of
George Mason University
in Partial Fulfillment of
the Requirements for the Degree
of
Master of Science
Conflict Analysis and Resolution
Master of Arts
Conflict Resolution and Mediterranean Security

Committee:

_____ Chair of Committee

_____

_____

_____ Graduate Program Director

_____ Dean, School for Conflict Analysis and Resolution

Date: _____ Fall Semester 2016
George Mason University
Fairfax, VA
University of Malta
Valletta, Malta

On the Ethics of Cyber Warfare and International Relations

A Thesis submitted in partial fulfillment of the requirements for the degrees of Master of Science at George Mason University and Master of Arts at the University of Malta

by

Brenna Fitzpatrick
Bachelor of Science
Virginia Tech, 2015
Bachelor of Arts
Virginia Tech, 2015

Director: Richard Rubenstein, Professor
Department of Conflict Analysis and Resolution

Fall Semester 2016
George Mason University
Fairfax, VA
University of Malta
Valletta, Malta

DEDICATION

This is dedicated to my supportive father and mother, Drew and Theresa.

ACKNOWLEDGEMENTS

I would like to thank the many friends, relatives, and supporters who have made this happen. My best friend, Beth, who pushed me to keep at it, even when things seemed bleak. My cohort for being a great source of inspiration and strength. Dr. Schoeny, my wonderful and patient advisor, and the other members of my committee were of invaluable help. Mary Oberlies, librarian for conflict and peace studies, for being a superb resource to lean on. Finally, thanks go out to my hosts in Ireland for providing a clean, quiet place in which to work.

TABLE OF CONTENTS

List of Abbreviations

Basic Input / Output System ..... BIOS
Denial of Service..... DoS
Domain Name System .....DNS
Information and communication technologies.....ICTs
Virtual private network.....VPN

ABSTRACT

ON THE ETHICS OF CYBER WARFARE AND INTERNATIONAL RELATIONS

Brenna L. Fitzpatrick, M.A.

George Mason University, 2016

Thesis Director: Dr. Richard Rubenstein

This thesis interrogates the development of cyber warfare and how state governments engage cyber warfare. Cyber warfare is a highly modernized form of conflict between state actors, calling for those studying conflict to understand it as much as possible. While researching and writing this thesis, the author conducted a literature search and reviews of news articles, government documents, government press releases, and statements by government officials.

CHAPTER 1: INTRODUCTION

In this chapter, I will introduce my topic of inquiry (the ethics of cyber warfare). To begin, I will detail and define what cyber warfare is, detailing some of the many forms that cyber warfare may take. I will also trace the beginnings of cyberspace, the domain of cyber warfare, in order to better explore this emerging arena of warfare. I will also critique how most scholars approach this field of inquiry and explain why this approach is inadequate to fully explain and support arguments for cyber warfare. Finally, I will describe my case studies (one being the United States and the other being China) to provide background details necessary to fully understand data presented later.

I chose to investigate the ethics of cyber warfare and international relations for several reasons. Firstly, in the current state of the world, individuals have little true power. The sites of power seem to be large institutions that function within this global system, pulling and prodding individuals into place as it suits the larger structure. Bearing this in mind, it seems far more useful to investigate how these institutions are engaging with the world. For this study, I will focus on the institution of state government. Secondly I suspect that the kinds of arguments and narratives that state governments deploy carry positive messages—such as improving human rights conditions or lessening the burdens of warfare—but the actions and workings of cyber warfare act instead to prop up the status quo or even to engage in more malicious activity than would be otherwise permissible.

That is to say that I suspect that state governments are hailing cyber warfare as a great advance for humanity, but it is rather just a new and more devious tool in the toolbox for states to engage in aggressive action. Thirdly cyber warfare remains largely understudied, particularly in conflict resolution. My aim in this project is to shine a new light on cyber warfare that goes beyond a clinical cost-benefit analysis of cyber warfare and to add more space for discussion in this emerging field of inquiry.

There have been instances that follow this thinking, such as the case of chemical and biological weapons. After the end of World War I, approximately 125,000 tons of poison gas had been deployed by all parties involved (Everts, 2015a). It has been argued by the majority of World War I historians that "chemical weapons had no decisive effect on the outcome of the war," an ineffective weapon and a waste of resources. However there were people of prominence that saw benefits to using chemical weapons. Winston Churchill argued that "gases could be used to inconvenience the enemy and spread terror, not necessarily to kill" (Everts, 2015a). There was an attempt to create international legislation to regulate noxious gases and submarines following the war at the Conference on Limitation of Armament, however the agreement never entered into force due to objections from an influential state, France (Gilbert, 2014). Instead the Geneva Protocol was adopted in 1925 by the League of Nations which prevented the use of chemical and biological agents in war (Everts, 2015b). However, the development, production, and stockpiling of chemical and biological weapons was not prohibited. Of the countries that were signatory to the treaty, many had reservations allowing them to respond in kind if attacked with chemical and biological weapons. Chemical and biological weapons were

used in World War II, the Vietnam War, and the Iran-Iraq War, all following the Geneva Protocol. The Biological and Toxin Weapons Convention was completed in 1972, intended to couple with the Geneva Protocol and ban the development, production, and possession of these kinds of weapons. However, there was no compliance mechanism in place to ensure signatories and adoptees would fulfill their obligations (Everts, 2015b). The United States signed this convention in April of 1972, ratifying it in March 1975 (Davenport, 2016). During the Cold War, both the United States and the Soviet Union rushed to develop and stockpile large amounts of chemical and biological weapons (Gilbert, 2014). It was only after the fall of the Soviet Union in 1991, that the Chemical Weapons Convention was signed in 1993. This convention forced all signatories to stop the production, stockpiling, and use of chemical weapons (Gilbert, 2014). This agreement was arguably only possible because there was only one "superpower" left in the world: the United States.

The world is becoming increasingly dependent and integrated into information and communication technologies. The infrastructure that supports modern life is becoming necessarily tied to these technologies, making their involvement in the sphere of war particularly troubling. In the past, it was relatively easy to tease out what "wartime" meant. There had to be specific actions—such as an act of aggression or a speech act declaring war—for a state to be engaged in warfare. The lines defining wartime have been increasingly blurred during the twentieth century, however cyber warfare has the potential to make the lines between war and peace seemingly nonexistent. The development and

evolution of cyber warfare must be closely followed in order to create acceptable guidelines and criteria for this new arena of war.

I chose the United States as a case study for several reasons. The United States is an ever-present global force and is a military superpower. It is hard to underestimate its power and reach in military affairs, making it a key case study to understand the development and history of cyber warfare. In addition, there is more scholarship on cyber warfare in the United States available for me to study. This increased scholarship provides me with more sources and data to source from, allowing me a richer understanding of the issue.

In kind, I chose China as the other case study for several reasons. China is a rising power in the world, often thought of as the rising rival of the United States. This has several benefits and ramifications. Firstly, there is more scholarship and data available on China than other states due to its rising prominence. Secondly, there have been tensions between the United States and China. They are often portrayed and discussed as completely different powers. By comparing these two cases, I hope to gain insights on the real similarities and differences between these powers in regard to cyber warfare. Lastly, the Chinese perspective has power, especially with those who are against the United States. If there were a power that would provide an alternate method of cyber warfare, China would be a top contender.

CHAPTER 2: LITERATURE REVIEW

Before discussing cyber warfare in particular, it is important to understand why there has been a shift towards cyber warfare in recent decades. Much of this stems from a shift in conflict that has been happening over the past century. To trace these roots, I will provide an overview of literature on the concept of nonlethality, the emergence of cyberspace and the information age, the meaning of cyber warfare, and international agreements that pertain to cyberwarfare. This overview will serve as a foundation for my study of how cyber warfare is coming into its own.

Cyber Warfare: a new kind of arms race

Since the early days of the 20th century, the international community has put in serious effort to curtail violence during wartime. Some of the notable, early attempts at regulating hostilities include the Hague Conferences and the Washington Naval Conference (Bowers & Mielnik, 1998). Military strategies changed drastically with the rise of nuclear weaponry, becoming centered on avoiding nuclear war rather than engagement. This period of transition has been characterized both by frequent wars using conventional (non-nuclear) weaponry and the emergence of critics of the new nuclear age. These critics were inspired by technological innovations, medical advances, and constant media surveillance (Bowers & Mielnik, 1998). Eventually the fear of nuclear winter gave way to a new concern of developing nonlethal weapons for offensive and defensive

capabilities, rather than developing and increasing a stockpile of lethal weapons (Bowers & Mielnik, 1998).

Emergence of nonlethal weaponry

The term *weapon* "generally refers to something designed to cause bodily harm and / or destruction of inanimate objects" (Bowers & Mielnik, 1998). This would imply that a *nonlethal weapon* will have absolutely no—zero—fatalities with its use by definition. However the term "nonlethal weapon" is often highly criticized as both a euphemism and an oxymoron for this reason, as zero fatalities is an unrealistic goal and often inaccurate representation of their effects (Lewer, 1999; Bowers & Mielnik, 1998). Therefore, nonlethal weapons are often referred to as *less than lethal*, *sublethal*, *pre-lethal*, or *disabling* weaponry in the literature in order to more accurately capture their reality (Bowers & Mielnik, 1998; Coppernoll, 1999). These descriptions sound reassuring and remain interchangeable in modern discourse (Guyatt, 1997; Lewer, 1999).

The lasting preference for these reassuring terms has much to do with public distaste for the casualties that come with warfare. "Blood, guts, and especially death are no longer politically acceptable" in the modern political climate (Guyatt, 1997). Over the past century, public opinion has found it more and more unacceptable for there to be any deaths or serious casualties from military action. This shift is largely attributed to the rise of instant media coverage (Lewer, 1999). In the current political climate, military operations both outside of open warfare and during urban warfare must have the capacity to nonlethally overwhelm their opponent—regardless if that opponent uses lethal force (Morris, Morris, & Baines, 1995). Proponents of the term *nonlethal weaponry*

acknowledge that the term is ambiguous (Lewer, 1999). However, proponents also argue that it accurately represents the intention behind such weapons, seeking not to kill or permanently harm their opponents, and their development signifying a willingness from advanced nations to act civilly and with restraint (Lewer, 1999; Coppernoll, 1999).

Yet suppose we do accept the term *nonlethal weaponry*. This would imply that conventional weapons are necessarily lethal by definition. However most conventional weapons are not *lethal* in this definitional sense. For example, rifles only inflict a 20 – 25% casualty rate (Bowers & Mielnik, 1998). Antipersonnel mines often maim—and do not kill—their victims (Bowers & Mielnik, 1998). The concern for creating nonlethal weaponry raises a new ethical question: is it more humane to disable or to kill an opponent?

Contrary to current trends in military development, the creation of lethal weaponry was heavily stressed during the Cold War (Bowers & Mielnik, 1998). During this period, national security was measured by a state's capacity for overkill, creating a credible threat of a totalizing second strike against any opponent. For this reason, technology was designed to be increasingly destructive in nature (Bowers & Mielnik, 1998). Since the Cold War, there has been a declining likelihood for largescale interstate wars. This has shifted the focus of technological innovation away from destruction towards creating a stockpile of nonlethal weapons to use in military operations outside of war (Bowers & Mielnik, 1998; Lewer, 1999). During this time, a variety of nonlethal weapons have been developed. Some of the low cost weapons developed include technologies such as pepper sprays and other gaseous weapons, plastic bullets, and water cannons. Some of the high cost weapons developed include technologies such as "blinding" lasers and acoustic, radio-

frequency, and directed energy weapons (Guyatt, 1997). The effects of these new categories of nonlethal weaponry on warfare are often debated within many international bodies (Bowers & Mielnik, 1998).

There are several advantages of using nonlethal weapons. Namely nonlethal weapons are not limited to times of war like conventional weapons, meaning that they have a multitude of uses (Bowers & Mielnik, 1998). Whereas conventional weapons are often limited to use by the military, civilian law enforcement can also use nonlethal weapons to handle civil issues. Some nonlethal weapons can be used for crowd and riot control, hostage situations, and apprehension of violent criminals without the intended risk of permanent harm (Bowers & Mielnik, 1998). Because nonlethal weapons are not intended to kill their targets, nonlethal weapons are perceived to be a more humane method of conflict intervention. Nonlethal weapons reduce the risk of excessive military force during operations, can serve as a credible deterrent that is not as extreme as massive military deployments, promote political support for peacekeeping and diplomatic missions internationally, and significantly reduce the damage to infrastructure and the environment from interventions (Bowers & Mielnik, 1998; Lewer, 1999; Morris *et al.*, 1995).

Nonlethal weapons have already been successfully used by United States military forces in several conflicts, such as: the Gulf War, Somalia, and the former Yugoslavia (Bowers & Mielnik, 1998). The use of nonlethal weapons in military operations deliver results that conserve lives, reduce costs, and reduce environmental impacts in comparison to conventional weaponry (Bowers & Mielnik, 1998; Morris *et al.*, 1995). These weapons are meant to "project high-precision power in a timely fashion," which is to say they are

meant to bring the might of a state to bear swiftly, without damaging unintended targets (Morris *et al.*, 1995). Several rapid advancements have been crucial to the development of these credible, nonlethal alternatives to conventional weaponry, including the areas of precision targeting, unmanned weapons-delivery systems (e.g. drones), sophisticated command-and-control systems, intelligence gathering and analysis, shrinking scale of electrical components, and power-portability (Bowers & Mielnik, 1998; Lewer, 1999). When viewed collectively, these characteristics make nonlethal weaponry particularly attractive during low-intensity conflicts. Namely, nonlethal weapons reduce the risk of any legal, ethical, or political challenge either domestically or internationally (Coppernoll, 1999).

Additionally, warfare has never been considered a cheap endeavor. Even by comparison, modern warfare generally requires a large amount of resources. One of the most important and expensive of these resources is data (Bowers & Mielnik, 1998). For the past two decades, information and communication technologies have become a useful and valuable asset in military operations, having been deployed in most of the conflicts since the second Iraqi war (Taddeo, 2012a; Krotofil, 2014). Modern military operations require data about: the allied resources, the enemy resources, the terrain of the engagement area, and the intentions of the adversary (Bowers & Mielnik, 1998). Military operations of any size or importance—large or small—need secure spaces to store essential necessary for the planning and engagement of modern warfare. The move towards computer-based information networks has made these secure storage spaces far more vulnerable. Previously, saboteurs had to illicitly enter well-guarded facilities to access this essential

sensitive information. As information increased in sensitivity and importance, the protection of the facility would increase in kind. These protective measures meant that saboteurs were likely to be detected, captured, and thwarted (Bowers & Mielnik, 1998). Now with the assistance of the Internet, saboteurs do not have to risk physical harm and can collect data from distant and relatively safe bases. As long as modern saboteurs are careful when discussing their illicit activities, it is highly unlikely that authorities will apprehend them (Bowers & Mielnik, 1998).

Formation of cyberspace

The rising demand for nonlethal weaponry grew alongside and was met by technological innovations, such as cyberspace (Bowers & Mielnik, 1998). The rise of cyberspace offered the military the ultimate nonlethal weapon. In the beginning, it was inconceivable to intentionally kill another human being via electronic means. While it the increased possibilities for intelligence gathering and data mining, hacking into an individual's pacemaker was not even a remote possibility at the time. This made any advancements in cyberweapons an attractive, nonlethal alternative to conventional weapon development.

Cyberspace is often discussed like it is commonly understood in modern discourse, but the reality is that cyberspace is the result of complex, multilayered connections between information and communication technologies (ICTs) made through the Internet (Mezher, Khatib, & Sooriyaarachchi, 2015). This sophisticated network does not lend itself well to a simplistic understanding of how this intangible space relates to reality. One possible definition of cyberspace is "the diverse experiences of space associated with computing

and related technologies" (Strate, 1999). Alternatively, cyberspace could be understood as the network that "encompasses email, the Internet, file transferring" and other programs connecting computers together (Patterson, 2015). Over the past two decades, it has become clear that cyberspace and the Internet has become profoundly useful across all domains of life—individual, social, political, military, and business—necessitating the development and spread of information and communication technologies (Huhtinen, 2015; Taddeo, 2012a; Mitra & Schwartz, 2001). Today people all over the world have access to the Internet. Most of these people can and do use the Internet without any particular training or skill, changing how people relate and interact with one another (Huhtinen, 2015; Mitra & Schwartz, 2001). The impact of these technological innovations have fundamentally changed modern life.

Societal disruption by new technologies is not limited to the social sphere of life. Operations that are essential to a state's ability to function as a modern, secure state can be disrupted by new technological innovations (Bowers & Mielnik, 1998). As these new technologies have dispersed throughout society and enhanced our collective working effectiveness, a new class of threat has emerged onto the scene: cyberthreats (Bowers & Mielnik, 1998; Brenner, 2007). Very broadly, a *cyberthreat* can be understood as "using computer technology to engage in activity that undermines a society's ability to maintain internal or external order" (Brenner, 2007). Many modern, complex systems—such as state critical infrastructure—are connected through cyberspace and can be assaulted by anonymous computer attackers (hackers). These hackers can reach remote and vulnerable facilities without any real personal risk (Mezher *et al.*, 2015; Bowers & Mielnik, 1998).

There are many critical infrastructure sectors that could be disrupted via information and communication technological attacks, such as but not limited to: commercial facilities, critical manufacturing, defense industrial bases, emergency services, energy facilities, financial services, government facilities, transport systems, etc. (Hurley, McGibbon, & Everetts, 2014). However, all of these technological advancements also have significant benefits. There has been increased life expectancy, increased comfort levels, unmatched levels of material productivity, increased and more immediate access to information, and enhanced and sophisticated degree of national security (Bowers & Mielnik, 1998).

Nevertheless, cyberspace has become the fifth domain of war; the military uses the space for operations, alongside land, sea, air, and space (Taddeo, 2012a). Cyberspace is a stateless space in the same way the high seas are stateless. Where many domains of war are localized, both space and cyberspace are the most globalized domains of war (Delpech, 2012). Cyberspace has fundamentally changed how militaries act and how wars are waged (Taddeo, 2012a). The concerns of the military have changed with the technological modernization of military operations. For example, the maintenance of effective systems of communication and control has become one of the most fundamental military concerns (Bowers & Mielnik, 1998).

A new kind of warfare

There are many different definitions that academics use to frame cyber warfare, however the term itself was first used in the Oxford English Dictionary in 1994, only gaining widespread media attention since 2009 (Dipert, 2010). Taddeo defined cyber warfare as:

> "[warfare grounded on certain] uses of ICTs within an offensive or defensive military strategy endorsed by a state and aiming at the immediate disruption or control of the enemy's resources, and which is waged within the informational environment, with agents and targets ranging both on the physical and non-physical domains and whose level of violence may vary upon circumstances" (Taddeo, 2012a).

This framework understands cyber warfare as not necessarily violent and destructive, but still maintaining a possibility for severe damage without any physical force or violence (Taddeo, 2012a). Brenner offered a simpler definition that has a similar sentiment behind it, cyber warfare "is the conduct of military operations by virtual means" (Brenner, 2007). These definitions mark cyber warfare as distinct from other forms of cyber-attacks, such as cybercrimes and cyberterrorism. A *cybercrime* is "the use of computer technology to commit crime; to engage in activity that threatens a society's ability to maintain internal order" (Brenner, 2007). Alternatively, an act of *cyberterrorism* requires using computer technology in terrorist activity. In other words, it is the use of computers "to demoralize a civilian population and thereby undermine a society's ability to sustain internal order" (Brenner, 2007).

These frameworks do not necessarily involve human beings, but Taddeo argued that cyber warfare should be just as feared as traditional warfare. For Taddeo, traditional warfare was a necessarily violent phenomenon, which implies the sacrifice of human lives and damage of both military and civilian structures (Taddeo, 2012a). As technological systems become more advanced and opportunities for attacks in cyberspace increase, the ad hoc approaches for handling these attacks become less satisfactory (Brenner, 2007). Additionally, states conceive of cybersecurity in terms that encompass all of cyberspace,

ranging from cyber warfare and cyber terrorism to intellectual property protection and child online safety (Stevens, 2013). This totalizing perspective makes cyberspace and cyber security exceedingly complex for both policy makers and scholars alike to approach these issues.

There are several features unique to cyber warfare. Cyber warfare is the first new form of warfare since the dawn of nuclear weapons and intercontinental missiles (Dipert, 2010). In this new arena, there is a problem of attribution, meaning it is exceedingly difficult to determine the source of a cyber-attacks (Dipert, 2010; Patterson, 2015). Borders no longer have the same kind of stopping effect they have in traditional warfare (Krotofil, 2014). Additionally, proxies serve as a considerable problem to correctly attributing an attack to an aggressor in cyberspace, making it even harder to response appropriately (Delpech, 2012). This gives those that engage in cyber warfare credible deniability and makes warfare ambiguous in a way that it was not before the advent of cyber warfare (Dipert, 2010; Brenner, 2007).

Firstly, it is very easy for a state to claim that while a cyber-attack may have originated from within their borders or territory, their governments did not initiate the cyber-attack itself (Dipert, 2010). The origin of an illicit cyber-attack could be traced to a non-state actor, requiring a victim state to prove another state had sufficient control over the non-state actor in order to hold that state accountable (Patterson, 2015). Secondly, it used to be that only states had the resources and capability to wage war (Brenner, 2007; Patterson, 2015). Unlike nuclear and other advanced technological weaponry, cyber warfare does not require any exotic or hard-to-acquire materials (Dipert, 2010). With the

rise and spread of technological innovations, anyone with sufficient knowledge of ICTs and a computer could wage cyber warfare (Brenner, 2007; Dipert, 2010). Cumulatively, these new systems create spaces where attackers can remain anonymous and unidentifiable (Bowers & Mielnik, 1998; Brenner, 2007). This would make any treaty to ban cyberweapons virtually impossible (Libicki, 2009). Thirdly, cyber warfare often will not be lethal, not even causing permanent damage to physical objects in the world (Dipert, 2010). This makes cyber warfare extremely attractive in the post-nuclear age, piggybacking on the attraction to nonlethal weaponry. Lastly, the nature of cyber-attacks is often never identified, making the intent behind the attack uncertain (Brenner, 2007). Without the knowledge of intent, it becomes increasingly difficult to determine what kind of attack a victim has experienced.

Yet cyber warfare does share some features with traditional warfare. In both cases, defense against either form of warfare is expensive and likely to fail (Dipert, 2010). Unlike traditional warfare, offensive cyber-operations are comparatively cheap. For this reason, cyber warfare is an attractive option for small and developing countries and large countries alike (Dipert, 2010; Krotofil, 2014). It is worth mentioning that the cost of large-scale, sustained cyber-attacks should not be underestimated. They require lengthy preparatory work and a team with advanced technological skills that are hard to come by (Krotofil, 2014). In both forms of warfare, commanders make guesses and projected outcomes of attacks. These predictions only hold so much truth, as they have a low degree of certainty. It is really unclear in both cases what the result from a given attack; very distant or

damaging side effects of an offensive operation are nearly impossible to adequately anticipate (Dipert, 2010).

Just like traditional warfare, cyberwarfare has a variety of cyber weaponry and cyber-attacks. Cyberweapons themselves belong to a very broad category of various kinds of attacks on information systems, including: traditional counterespionage and disinformation campaigns; destruction of telephone lines; jamming of radio signals; killing of carrier pigeons; etc. (Dipert, 2010). However in cyber warfare, this is limited to attacks on modern digital information systems (i.e. computers and computer systems), which includes acts such as intentional damage to the software, the hardware, and the operations of modern ICTs. While most authors use *cyber-attack* to refer to attacks on digital information systems via the Internet or other networks, there are other possible forms for cyber-attacks to take (Dipert, 2010). A cyber-attack may come from a means other than the Internet, such as a flash drives and CDs, or could be secretly incorporated in the BIOS (Basic Input / Output System) of the computers themselves before sale. The latter is particularly insidious. A BIOS is part of most computers, a form of relatively simple firmware that survives powering down required for a computer to know to load an operating system upon startup (Dipert, 2010).

In regard to the more typical use of cyber-attack, there are several forms of attack via the Internet. There are nonintrusive cyber-attacks, such as a *Denial of Service* (DoS) attack (Dipert, 2010). Unlike other cyber-attacks, the attacker never actually gains access to the site or information itself in a DoS attack. Instead the targeted site, server, or sections of network are overwhelmed by hundreds or thousands of unnecessary requests for

information or security. These systems cannot handle the sheer amount of requests, making the whole system inaccessible for its intended use (Dipert, 2010). This form of attack can prevent a system's intended users from accessing their email, websites, online accounts, or other services that rely upon that system (McDowell, 2013). No damage is really done to the system, as the attacker never gains access to the internal workings of the software or hardware of the system (Dipert, 2010).

Another form of nonintrusive cyber-attack is a *Distributed Denial of Service* (DDoS) attack (Dipert, 2010). Similar to the intent of a DoS attack, a programmer deploys a DDoS attack to render a target system useless, with one key difference. A DDoS requires a programmer to create a malicious piece of software (malware) that can embed itself in hundreds or thousands of computers around the world. These infected computers become networks of remotely controllable slave computers (botnets) that can—at either a pre-set time or on command—bombard a targets site with emails or requests for responses (Dipert, 2010). A DDoS is "distributed" because of the attacker uses multiple computers in order to carry out the attack (McDowell, 2013). This form of attack seriously interferes with the normal operation of the Domain Name System (DNS) of a site, a crucial element of the Internet infrastructure (Mezher *et al.*, 2015). The DNS is the mechanism responsible for recognizing Internet addresses (Janczewski & Colarik, 2008). Unlike a simple or direct DoS attack where an IP address can be blocked to stop the attack, DDoS attacks cannot be blocked because there are too many IP addresses attacking the system (Dipert, 2010). This could be resolved by requiring a confirming dialogue (a kind of a handshake between the system and a user) between the source and the target. However, the confirming dialogue

itself could overwhelm the system capabilities, rendering the system useless regardless and defeating the purpose of the patch. This form of attack can also be identified and blocked by monitoring Internet traffic carefully, separating malicious traffic out from legitimate Internet traffic. There are common identifying features ("fingerprints" or "DNA") in malicious messages, allowing them to be traced online to find the actual source of the attack. However, this kind of defense can be very expensive in terms of human and computer resources required (Dipert, 2010).

Another form of cyber-attack are intrusive cyber-attacks, which result mostly from some form of malware. In an intrusive cyber-attack, a piece of malware gains access to parts of a computer's software or stored data through the Internet (Dipert, 2010). Once inside of a system, malware can alter pieces of software or data, crash the system, stop certain software from functioning, erase hard drives, send emails posing as the user, send information about the user back to the creator of the malware, etc. Intrusive cyber-attacks attempt to mine data illicitly from a computer or system. A *self-replicating* piece of malware can infect more computers, even in modified form, once it is sent by its creator. A *virus* is a piece of malware that spreads between computers and systems by attaching itself to another file, program, or email (Dipert, 2010). Viruses execute their code when a particular file is used (Janczewski & Colarik, 2008). Viruses are various in nature. Some do no harm (pranks), but the virus is still not wanted on the system. Some viruses can alter their own code, making the virus harder to track and to identify by anti-virus programs. Some viruses can even "blind" anti-virus software to their existence or prevent anti-virus software from updating. A *worm* is a piece of malware that is a standalone program that

can travel through information pathways (Dipert, 2010). Unlike a virus, a worm does not require another file or program to replicate itself. Worms are self-sustaining in a way that other forms of cyber-attacks are not (Janczewski & Colarik, 2008). A *Trojan (horse)* is a piece of malware that is not self-replicating and is either not easy to detect at first or does no detectable damage. A Trojan can even be perceived as a useful program by the user (Dipert, 2010). Many viruses and worms are transmitted via Trojans (Janczewski & Colarik, 2008). All of these forms of attack can utilize a zero-day vulnerability, defined as a previously unknown critical security weakness in a program or a system that do not allow for any response time to a threat (Economist, 2010; Kushner, 2013; Janczewski & Colarik, 2008).

In cyber warfare generally, malware is often strictly an espionage effort, not directly damaging a targeted state's information (Dipert, 2010). In these cases, a state's interests are threatened only through gathered intelligence. In this manner, malware strictly for espionage purposes are not truly "cyberweapons," intending to do harm. However, the use of real cyberweapons is peculiar. Once intrusive malware has been found in a system, countermeasures and patches can be deployed by sufficiently advanced users or states in minutes, hours, or days. With this in mind, the offensive use of cyberweapons is often a "one-time use," with their effectiveness rapidly diminishing thereafter (Dipert, 2010). In other words, once a cyberweapon has been deployed, it is released forever allowing for analysts to defend against that kind of cyber-attack from then on. This means that attackers are often reluctant to deploy their best cyberweapons until it is worth losing those system weaknesses.

Cyber-attacks come in many different forms, more than are even described in this chapter. The importance of this varied nature cannot be overstated. In conventional warfare, operations generally have a numerous, but still limited to a set of criteria that must be taken into account for a given operation. An entity engaging in conventional warfare must take into account its available resources, the capability of those resources, and manage the advantages and disadvantages of a given action. If the entity measures these criteria and are not satisfied with any particular criteria, that entity now knows where to focus its energies in order to either attack or defend. In cyber warfare, an attack can come from a crack in any line of code on a system or from any mismanaged system. Currently, the potential weaknesses of a system are nearly infinite and can come from any direction. This nigh infinite number of possibilities makes cyber warfare uniquely problematic to not only define, but also legislate and manage.

At the beginning of the Internet age in the 1990s, malware was not particularly pernicious (Kushner, 2013). Most pieces of malware were the creation of pranksters or hackers looking to cause some sort of mischief, such as crashing the system or inserting graffiti on an Internet page. During this period, most malware was found by searching code by hand, requiring antivirus hackers to have an intimate working knowledge of coding language. However, this changed significantly over the following decade. The manual detection of viruses was unsustainable as modern ICTs became more commonplace, requiring detection methods to become automated. These automated systems can find as many as 250,000 new malware files every day. During the first decade of the 2000s, state-

against-state cyberwars seemed like a far off possibility, a topic of science fiction (Kushner, 2013).

International legal agreements

There are several international legal instruments that apply to nonlethal weapons broadly, mostly pertaining to the concept of "proportionality" in the legal framework of armed conflict. This concept means that when "any military action or weapon inevitably causes suffering, that suffering must be balanced against military necessity" (Coppernoll, 1999). Most of these legal instruments are a subset of the larger legal concept of "humanity," which requires that both combatants and noncombatants are not subject to needless or unnecessary suffering. Much of the legal framework pertaining to nonlethal warfare was outlined in the Lieber Code of 1863 and the Declaration of St. Petersburg of 1868. The Lieber Code, created during the American Civil War in order to regulate the northern Union forces, became the foundational document for later international humanitarian law (Coppernoll, 1999). The Lieber Code established that long-term effects of a particular weapon must be accounted for before its use, meaning that armed forces should not embrace cruel methods and means in order to achieve victory. Only a few years later the Declaration of St. Petersburg was signed, resulting from a general aversion to inhumane weaponry. Specifically, the declaration prohibited any weapon that "uselessly [aggravates] the sufferings of disabled men, or [renders] their death inevitable" (Coppernoll, 1999). Both of these documents, joined by several Hague conventions and declarations [Hague Declarations Asphyxiating Gases and Concerning Expanding Bullets (1899); Hague Convention Respecting the Laws and Customs of War on Land (1907);

Geneva Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous, or Other Gases, and of Bacteriological Methods of Warfare (1925); Chemical Weapons Convention (CWC) (1993); Biological Weapons Convention (1972); Certain Conventional Weapons (CCW) Convention [the Convention of Prohibitions or Restrictions on the Use of CCWs Which May Be Deemed to Be Excessively Injurious Or to Have Indiscriminate Effects] (1980); Nairobi International Telecommunications Convention (1986); and Environmental Modification Convention [the Convention on the Prohibition of Military or any Other Hostile Use of Environmental Modification Techniques] (1977)], create the international standards associated with nonlethal weaponry (Coppernoll, 1999). While cyber warfare is a subset of nonlethal warfare, it is not clear how much—if any—of this legal framework can be applied. This largely has to do with the ambiguity surrounding what constitutes "armed conflict" in relation to cyber warfare.

Just War Doctrine: an old ethic

In political realist thought, politics operate under objective laws that have their roots in a particular form of human nature, where human beings are self-interested (Morgenthau, 1967). By extension, states are self-interested as they are fundamentally comprised of human beings. Political realists understand the international field through the concept of state interest. Under this view, the immediate aim of international politics is always a struggle for power, while states ultimately aim for concepts of freedom, security, prosperity, or power itself. While international state action is always having to do with state power, political realism acknowledges that states are not always engaged in international politics. When states are involved in international politics, political realism

also acknowledges that states are engaged in varying degrees (Morgenthau, 1967). This means that every single state action is not necessarily tied to international power and every state is not as invested in the international system to the same degree. In this framework, state action ought to be understood through a rational lens, where states make calculated decisions that they expect to enhance their power. Left unchecked, political realism could be used to justify horrible atrocities. Individual states could potentially defend war crimes if they claimed that it furthered their ultimate aim for freedom or for security. For the individual state, this seems justifiable if there are no norms that prohibit this kind of action.

However, the principles of Just War seem to provide a means of oversight and control over state interest in international politics. Several international organizations (such as the United Nations) have embraced Just War theory as the foundation for international norms of state action, providing a legitimizing set of guidelines for states to carry out war action (Patterson, 2005). The Just War doctrine is used as the central point of reference to justify both the use of force and how much force may be deployed during conflict (Coppernoll, 1999). There are four ethical tenets to Just War doctrine, providing a strong moral foundation for conducting war (Patterson, 2005). The first ethical tenet is the normative value of human life. That is to say in Just War doctrine, human life ought to be respected in all cases. This principle of respect sets the tone for the following principles (Patterson, 2005). The principle of *jus ad bellum*, the international law dictating when a state may engage in war and coming out of Just War doctrine tenets, outlines the essential criteria for a war to be considered legally sound. There are seven essential criteria for going to war: (1) just cause, (2) right authority, (3) right intention, (4) goal of restoring

peace, (5) proportionality, (6) reasonable hope of success, and (7) force as a last resort (Coppernoll, 1999).

The second ethical tenet calls for accountability for one's actions (Patterson, 2005). This principle applies to both individuals and collectives. This implies that actors in wartime must claim the actions they commit and be held responsible for any unjust action. The third ethical tenet, related to the concept of accountability, places significance on the motivation of wartime actors (Patterson, 2005). From these concepts, Just War doctrine also outlines acceptable practices within armed conflict once war is underway, in international regulations cumulatively called *jus in bello* (Coppernoll, 1999). The mechanisms applicable during wartime include just cause, right intent, and last resort (Patterson, 2005). These practices ethically limit military decisions made during conflict, with certain kinds of decisions justifiable and others not; thereby, a state must be able to explain wartime action through one of those mechanisms (Coppernoll, 1999; Patterson, 2005). The fourth ethical tenet assumes that the world has order, which is a moral concept. This understanding of order is based in the legitimate authority of both government and law. This order is seen as essential for both justice and security in Just War doctrine (Patterson, 2005).

Additionally, there are practical tenants to the Just War doctrine. Two important practical tenants include proportionality and discrimination, both serving as the foundation for just conduct of war (Patterson, 2005; Coppernoll, 1999). The principle of proportionality argues that wartime action ought to use only the minimum amount of force necessary to accomplish goals (Patterson, 2005). This means that states should not go

beyond the destruction necessary to accomplish their goals (Patterson, 2005). The principle of discrimination provides immunity to noncombatants, meaning that intentionally attacking civilians is not acceptable and comes with repercussions (Patterson, 2005). Any damage to a civilian target must be weighed against and proportionate to the military advantage gained through the military action (Coppernoll, 1999). Just War doctrine provides a structure that mitigates the kinds of actions states can do in their pursuit of power.

With the criteria set out in Just War doctrine, nonlethal weaponry is particularly attractive, especially in regional contingencies (Coppernoll, 1999). Many contemporary military options are unclear, meaning that the distinctions between operations other than war and "armed conflict" are becoming less clear (Coppernoll, 1999). Nonlethal weaponry seems to address many of the concerns of Just War doctrine by minimizing the effects that force has on combatants and noncombatants alike (proportionality and discretion). In many cases, a state can morally justify the use of nonlethal weapons "on the basis of moral and legal obligations to stop wrongdoing, to provide protection and justice, and to promote the return to order" (Coppernoll, 1999). However, the emergence of the Internet and cyber warfare seem to undermine the essential ethical and practical tenants of Just War doctrine, allowing a grey area for states to pursue state interest otherwise unchecked.

In summation, all of these new technological systems create an environment where the Just War doctrine seemingly cannot be applied. Just War doctrine demands accountability of actions, whereas cyber-attackers can remain anonymous and thereby escape any negative repercussions that may usually follow. Just War doctrine demands

just motivations, but often the motivations of cyber-attacks remain mysterious and unidentifiable. By obscuring these principles, Just War doctrine loses its potency in how states interact with one another through cyberspace and results in the need to develop new norms in this space. While there seems to be research on the implications of cyber warfare, there seems to be little research on how powerful states are setting the tone on the issues within cyber warfare.

Case Background: the United States

I will investigate two case studies for this research: the United States and China. The areas that I describe are relevant to cyber warfare and international relations broadly, not only each case in question. For the background of the United States, I will provide a brief overview of the composition and history of the United States, outlining how the government is structured in general. Then I will detail how the media is involved in American society. This is important as the media is treated very differently in the United States than in the other case, China. I will then briefly cover how the U.S. government funds its military operations. This is to provide an idea of how much of the national budget is spent on the military. I will then discuss the military operations the United States has been involved in since the fall of the Soviet Union. This is the era where cyber warfare began to appear, so it is important to understand how the U.S. was using its military conventionally. Then I will cover how the United States is linked with other states internationally. This is to give an idea of not only the breadth of her allies, but also the reach of her power internationally. To finish, I will cover how cyber warfare has unfolded in an American context.

The United States stands as "the world's oldest, continuing, modern federal democracy" (Tarr, 2005). The United States Constitution came in effect in 1788 and has become widely regarded as the beginnings of modern federalism (BBC, 2012; Tarr, 2005). This constitution has served as the model and guide for federal democracy worldwide, with many of its key principles gaining acceptance across the globe. Many of these principles are taken for granted in the modern age, such as federalism, the separation of powers, an independent judiciary, and individual rights (Tarr, 2005).

When it was founded, the United States was comprised of thirteen states, with a population of 2.5 million (Tarr, 2005). Today the United States has expanded to fifty states, a federal district, fourteen island territories (e.g. Puerto Rico), and 562 federally recognized Native American tribes (Tarr, 2005; U.S. State Department, 2011; CivilRights.org, 2016). As of July 2015, the United States had approximately 321.4 million residents, a far cry from its beginnings (U.S. Census Bureau, 2015). Modern demographics in the United States reflect U.S. history of immigration. As of July 2015, about 62% of the population was white, but this figure included a variety of different European ancestries other than those from the United Kingdom (U.S. Census Bureau, 2015; Tarr, 2005). Additionally, about 18% of the population was of Hispanic or Latino descent, about 13% of the population was African American, about 6% of the population was of Asian descent, about 1% of the population was of American Indian or Alaska Native descent, and less than 1% of the population was of Native Hawaiian and other Pacific Islander descent (U.S. Census Bureau, 2015). While never specified in the United States Constitution, English is the national language by social custom (Tarr, 2005).

The country itself has grown into a large, complicated patchwork of overlapping local and regional governments and governing structures, all responsible to the national government. The United States federal government was founded on the ideas of divided, shared, and limited powers. This was intended to both separate powers of the national and state governments, but also to allocate authority among the federated state (Pagano, 2009). As the United States has become more influential internationally, the powers of the president have also expanded. The Constitution vested a major role concerning foreign policy to the president, making their position particularly impactful in the international arena (Tarr, 2005).

Media

Freedom House rated the United States being free in the press and the "net" (in reference to the internet) (Dunham, 2016). The free press has a long tradition in the United States and is protected within the constitution of the United States, granted special protections in the First Amendment (Shah, 2012; Press Reference, 2016a). These strict protections for the press was part of what made the early United States markedly different from its contemporaries (Press Reference, 2016a). "A free press is crucial for a functioning democracy, but if not truly free, paves the way for manipulation and concentration of views, thus undermining democracy itself" (Shah, 2012). The arguments that protect the free press and other forms of modern media, coupled with the concept of free speech, influence the manner that the Internet is treated within the United States. It is often taken for granted in the United States that a unobstructed Internet is essential for democracy to function in the modern age.

The media in the United States has had many problems in recent years, not limited to: sliding profits, plagiarism scandals, propaganda scandals, and shrinking audiences (Shah, 2012). The omissions, distortions, inaccuracies, and biases in the media within the United States has been acknowledged by people outside the United States, and only recently being acknowledged within the United States (Shah, 2012). In general, foreign media representatives are treated much like domestic ones (Press Reference, 2016a). That is to say that foreign journalists are not required to acquire a special visa or are restricted to sending news back to their home countries (Press Reference, 2016a). However, the media has played an increasingly complicated role in society (Dunham, 2016). A major focus of the appeal of a particular presidential candidate has been their criticism of and antagonism towards individual journalists and media outlets (Dunham, 2016). This could signal a mistrust between at least a section of the American public and the media.

There is no formalized censorship in the United States, meaning there is no official mechanism in place for the government to censor media in the United States (Press Reference, 2016a). Rather there is something called "market censorship" (Shah, 2012). This is where the mainstream media will not run news stories that could offend either its advertisers or its corporate owners (Shah, 2012). In this manner, the media often does not report on important issues (Shah, 2012). Additionally, the mainstream media will provide coverage for what will attract audiences over providing objective coverage (Shah, 2012). They tend to cater to what the media outlet believes that the what their audiences would like to read about, rather than events and topics that would be considered more traditionally news worthy. However, there are pressures outside of corporate interest that affects media

coverage. Both political and cultural influence media coverage in the United States. Dan Rather, a member of CBS, noted that American journalists felt immense pressure from patriotic fervor following the September 11 terrorist attacks (Shah, 2012). This often translated to a resistance to asking tough questions that could criticize America too far (Shah, 2012).

Economics

The United States continues to increase its spending steadily, however the defense budget is also in decline. In 2014, the U.S. federal government spent approximately $3.23 trillion (InsideGov.com, 2016a). While the majority of this money was spent on mandatory spending (accounting for about $2.15 trillion of federal spending), only $1.09 trillion was dedicated to discretionary spending (InsideGov.com, 2016a). Defense spending falls into discretionary spending, accounting for about 17% of federal spending or 51% of discretionary spending in 2014 (InsideGov.com, 2016a). In 2015, the U.S. federal budget was approximately $3.36 trillion (InsideGov.com, 2016b). While spending increased over all, about $2.29 trillion was spent on mandatory spending and $1.06 trillion was discretionary spending (InsideGov.com, 2016b). The defense spending decreased, to about 16% of federal spending or 50% of discretionary spending in 2015 (InsideGov.com, 2016b). Federal spending is estimated to reach $3.95 trillion in 2016 (InsideGov.com, 2016c). Of this money, $2.44 trillion is estimated to be spent on mandatory spending and $1.1 trillion is estimated to be spent on discretionary spending (InsideGov.com, 2016c). The declining trend for defensive spending continues, with only an estimated 14% of federal spending or 49% of discretionary spending going to national defense in 2016

(InsideGov.com, 2016c). This declining budget has effects on how the U.S. armed forces operate both on and off engagements, requiring either cuts or innovations in tactics.

Military operations

In the United States, there is a long-standing law that "requires that any new weapon undergo a legal review by the Judge Advocate General of the military department involved" in order to verify the weapon's intended use is consistent with all treaties the United States is party to (Coppernoll, 1999). Additionally, any weapons bought or acquired by the United States must also be consistent with applicable treaties and international law, cleared by the Under Secretary of Defense for Acquisition and Technology. These measures are coordinated in conjunction with the Office of the Secretary of Defense General Counsel and the Under Secretary of Defense. All contracts must be legally reviewed before being awarded to the engineering and manufacturing contractors and reviewed again before the initial production of new weaponry (Coppernoll, 1999).

The United States has been involved in many military interventions since the fall of the Soviet Union. In the 1990s, these interventions included, but were not limited to: the First Gulf War, the Somali civil war, the Bosnia war, the Kosovo war, and "Operation Desert Fox" (Kutsch, 2013). While some of these interventions involved traditional soldiers, many of these interventions were from a distance, involving airstrikes or cruise missile strikes. They were often—but not always—framed as humanitarian interventions. Following the September 11 terrorist attacks, many large-scale operations followed. These operations included, but were not limited to: the Afghanistan war; the Iraq invasion and

occupation; and a drone campaign in Pakistan, Yemen, and Somalia. These interventions were almost always framed as attacks against "terrorists" or those who were suspected of cooperating or aiding terrorists. Some of these interventions continue to this day. In more recent years, the United States was involved in the Libyan uprising, providing air support in NATO-led airstrikes against Muammar Gaddafi's regime (Kutsch, 2013). The framing here returned to humanitarian efforts in the conflict.

Now that President Obama's tenure is near its end, there has been discussion of something called the "Obama Doctrine" (Goldberg, 2016). The term *Obama Doctrine* is meant to conceptualize the shift that Obama's presidency has had on American foreign policy. President Obama's policy has been to avoid conventional military interventions in all cases that are not existential threats to the United States. It is a rejection of the traditional Washington playbook, that President Obama sees as overly reliant on physical force as a credible deterrent. In cases that guarantee results with minimal to no collateral damage, President Obama did not hesitate to use force (Goldberg, 2016). John Brennan, President Obama's CIA director, has said the following on their mutual perspective on interventions:

> "[We] have similar views. One of them is that sometimes you have to take a life to save even more lives. We have a similar view of just-war theory. The president requires near-certainty of no collateral damage. But if he believes it is necessary to act, he doesn't hesitate" (Goldberg, 2016).

President Obama is a proponent of multilateral interventions, using them as a partial check of American hubris and as an effort to reduce the number of "free riders" benefiting from

American military power. President Obama's perspective also marked a shift away from the Middle East towards Asia (Goldberg, 2016).

International linkages

The United States is party to several collective defense arrangements internationally. The most notable in the North Atlantic Treaty (NATO), which has a clause stating if one of the members is attacked, all the other states will respond in kind (U.S. State Department, 2016). Other members of NATO include: Albania, Belgium, Bulgaria, Canada, Croatia, the Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy Latvia, Lithuania, Luxembourg, the Netherlands, Norway, Poland, Portugal, Romania, the Slovak Republic, Slovenia, Spain, Turkey, and the United Kingdom (U.S. State Department, 2016). There is an agreement between the United States, Australia, and New Zealand, signed in September 1951, stating that if there is an attack in the Pacific, all parties would work together to defeat the threat (U.S. State Department, 2016). There is a bilateral agreement between the United States and the Philippines, signed in August 1951, where both parties would work together to defeat a threat in the Pacific upon an attack (U.S. State Department, 2016). The United States is party to the Southeast Asia Treaty, signed in September 1954, which works similarly as the previous two agreements in the Pacific area (U.S. State Department, 2016). The states party to this agreement are: Australia, France, New Zealand, the Philippines, Thailand, and the United Kingdom (U.S. State Department, 2016). There is also the bilateral agreement between the United States and South Korea, signed in October 1953, which operates as the previous three agreements in the Pacific area (U.S. State Department, 2016). There is a bilateral

agreement between the United States and Japan, signed in January 1960, where an attack on either Japanese or American forces in Japanese territories would trigger a response from both parties (U.S. State Department, 2016). Finally, the United States is also party to the Rio Treaty, signed in September 1947, where an armed attack against any American state would be considered an attack on them all (U.S. State Department, 2016). The other parties to this treaty are: Argentina, the Bahamas, Bolivia, Brazil, Chile, Colombia, Costa Rica, Cuba, the Dominican Republic, Ecuador, El Salvador, Guatemala, Haiti, Honduras, Nicaragua, Panama, Paraguay, Peru, Trinidad & Tobago, Uruguay, and Venezuela (U.S. State Department, 2016).

Context of cyber warfare

The United States has understood the threats emanating from cyberspace as early as the 1990s at a high-level (Dombrowski & Demchak, 2014). Unlike other countries, the United States "is in a unique position because of its intensive and extensive use of space-based systems and computer networks" (Delpech, 2012). The United States has a "decades-old and growing dependence" on ICTs for both economic and military dominance (Dombrowski & Demchak, 2014). While the United States has asymmetrical advantages in ICTs, it also has major weaknesses. It is most reliant on these spaces, making the United States the most at risk in the face of cyber warfare in the world (Delpech, 2012). In 1996 President Clinton signed Executive Order 13010, creating the President's Commission on Critical Infrastructure Protection (Dombrowski & Demchak, 2014). This executive order included measures to protect economic and national security interests from cyber-attacks. Several cyber security-related organizations were established under the

Presidential Decision Directive 63, born of recommendations from the presidential commission and mostly focused on threats posed by malicious hackers or cybercriminals seeking to attack critical infrastructures. The threat of cyber-attacks only increased after the September 11 terrorist attacks in 2001. Materials were found in Al Qaeda hideouts that provided instructions on how to use electronic methods to attack the United States. These materials suggested that most of Al Qaeda's future efforts against the United States would involve cyberspace (Dombrowski & Demchak, 2014).

Case Background: the People's Republic of China

For the background of China, I will provide a brief overview of the composition and history of the China, outlining how the government is structured in general. Then I will detail how the media is involved in Chinese society. This is important as the media is treated very differently in China than in the U.S. I will then briefly cover how the Chinese government funds its military. This is to provide an idea of how much of the national budget is spent on the military. Because China has not been involved in any open military operations since the fall of the Soviet Union, I will not describe any military operations in this section. Then I will cover how the China is linked with other states internationally. This is to give an idea of not only the breadth of her allies, but also the reach of her power internationally. To finish, I will cover how cyber warfare has unfolded in a Chinese context.

China is not only the second-largest economic power in the world today, but China is also on the permanent United Nations Security Council and is the only Communist Party-led state in the G-20 (Lawrence & Martin, 2013). These—among other things—make

China a truly unique actor in the modern world. The Chinese Communist Party came to power in 1949 after a has stayed in power ever since. The institutions within the Chinese government reflect the Party's commitment to maintaining its monopoly on the government, remaining largely intolerant of dissent. However, many analysts outside of China would not call Chinese institutions as "monolithic" or "rigidly hierarchical." There are those both inside China and abroad that find China's political system unsustainable, calling for political reform (Lawrence & Martin, 2013).

Media

Freedom House rated the Chinese media as not free, not having the freedom of the press or freedom on the "net" (Dunham, 2016). The Chinese Communist Party, as a monopolistic regime, emphasizes central control of the press as a government tool for public education, propaganda, and mass mobilization (Press Reference, 2016b). The "mass line" governing theory is the linchpin for the Chinese government, where Chinese officials are not elected by the people they govern. Government officials are not held responsible to the population, but are instead held responsible to the Party. This responsibility extends to journalism in China, where the media becomes an arm of the state. The media is meant to educate the people in a top-down fashion, moving the population towards socialist progress. The media only reports on the implementation and impact of policies, but not the internal policy-making process itself (Press Reference, 2016b). This makes gaining insight into Chinese government actions very difficult, leaving much of Chinese policy quite mysterious.

Within the Chinese Constitution itself, Article 35 states that "citizens of the People's Republic of China enjoy freedom of speech, of the press, of assembly, of association, of procession and of demonstration" (Press Reference, 2016b). However, several laws and administrative orders have been put into place in order to regulate the media since 1949. For example in 1994, there were regulations circulated in top media institutions that stipulated many requirements for the media, including but not limited to: no private media ownership and no discussions of a press law. The Party reserves the right to make any information a "state secret," including information already publically available. With this in mind, it has been made clear that sharing classified documents in any manner is strictly prohibited in Chinese media. While there is little pre-publication censorship, the threat of post-publication censorship is omnipresent. Punishment for writing anything the Party does not approve of could result in requiring writing a self-deprecating statement to imprisonment (Press Reference, 2016b).

In order to maintain control over the flow in information in China, the government has created a filtering system popularly known as the "Great Firewall" (Crowcroft, 2016). This filtering system censors what is available to Chinese citizens via the Internet. The Great Firewall blocks many internationally popular websites, such as: Google, Facebook, Twitter, Instagram, YouTube, and some of the world's largest news outlets. On search engines allowed past its defenses, the firewall can also censor what results it allows for citizens to view. For example, any references to the 1989 Tiananmen Square Massacre are blocked by the Great Firewall. Some Chinese citizens have relied on using virtual private networks (VPNs) to work around the Great Firewall; however, the Chinese government

began blocking VPNs in March 2016. President Xi Jinping has been fortifying the Great Firewall since he took office. Before his presidency, 14% of all Internet sites were blocked. Now that number has risen to 25% of all Internet sites, coinciding with suppressing the freedom of the press greatly (Crowcroft, 2016).

Economics

Unfortunately, the Chinese government only releases their spending after the year is complete. This means that reporting on government expenditure is a year behind. In 2013, the national government expenditure was 140,212.10 hundred million yuan (National Bureau of Statistics of China, 2014). Of that budget, approximately 7,410.62 hundred million yuan were spent on national defense (National Bureau of Statistics of China, 2014). In 2014, the national government expenditure was 151,785.56 hundred million yuan (National Bureau of Statistics of China, 2015). Of that budget, approximately 8,289.54 hundred million yuan was spent on national defense (National Bureau of Statistics of China, 2015). This indicates that China is increasing its defense budget, allowing for its military to modernize faster and operate in larger numbers as the years progress.

International linkages

China is party to three major international agreements. Foremost is the treaty of "friendship and cooperation" signed between Russia and China in July 2001 (Tyler, 2001). This agreement is an attempt to be a check against NATO—namely the United States—after the Cold War. It promises joint military opposition against U.S. frameworks for international security. While there are no overt mentions of military cooperation in the agreement itself, there are promises to coordinate responses closely following aggressive

pressure or an act of aggression from another power. The agreement also reaffirms an opposition to humanitarian interventions from both parties (Tyler, 2001). In June 2001, the Shanghai Cooperation Organisation (SCO), a permanent intergovernmental international organization, was created (Russia's Presidency in BRICS, 2014). There are six states, including China, party to this organization. The other countries are: the Republic of Kazakhstan, the Kyrgyz Republic, the Russian federation, the Republic of Tajikistan, and the Republic of Uzbekistan. This organization is both economic and military in nature, seeking to promote anti-terrorism activities, anti-mafia activities, and establishing a free-trade zone in the area (Russia's Presidency in BRICS, 2014). In June 2002, the Asia Cooperation Dialogue was established, creating a continent-wide forum in Asia (Asia Cooperation Dialogue, 2016). There are thirty-four members in the organization, including China. The other party states are: Bahrain, the Republic of Korea, Pakistan, Thailand, Bangladesh, India, Lao PDR, the Philippines, Vietnam, Brunei Darussalam, Indonesia, Malaysia, Qatar, Cambodia, Japan, Myanmar, Singapore, Kazakhstan, Kuwait, Oman, Sri Lanka, Bhutan, Iran, Mongolia, the United Arab Emirates, Russia, Saudi Arabia, Tajikistan, Uzbekistan, the Kyrgyz Republic, Afghanistan, Turkey, and Nepal. The purpose of this organization is to increase solidarity and cooperation in the region (Asia Cooperation Dialogue, 2016).

Context of cyber warfare

While the Chinese are relatively new to cyber warfare, the Persian Gulf War of 1991 demonstrated to the Chinese the effectiveness of highly-advanced technological militaries (Dombrowski & Demchak, 2014). The Chinese saw the superiority of the U.S.

troops in that conflict, serving as the driving factor for China to develop their own technological capabilities. Some suggest that this led the Chinese to rediscover Sun Tzu's concept of "indirect warfare." Within the Chinese military itself, there have been suggestions of "unconstrained warfare." This kind of campaign would begin long before any armed conflict would be apparent, wanting to takedown potential enemies by using vulnerabilities within their own information systems. This concept would disregard international norms or laws (Dombrowski & Demchak, 2014). It has been said by a Western analyst that "China [now] has the most extensive and most practiced cyber-warfare capabilities in Asia, although the technical expertise is very uneven" (Ball quoted by Dombrowski & Demchak, 2014).

CHAPTER 3: METHODS

As a researcher, my worldview is complex. I would classify myself as something between a social constructivist and pragmatist. Creswell described social constructivists as people that "hold assumptions that individuals seek understating of the world in which they live and work. Individuals develop subjective meanings of their experiences—meanings directed toward certain objects or things" (Creswell, 2009). Furthermore, Creswell explicated that social constructivists find these meanings to be varied and multiple in nature, allowing for complexity in how people understand reality. For the social constructivist, reality becomes a negotiated—both historically and culturally—space (Creswell, 2009). In an individualistic sense, I agree with this standard social constructivist worldview. That is to say that any research I may conduct, I approach with my own implicit understandings of the world that could potentially influence my research. This means that I must check myself throughout my research process in the attempt to not pass impromptu judgements as a key part of my reflective practice. As an American, it would be easy to be ungenerous to China, becoming overly sympathetic to the stance of the United States.

However in a larger sense, I ascribe more to what Creswell described as a pragmatic worldview, where there is more of a concern of applicability, stemming from actions, situations, and consequences (Creswell, 2009). Creswell further explained that pragmatists see the truth as "what works at the time," while also agreeing that research is embedded

within social, historical, and other contexts (Creswell, 2009). I also agree with this worldview, but in a larger sense. I believe that there is also an independent truth to how the world is and how it operates away from perception. This pragmatic belief is the driver of my critical analysis of this paper. Therefore, this research is centered on what is practically happening in the discourse and alleged action in cyber warfare.

The driver behind this paper is the suspicion that not only are what states doing and saying in regard to cyber warfare at odds, but also it is really what states are doing that will really set the foundations for how cyber warfare develops. Cyber warfare is hard to create legislation for, as cyberspace is fundamentally an information network across national lines. States will likely continue to act as they please unless there is viable legislation in place, demarking the actual bounds of acceptable action through action in the moment.

My aim is to critically investigate the actions and frames of state actors engaged in cyber warfare. Cyber warfare is new ground in terms of weaponry and method of attack. Some would argue that this means that new ethical frames are required in order deal with this new frame of war. While it is true that old ethical frames are ill-suited for managing or mitigating cyber warfare as things currently stand, I suspect that what is happening today harkens back to older ways of waging war, regardless of the new mode of attack.

In order to answer the underlying thesis of this paper, I investigated two exploratory case studies: the United States and China. In the international system, the United States, China, and Russia are the trendsetters—or at least the most vocal—around cyber warfare and could thereby be called the "critical cases" for cyber warfare, defined as "having strategic importance in relation to the general problem" (Flyvbjerg, 2006). Unfortunately,

due to both time constraints and a lack of available public data, doing all three was not feasible. Both the United States and China had sufficient data available, therefore those were the two cases I worked with. This set of cases does not constitute a true comparative case study analysis because I am not trying to figure out which case is "better," but rather gain an in-depth understanding of the direction of cyber warfare. A collective case study would be a more accurate description of this paper, defined as "several cases … studied to form a collective understanding of the issue or question" (Stake referenced in Simons, 2009).

This approach is particularly useful in the area of cyber warfare. The clandestine nature of cyber warfare adds broad difficulties unique to the topic. Its nature does not allow for most or any government officials to discuss cyber warfare particulars in interviews, talks, or reports. Most interviews, talks, or reports will be heavily censored to protect classified interests or project a particular image to the world at large. While I am definitely interested in the image or frame that each case is attempting to present for cyber warfare, I also need to access details on what is actually happening in each event. For this reason, I have to rely heavily on news reports for information relating to state actions, corroborated as much as possible through publically available official reports. Reporters often have access to anonymous sources or a classified report that I as a regular civilian would not have access to.

The data I am using for this investigation are in the form of news articles, policies, and statements, speeches, and interviews from government officials. As previously stated, I am using news articles as a response to the clandestine nature of cyber warfare. While

the actions within cyber warfare are steeped in mystery, government policies are public. I am using policy to understand what each state considered legal in cyber warfare. Where there is little formal policy, strategy documents can also assist in this matter. I am using the statements, speeches, and interviews of government officials to understand how each state frames cyber warfare. These statements are comparable because they come from similar positions of power or similar governmental departments (such as President Barak Obama to President Xi Jinping, the U.S. State Department to the Ministry of Foreign Affairs, and the U.S. Department of Defense to the Ministry of National Defense).

These two cases are not perfectly comparable. Firstly, the United States is an established world military power and has been for a significant amount of recent history. This has two effects. On the one hand, China is just not yet on the same military footing as the United States, making comparisons inexact. On the other hand, the United States simply has a greater continuity within the modern world framework than China, often making it easier to see how the United States has evolved over time. Secondly, there are different demands on each state internationally. The United States has been "policing" the world since the end of the Cold War and has specific obligations to a mostly European cohort of states. China does not have the same kind of international obligations and has not been as involved in conflict on the scale that the United States has been as of the past century.

There is a concern particular to the case of China. I do not speak any Chinese; therefore, I must rely on the English translations of data. This could be problematic as both official documents and news reports are translated or produced specifically for Western

consumption. This could result in having an incomplete or misleading image of either the official Chinese stance or acts of cyber warfare China may or may not be involved in. This is a limitation of my research, however I attempted to ameliorate this issue as much as possible by trying to find a diverse, non-Western supply of information when available.

CHAPTER 4: UNITED STATES
THE WORLD SUPERPOWER

To begin, I will present the most notable example of the United States engaging in cyber warfare. This case is of particular importance to cyber warfare as a whole and cannot be understated. Then I will present how the United States frames and discusses cyber warfare. To finish, I will discuss how the actions of the United States align with what they say are their intentions for acting internationally.

Stuxnet: the first cyberweapon

Shortly after President Obama took office, the White House released its "Cyberspace Policy Review" (2009) (the White House, 2016). This was President Obama's first effort to address U.S. cybersecurity. The document itself touched on many of the themes that came to prominence in years to come. The policy review openly stated the vulnerability of the United States to cyber-attacks (the White House, 2009). Finding the U.S. digital infrastructure neither secure nor resilient, the policy review emphasized the responsibility of the U.S. government to its people to strengthen cybersecurity measures in order to protect U.S. citizens from "the growing threat of cybercrime and state-sponsored intrusions and operations" (the White House, 2009). Already by 2009, the United States government had fallen prey to intrusions from both cybercriminals, nation-states, and other entities (the White House, 2009). The policy review document cited three examples of how ineffectual cybersecurity could harm the United States: destruction of critical

infrastructures, exploitation of globalized financials services, and systematized loss of U.S. economic intellectual property (the White House, 2009). Many of the concerns laid out by this policy review revealed areas that the United States planned to attack in the months and years to come. While speculative, it is entirely possible that the United States was coming to understand its own cyber-fragility by its efforts to attack and undermine the cyber defenses of others.

In January 2010, inspectors from the International Atomic Energy Agency, the UN's nuclear facility watchdog, noticed that about half of the centrifuges in Iran's Natanz uranium enrichment plant did not function and the other centrifuges yielded very little (Economist, 2010; Zetter, 2014). The rate of failure for the centrifuges was unprecedented and mysterious to both the Iranian technicians and the UN inspectors onsite. In a seemingly unrelated event in June 2010, Iran contacted a security firm in Belarus, VirusBlokAda, to help troubleshoot Iranian computers that were crashing and rebooting repeatedly for no apparent reason (Zetter, 2014). Upon investigating, VirusBlokAda identified a handful of malicious files on one of the Iranian systems that ostensibly caused the system malfunctioning (Economist, 2010; Zetter, 2014). The malware had counterfeited digital certificates, making it appear the malware came from reliable sources. The antivirus community did not have the capacity to handle these falsified certificates, as that kind of threat had never been encountered before. The automated malware-detection programs simply could not identify the malware because of the forged digital certificates (Kushner, 2013). These malicious files were a part of the world's first cyberweapon, Stuxnet, a 500-kilobyte computer worm (Zetter, 2014; Kushner, 2013).

Stuxnet was the first cyber-attack of its kind. It was the first cyber-attack to reach beyond the workings of a digital system and actually physically destroy equipment controlled by a computerized system (Zetter, 2014). Early versions of Stuxnet manipulated the pressure within the centrifuges by tinkering with the valves, increasing the pressure inside the centrifuges and damaging both the devices and the nuclear enrichment process. After approximately a year of letting these early versions take a toll on Natanz, Stuxnet creators changed the worm in 2009 (Zetter, 2014). This new version attacked the Iranian systems in three phases. To begin, Stuxnet targeted computers running Microsoft Windows and networks of computers, replicating itself through those devices (Kushner, 2013). Then Stuxnet targeted Windows-based computer systems designed by a German firm, Siemens (Zetter, 2014; Kushner, 2013). These management systems controlled and monitored industrial equipment, such as: controller valves, pipelines, and enrichment equipment (Economist, 2010; Zetter, 2014; Kushner, 2013). The particular piece of Siemens software targeted was called WinCC, a specific supervisory control and data acquisition (SCADA) system (Economist, 2010). SCADA systems are not usually connected to the Internet due to their essential nature to a facility's functioning; operators do not want to allow remote hackers to directly reach SCADA systems (Economist, 2010; Zetter, 2014). Finally, Stuxnet would compromise the programmable logic controllers on the systems (Kushner, 2013). In doing this, Stuxnet creators could simultaneously monitor the system and cause damage to industrial parts.

To overcome the obstacle posed by isolated SCADA systems, Stuxnet creators figured out how to make the worm spread via infected USB flash drives (Economist, 2010;

Zetter, 2014). The worm would start itself once the USB was inserted into a computer (Zetter, 2014). Then the worm would check to see if the computer was running WinCC (Economist, 2010). If the worm detected WinCC on the computer, it would attempt to infiltrate the program. To do this, Stuxnet would attempt to simply log onto the software. If the worm was successful, Stuxnet would then install a clandestine "back door" to the Internet. This would desegregate the system, allowing servers in either Denmark or Malaysia to supply instructions to the system. However if WinCC was not found on the computer upon startup, Stuxnet would attempt to self-replicate onto other USB devices or spread across the local network of computers (Economist, 2010). In order for Stuxnet to succeed, the creators had to infect five private companies outside of Iran first, which were believed to have connections to the Iranian nuclear program. These companies unwittingly carried the updated version of Stuxnet as "patient zero," helping the spread and transport of the worm to otherwise protected facilities on infected flash drives (Zetter, 2014).

At first, it was believed that Stuxnet was simply another attempt at industrial espionage or blackmail, serving as a credible threat from hackers to completely shutdown vital systems (Economist, 2010). However, these explanations did not fit the design of Stuxnet. WinCC was not a common SCADA system by any means and hackers trying to target a large pool of companies would have been better off targeting a different, more popular SCADA system. Additionally, Stuxnet would only launch itself when it found a particular configuration of industrial equipment, searching for a match (Economist, 2010). The creators took great care to ensure Stuxnet would only affect specific targets (Broad, Markoff, & Sanger, 2011).

Oddly, the worm utilized four different zero-day vulnerabilities (Economist, 2010; Kushner, 2013). Stuxnet used two compromised security certificates to gain system-level privileges, a shared print-spooler vulnerability to spread on local networks, and a security hole in Windows itself to launch itself automatically and to spread on USB drives (Economist, 2010; Kushner, 2013). While using a zero-day vulnerability is not particularly unusual, they are incredibly valuable to hackers. These vulnerabilities are so valuable that it is extremely unusual for a hacker to use more than one on any given cyber-attack (Economist, 2010). Stuxnet creators seemed to have used four to increase the chances of success, using them in extremely complimentary ways (Economist, 2010; Kushner, 2013). The design of Stuxnet also required specific knowledge of Siemens's industrial-production processes and control systems, along with the specific blueprints of the targeted facility (Economist, 2010). For all of these reasons, it would be almost impossible for an amateur, a cybercriminal, or a malicious hacker to have created Stuxnet. The design of the worm would require a well-financed team of experts, making a state the only likely backer of the worm (Economist, 2010; Kushner, 2013).

However, the initial discovery of Stuxnet brought other cyberweapons to light. In 2012 a precursor to Stuxnet, a 20-megabyte piece of malware that came to be known as Flame, was discovered (Kushner, 2013). At first Flame was believed to be unrelated to Stuxnet, but Flame was eventually found in the heart of Stuxnet's code. While Stuxnet was designed with destruction in mind, Flame was designed with espionage in mind. Flame could secretly search from key words on classified PDF files and send document summaries of files from infected computers (Kushner, 2013). Where Stuxnet had overt

symptoms such as system crashes, Flame could function unseen. Flame would only transmit small piece of information at a time to avoid notice from system monitors.

Flame was particularly insidious because of its method of infection. Flame disguised itself on a Windows 7 operating system update (Kushner, 2013). Users would believe they were downloading a legitimate patch from Microsoft to protect their systems, but would instead download Flame and compromise them. This infection method was more remarkable than the program itself, which was quite sophisticated in its own right. It was estimated by antivirus community experts that there were only about ten programmers in the entire world that had the ability to design that kind of behavior in a piece of software. Flame creators broke some of the world's best encryption, something that would require a supercomputer and many scientists (Kushner, 2013).

In August 2010, Microsoft claimed that Stuxnet had successfully infected more than 45,000 computers and fourteen industrial facilities in Iran (Economist, 2010; Kushner, 2013). By June 2009, the Nanatz facility had been able rebound from the early versions of Stuxnet (Zetter, 2014). At the beginning of the year, technicians began installing new centrifuges once more. By the end of February, approximately 5,400 centrifuges had been replaced. While not all of the centrifuges were functional yet, the facility was progressing nuclear material again. By June, technicians had replaced 7,052 centrifuges. Of the centrifuges in place, 4,092 centrifuges operational. Production numbers were up 20% and were expected to remain consistent over the summer of 2009. It was projected that Iran would be able to make two nuclear weapons within the year at the rate they were enriching

uranium (Zetter, 2014). This was the moment that the new version of Stuxnet arrived at the facility.

It's unclear how long it took the modified version of Stuxnet to reach the target facility after the perpetrators infected the "carrier" companies (Zetter, 2014). However, between June and August of 2010 the centrifuges were not putting out the same amount of product. By the end of August, the number of functioning centrifuges decreased by 328 centrifuges, leaving only 4,592 centrifuges functioning. By November, the number of functioning centrifuges dropped further to 3,936 centrifuges. In other words, the number of working centrifuges dropped by 984 in the course of five months. Throughout this entire period, new machines were being installed, but none of the new machines were processing nuclear product. Technicians at the facility saw the problems they were experiencing, but could not understand why those problems were presenting (Zetter, 2014). Stuxnet was able to hide its activities in the facility by replaying recordings of the projected system values during the attack, making it appear the facility was operating as normal (Kelley, 2013; Broad *et al*., 2011). Iran initially denied reports that Stuxnet destroyed centrifuges in their facilities; however, the changes within the facility matched the attack pattern of Stuxnet (Zetter, 2014; Kushner, 2013; Sanger, 2012). Iranian officials later claimed that technicians had found Stuxnet and had contained the worm (Sanger, 2012). In a 2010 statement that did not name Stuxnet directly, Iranian President Mahmoud Ahmadinejad admitted a malicious piece of software damaged Iranian centrifuges (Clayton, 2010).

Stuxnet marked a shift in geopolitical conflicts, where cyberweapons—an imagined, theoretical threat—suddenly became a plausible reality. Stuxnet was the first

foray into a state-against-state cyberwar (Kushner, 2013). If the creators of Stuxnet were trying to stop all Iranian efforts at creating a nuclear weapon, they were only partially successful. Stuxnet seems to have destroyed about a fifth of the centrifuges in Iran, helping to delay Iranian attempts of creating a nuclear weapon. Parts of Iran's operations stopped completely and other parts survived the cyber-attack (Broad *et al.*, 2011). Research commissioned by a NATO defense center claimed that the cyber-attack was likely an illegal "act of force." Of the twenty experts that produced the report, all were in agreement that Stuxnet was an act of force, action prohibited under the charter of the United Nations except in times of self-defense. However, it was not as clear that Stuxnet sufficiently constituted an "armed attack," a kind of aggression that would justify a response from Iran (Zetter, 2013).

While no one in the international community has officially claimed responsibility for Stuxnet, officials from the United States and Israel leaked information to the press strongly suggesting the cyberweapon was a result of a partnership between the two states (Kushner, 2013). Stuxnet was reportedly tested at the Israeli Dimona nuclear complex (Kelley, 2013). This facility spun nuclear centrifuges nearly identical to those found at Nanatz; however, neither American nor Israeli officials will speak of Stuxnet officially, let alone admit to having anything to do with its creation (Broad *et al.*, 2011). It was only in 2012 that American officials admitted to developing cyberweapons, but they have not admitted to using any of the cyberweapons developed (Sanger, 2012). Interestingly, some computer scientists claim that knowingly or not, both the Germans and the British helped with the creation of Stuxnet (Broad *et al.*, 2011).

It was clear that this attack was not meant for economic gains, but political ones (Kushner, 2013). In 2008, President G.W. Bush refused a secret Irsaeli request to attack Iranian nuclear facilities with specialized bunker-busting bombs (Sanger, 2009). At the time, President Bush had already authorized a new clandestine program, code-named Olympic Games, in order to sabotage Iran's suspected efforts to create a nuclear weapon (Sanger, 2009; Sanger, 2012). The Bush administration had come to the conclusion that while sanctions imposed on Iran were failing to slow down Iranian uranium enrichment efforts, an overt attack would likely prove ineffective, further driving Iran's efforts out of view (Sanger, 2009). Once he took office, President Obama sped up the program (Broad *et al.*, 2011). Understanding the unprecedented area they were working in, the Obama administration was resistant to developing a "grand theory for a weapon whose possibilities they were still discovering" (Sanger, 2012). In 2012, President Obama said he would not allow Iran to obtain nuclear weapons (Goldberg, 2016). At the same time, the Israelis sped up their program against the Iranians, searching for a way to block Iranian advancements without triggering conventional warfare in response (Broad *et al.*, 2011). Unfortunately, all of this information came from current and former American, European, and Israeli officials in an anonymous capacity (Sanger, 2012). Much of the information surrounding the world's first cyberweapon remains highly classified, with parts of the worm still at work (Sanger, 2012).

Once a cyberweapon like Stuxnet is discovered, its code cannot be hidden. It is possible for hackers to reverse engineer the components of the cyberweapon, giving hackers either new ideas or new tools to use. Stuxnet was an incredibly sophisticated piece

of malware, providing anyone with access to highly advanced computing technology. Anyone can use the malware once they have sufficient training to use it. If these kinds of cyberweapons were to become more commonly used, the United States is in a particularly troubling position. There is no other state infrastructure more dependent on computer systems, and therefore more vulnerable to cyberweaponry, than the United States infrastructure. By releasing this kind of weapon into the world, the United States has only made it easier for other actors to attack the United States in a similar fashion (Sanger, 2012). This attack also made it readily apparent that there are many industrial machines vulnerable to this kind of cyberweapon. For example, it is possible to access the systems of the United States water utilities with the right kind of Google search terms (Kushner, 2013). Companies have been slow to update their systems, with some companies running 30-year-old operating systems (Kushner, 2013). All of these systems would be extremely vulnerable to an attack from a cyberweapon such as Stuxnet.

What does this event—the development and use of Stuxnet—tell us about cyber warfare? As the first attack that most international players identify as an act of force, rather than a form of espionage or possible prankster, this event is a defining moment for cyber warfare. The first notable attribute of the Stuxnet attack was its suspected multilateral nature. This clandestine project would not have been possible without the alleged cooperation of nations rather than one nation. Arguably, Stuxnet could be part and parcel of the *Obama Doctrine*; however, the initiative itself began under the Bush administration. Without alleged Israeli support, it is unlikely that the United States would have been able to pull off this kind of mission. But what about cyber warfare necessitated this

cooperation? Left to their own devices, it is unlikely that either state would have been able to create Stuxnet at the rate they did. Most importantly, it is unlikely that the states would have been able to keep the project hidden. In World War II, the nuclear program required a secure facility, the right minds, and the appropriate materials to be kept secret. This was relatively easy, as all of those things were attainable within the United States already and keeping a location deep within the United States is a comparatively simple task. Alternatively, Stuxnet required a secure facility, the right minds, advanced computers, an appropriate testing ground, and co-conspirators, suspecting or otherwise. The testing ground and the co-conspirators were the crux of the matter, where the United States could not create a facility similar enough to the Iranian facility to test the worm, whereas the Israelis would not have the connections necessary to infiltrate the appropriate co-conspirators necessary to disseminate the worm. Both states had a vested interest in keeping Iran away from nuclear capability, Israel fearing what a nuclear Iran could do in the Middle East and the United States having a great deal of interest in maintaining the Israeli state.

In a way, Stuxnet was an exertion of force by the Western block and a rising power in the Middle East. This mentality harkens back to Cold War era politics. During the Cold War, both the United States and the Soviet Union were notorious for interfering in the politics of developing nations. In these proxy wars, both states would supply arms and funding, covertly or openly, to various political movements within foreign states in order to achieve a particular political outcome within that foreign state. The point of a proxy war was not only to achieve a particular political outcome the more powerful state desired, but

also to accomplish that goal at minimal human or political cost to the more powerful nation at the same time. Many of these proxy wars left utter destruction behind. These proxy wars significantly influenced how the world has come to be shaped today.

How is Stuxnet like a proxy war? While not necessarily a completely comparable, there are aspects of Stuxnet that seem reminiscent of proxy wars. Without U.S. involvement in Stuxnet, it is unlikely that Stuxnet would have been developed. The United States provided the funding and arms to Israel (granted in a more joint fashion than in a traditional proxy war). Regardless of that, neither the U.S. or Israel were punished due to their alleged actions. This is in large part because they never claimed to be responsible for their actions. Because of the nature of how the worm operated, there only evidence—while strong evidence—is not sufficient to actually outright claim that the U.S. and Israel were directly responsible for the destruction of centrifuges in the Iranian facility. This meant that the aggressors were able to meet their political goals and were able to avoid almost all international repercussions.

Because there was no loss of human life in this attack, Iran's right to retaliate remains cloudy. That is to say that by the rules of proportionality, it is unclear if Iran had the right to either declare war or "respond in kind" on the creators of Stuxnet in response to the attack. Because Stuxnet was unprecedented, it is unclear what a proportional and rational response would even look like. In some ways, loss of life would have made it much easier to decide if Iran had a right to retaliate, but Stuxnet was not a worm designed to take down human life. This sets a precedent that cyber-attacks do not alone make retaliation permissible, but leaves the question open as to what sort of cyber-attack would.

As previously stated, Stuxnet is now available for others to use. In much the same way extremist groups have used remnants from proxy wars to engage in their own wars, Stuxnet could be turned around and used by others. It would be relatively easy for an actor—any actor—to create a cyberweapon like Stuxnet, but designed for loss of life in mind. There are other facilities, such as natural gas facilities, water treatment facilities, or electrical facilities, that rely on information networks in a similar fashion as the Iranian facility. What if a malicious actor gained access to nuclear power plant facilities? The meltdown in Japan a few years ago could pale in comparison to the destruction that would follow. These other facilities are often essential to not only national security, but also for life within a state. If the water treatment facilities within a state were to be destroyed, there is no telling the kind of loss of life that state would face. However, without a strong precedent set there is no telling what the appropriate response to such action would be.

Presidential policy

President Obama has tried several times to enact legislation to protect the United States from cyber-attacks. Cybersecurity has been a national security priority in the Obama administration (Schmidt, 2012). President Obama has put forward many policy directives and executive orders, such as the Presidential Policy Directive 8, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information" (2011); the Presidential Policy Directive 21, "Critical Infrastructure Security and Resilience" (2013); the Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" (2013); and the Presidential Policy Directive 28, "Signals Intelligence Activities" (2014) (the White House, 2016).

Cumulatively, these policies and initiatives indicate a strong desire from the U.S. government to create regulations to protect U.S. national interests. However, none of these measures constitute any comprehensive form of regulation on cyber warfare as a whole.

It may seem obvious, but it is still important to note that these policies and initiatives are all efforts to secure national interests. For this reason, the frame the United States is operating under a frame of securitization. A frame of securitization is to move items on the national agenda from one frame, such as economics or infrastructure, to one of security. Some of the items covered in these policy documents and executive orders are matters of national infrastructure or business. However, there are many benefits to making this move. Securitizing an issue can prioritize an issue within the media and the government. Issues of security tend to get more attention, often pushing a resolution forward. It can also give an issue more resources. Just as issues of security gain more attention, they also gain more funding and more human resources behind it. No one within a government would want to be accused of not taking the security of its people seriously. However, as the frame of security becomes increasingly dominant, securitization pushes other concerns to the background. Issues such as human dignity, economics, and liberty are often expendable in comparison to matters of security.

In his 2011 executive order, President Obama referred to how classified information must be secured, requiring a "sophisticated and vigilant means to ensure it is shared securely" (Obama, 2011). In the 2013 presidential policy directive, the White House outlined several areas that owners and operators of critical infrastructure must work together to become effective, such as: prevention, protection, mitigation, response, and

recovery (the White House, 2013). The purpose of that directive was to formalize the shared responsibility of all levels of the U.S. government, tribal and territorial entities, and the public and private owners of critical infrastructure in the United States (the White House, 2013). While the document acknowledged the existence of critical infrastructures owned by multinationals, there is little in the policy document itself to address the multinational nature of cybersecurity (the White House, 2013). The policy document stated the necessity for the U.S. government to engage international partners to secure critical infrastructure both within and outside the United States (the White House, 2013). However, the document placed great emphasis on the collective responsibility of these entities to protect the national interests of the United States instead. Obama made many references to the coordinated nature of any cyber defenses. Granted, these were all in reference to the coordination of the U.S. government and corporate partners, but it implicitly outlined an understanding of the necessity for a coordinated effort for cyber defenses.

In his 2013 executive order, President Obama sought to bring in "private sector subject-matter experts into Federal service on a temporary basis" (Obama, 2013). This was overtly for the purpose of help the federal government and the private sector to share cyber threat information; however, this process also has side effects other than information sharing. This measure, joined with other measures, puts at least some the burden of national security on private entities. This measure particularly makes private individuals responsible for public interests. In an area like cyber warfare where the lines between entities are already blurry due to the nature of cyberspace, measures like these make private

spaces—or rather civilian spaces—less distinct from the state. This could make a civilian target arguably a credible target during cyber warfare, further distancing cyber warfare from the purview of Just War doctrine.

Underneath all of the rhetoric of securitization, there were also overt references to values unrelated to cybersecurity. In his 2011 executive order, President Obama made several references to protecting privacy and civil liberties with the overt intent that the executive order would be consistent with legal protections of the day (Obama, 2011). President Obama even went as far as to create an oversight committee within the Department of Homeland Security in his 2013 executive order to monitor activities to protect the cybersecurity of national interests (Obama, 2013). In the 2014 presidential policy directive, the White House maintained that the U.S. government was obligated to treat others with dignity and respect during intelligence gathering, regardless of their nationality or place of residence (the White House, 2014). Additionally, the policy directive placed particular burdens upon the United States due to having a leadership role internationally in regard to upholding democratic principles and universal human rights (the White House, 2014). The policy directive went further to protect privacy and civil liberties, specifically stating that no intelligence gathering should take place in order to suppress or prevent dissent (the White House, 2014). Judging by their rhetoric, protecting civil liberties and privacy goes hand in hand for the Obama administration. It would be appropriate to say that the U.S. government positions itself as the protector of civil liberties both domestically and abroad. Under this frame, any state that has a position contrary to the position of the United States would be an affront to civil liberty.

In his 2013 executive order, President Obama wrote what the ideal kind of cyber environment would look like (Obama, 2013). The ideal cyber environment would encourage "efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties" (Obama, 2013). While this ideal cyber environment would be secure, the majority of the attributes listed have to do with things other than security. President Obama claimed in this executive order that an ideal cyber environment could be achieved through information sharing related to cybersecurity and creating risk-based standards collectively (Obama, 2013).

But who is the intended audience behind these policy reviews and executive orders? Because they are not press releases from an event with another foreign state or sent expressly to a foreign state, rather they are internal documents for the working of the national government, it is safe to assume that these documents are intended for domestic consumption. Therefore, when these documents make reference to what an ideal cyber environment would look like, it is likely that this ideal environment would be for American citizens. President Obama highlights these issues because they have salience in the American public, not necessarily because they have power with the broader world. This rhetoric is frequently deployed in order to create a coalition of forces that may not otherwise come together to work towards the particular interests of those in power. When this is compared to how the United States deployed rhetoric during the Cold War, this was very much the case. For example in the early 1950s, the Eisenhower administration deployed rhetoric emphasizing America's moral and spiritual authority in order to justify how the United States ought to engage with other states internationally (Medhurst, Ivie,

Wander, & Scott, 1997). This argument was able to portray particular actions as certainly good or certainly evil. By doing this the United States gave itself the moral high ground allowing for atrocities to happen during wartime, such as in the Vietnam War (Medhurst *et al.*, 1997). Similar positioning can be seen in these policy directives and executive orders.

In the 2014 presidential policy directive, the White House admitted to the necessity for intelligence gathering to protect and advance the national security and foreign policy interests of the United States (the White House, 2014). The White House admitted that this kind of necessary information gathering comes with great risk if it is discovered, including:

> "[U.S.] relationships with other nations, including the cooperation [they] receive from other nations on law enforcement, counterterrorism, and other issues; [U.S.] commercial, economic, and financial interests, including a potential loss of international trust in U.S. firms and the decreased willingness of other nations to participate in international data sharing, privacy, and regulatory regimes; the credibility of [U.S.] commitment to an open, interoperable, and secure global Internet; and the protection of intelligence sources and methods" (the White House, 2014).

The United States government identified *foreign intelligence* and *counterintelligence* as having different meanings within this policy directive. For the U.S. government, *foreign intelligence* means "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists" (the White House, 2014). Alternatively, *counterintelligence* refers to "information gathered and activities conducted to identify, deceive, exploit, disrupt, or

protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities" (the White House, 2014). While there seems to be a kind of definitional difference, the policy document further commented that both foreign intelligence and counterintelligence were understood as *intelligence* and could therefore be situated under the same guidelines of state necessity. When intelligence is understood within this framework, the envelope of intelligence gathering is rather broad. This does not seem to limit the acceptable practices of intelligence gathering in any significant fashion, driving intelligence gathering as necessary to national security.

CHAPTER 5: CHINA
A RISING SUPERPOWER

As previously stated, cyber warfare is shrouded in mystery due to its nature; Chinese cyber warfare efforts are doubly mysterious as the government rarely reports or allows its media to report on government action and events. Instead the government allows for the results of their policies and actions to be reported on. This makes any study into Chinese warfare difficult. Therefore, I will begin this case study by providing an overview of how the Chinese government portrays its own foreign policy, specifically in relation to security. Then I will present alleged examples of the Chinese engagement in cyber warfare. To finish, I will discuss how the actions of China align with what they say are their intentions for acting internationally.

Ethic of win-win relations

In all of their speeches and statements, Chinese officials constant reference their ideal goal for international relations, win-win situations for all parties involved. In his 2015 remarks at the United Nations, titled "Working together to forge a new partnership of win-win cooperation and create a community of shared future for mankind," President Xi referenced to the shared accomplishments of all humanity, starting with the creation of the United Nations as a "universal and most representative and authoritative international organization … [ushering] in a new era of cooperation" (Xi, 2015b). In these remarks, President Xi urged the world to come together to form new methods to achieve win-win

relations internationally. He relied heavily on the values of collective action, inclusivity, and respect and global peace to punctuate his talk and to promote the concept of win-win relations. President Xi saw collaborative security measures at the heart of win-win relations. President Xi claimed that in an unstable world, no state can truly be stable. Conflicts ought to be handled before they ever broke out into violence (Xi, 2015b).

Chinese officials repeatedly refer to their desire for a more open and free world trade. In his 2016 speech, Foreign Minister Wang Yi denounced any form a trade protectionism (Wang, 2016). The Chinese government sought to expand their trading potential as far as possible, seeing trade borders as a barrier to mutual gains between states. This could potentially explain China's loose interpretations of intellectual property and corporate espionage. In a 2011 speech, Ambassador Wang Qun addressed the vulnerability of cyber warfare specifically. Just like the United States, H.E. Wang highlighted the necessity for cybersecurity for national security reasons (Wang, 2011). Unlike the United States, H.E. Wang took this principle further, tethering the need for cybersecurity together with international security. This tied in with the Chinese government's broader emphasis on the value of collectivity.

However, the positions of Chinese government officials do not seem to be in sync in some regards. In his 2015 remarks, President Xi urged the world to turn its back on the Cold War mentality (Xi, 2015b). This would imply that something in the international order ought to change. But in his 2016 speech at the Center for Strategic and International Studies, Foreign Minister Wang staunchly supported the "international order and system established after the victory of the Second World War" (Wang, 2016). This would imply

that the Cold War style of international relations is exactly what the Chinese government would like to maintain.

International hacking

Unlike the case of the United States, China does not has not developed cyberweapons, such as Stuxnet, that go out to attack a target. Instead the Chinese have allegedly carried a number of international hacks against their opponents, namely the United States. Because these hacking operations are arguably just espionage attempts, it could be said that they are not really a part of cyber warfare. However, each example sets a precedent for how China has implemented the concepts of "indirect" and "unconstrained" warfare in the modern age.

Operation Aurora

Many high-profile companies, such as Google, Adobe, and dozens of others, were attacked by hackers attempting to gain access to source code (Zetter, 2010c). According to MacAfee (an anti-virus firm), the tactics used were unprecedented, combining encryption, stealth programming, and an unknown hole in Internet Explorer. Dmitri Alperovitch, the vice president of threat research for McAfee said:

> "We have never ever, outside of the defense industry, seen commercial industrial companies come under that level of sophisticated attack. It's totally changing the threat model" (Zetter, 2010c).

In January 2010, Google announced in a blog post that hackers stole intellectual property and tried to access the accounts of human rights activists (Zetter, 2010c). The international company discovered the intrusion in December 2009, quickly realizing it was more than a simple security breach (Zetter, 2010a). In response to their discovery, Google

"began a secret counteroffensive" against the hackers in December 2009. The company then accessed a computer in Taiwan suspected of being the source of the cyber-attack (Sanger & Markoff, 2010). On that computer, Google found that at least thirty-three other companies, such as Adobe Systems, Northrop Grumman, Juniper Networks, Rackspace, Symantec, Morgan Stanley, and Yahoo, were also attacked (Sanger & Markoff, 2010; Schwartz, 2013). Upon realizing the sheer scale of the cyber-attack, Google contacted Untied States intelligence and law enforcement to seek assistance (Sanger & Markoff, 2010).

Upon investigating at the time of the attack, Google was not able to fully determine the goals of the cyber-attacks. There are several possibilities: insert spyware, gain commercial advantage, or access accounts of Chinese dissidents and American experts on China (Sanger & Markoff, 2010). It could be one, or a mixture of all of these reasons. However, once it became apparent that other companies targeted by this attack were not going to go public, Google decided to go public in an effort to alert those potentially affected by the hack, namely the activist community (Zetter, 2010a). Shortly after Google's blog post, Adobe also announced that it had been attacked by a "sophisticated, coordinated attack against corporate network systems managed by Adobe and other companies," becoming aware of the intrusion in early January 2010 (Zetter, 2010c; Zetter, 2010a).

Neither Google nor Adobe were forthcoming about how the attacks occurred and it was unclear how precisely the malware got onto the corporate systems. However, the hole in Internet Explorer served as the key component of the attack after the initial piece of

malware got onto the system (Zetter, 2010c). The internet browser was exploited through a zero-day vulnerability to download other pieces of malware, unbeknownst to the users (Zetter, 2010c; Zetter, 2010b). A zero-day vulnerability is a software security flaw that does not have an existing patch (Zetter, 2010b). Hackers used almost a dozen pieces of malware and several layers of encryption to penetrate company networks and hide their activities. One of these pieces of malware opened a remote backdoor for hackers to exploit and gain entry to corporate systems (Zetter, 2010c). Some systems were breached through a malicious PDF e-mail attachment, exploiting a zero-day vulnerability in Adobe's Reader and Acrobat applications, to install a Trojan program called Trojan.Hydraq (Zetter, 2010c; Zetter, 2010b). This Trojan was used to compile user credentials and other data to get further inside a company's network (Zetter, 2010b).

McAfee dubbed the cyber-attacks "Operation Aurora," believing this is what the operatives called their mission (Zetter, 2010c). At least thirty-four companies in the technology, financial, chemical, media, and defense sectors were targeted in this operation (Zetter, 2010c; Zetter, 2010a). The diversity of modifications to the malware indicated that the attackers did not rely on only one technique to access these corporations. Rather the hackers used different files and different combinations to create a backdoor network (Symantec Security Response, 2010).

Google claimed the attack originated from China, but was more sophisticated than the company usually encountered (Zetter, 2010c; Zetter, 2010a). The degree of sophistication makes this attack unprecedented in the corporate world. Large companies are attacked daily, but Google engineers were unable to gain much concrete evidence

(Symantec Security Response, 2010; Sanger & Markoff, 2010). Google argued that the sophistication of the attacks strongly suggested that the cyber-attacks either came from Chinese government agencies or were approved by the Chinese government (Buchanan, 2010).

After the attack, there was great speculation as to why the Chinese government would want to hack into these corporations. It has been suggested that Operation Aurora was a counterespionage operation. Senior director of Microsoft's Institute for Advanced Technology, David Aucsmith said, "What we found was the attackers were actually looking for the accounts that we had lawful wiretap orders on," at a government IT conference in 2013 (Schwartz, 2013). With this information, Chinese espionage operatives could either evade detection or destroy incriminating information upon detection. Attacking corporations rather than the FBI makes sense if this were the case, as corporations tend to have less sophisticated anti-hacking tools at their disposal (Schwartz, 2013).

In response to these attacks, Google announced it would no longer censor search results in China (Zetter, 2010a). Google had been censoring its search results on Google.cn as a concession to the Chinese government in 2006; however, the company eventually left China later that year (Zetter, 2010a; Blodget, 2010). Google pulled out of the country, redirecting its Chinese site to Hong Kong (Blodget, 2010). While Google did not claim the attacks were behind the cyber-attacks, Google attributed this move to attempts by China to "further limit free speech on the web" (Zetter, 2010a).

What happened in this event? China allegedly attacked a company, based in a foreign country, partially to gain access information on its own citizens and partially to gain an understanding on the progress of U.S. counterespionage efforts. While this event does not necessarily feel like an act of war and it is uncertain if this would constitute an act of force legally, there are elements of this event that are similar to warfare. The allegedly Chinese cyber-attack on Google would have been understood as an act of war if phrased in a broader context: a foreign power attacked another power's interests or citizens. When understood in that broader context, it would seem reasonable to say that it was an act of war. However, China was able to escape repercussions unscathed, mostly due to plausible deniability. In turn, Chinese officials are able to come from the moral high ground when accused, making claims of American sentiments of superiority. The other piece, seeking information on U.S. counterespionage efforts, is another form of counterespionage which is not necessarily an act of war. That in and of itself stands as an act below war, but is certainly unfriendly.

How does this resemble a proxy war? Whereas in a proxy war, two great states fought inside developing countries, I would argue that this is a case of two great states fighting inside of corporations in a similar manner. This style of fighting would not have been possible in a previous age, because while a state could use corporate interests to leverage another state, a state could not infiltrate corporations in such a degree as to compromise state interests so completely. That is to say, China's alleged attacks on Google were able to compromise U.S. defenses in a manner previously unavailable. It could be argued that this is part and parcel to cyber warfare, but I would disagree. Cyber warfare

could be waged between government systems, leaving corporate systems largely alone. By that I mean a state would not have to directly attack a corporate information network in order to gain access to government details. However, by using a corporation—an entity that does not have the same funding or infrastructure at its disposal that a state does—as a medium to indirectly attack another state, China allegedly used Google functionally as a proxy state was used during the Cold War. Cyber warfare only introduced a new means, but the logic and method behind the attack remains similar to that of the Cold War mentality.

Attack on natural gas pipelines

From December 2011 through June 2012, cyberspies connected to China's military allegedly targeted twenty-three gas United States pipeline companies (Clayton, 2013; Peixe, 2013). During this period, information was allegedly stolen by hackers that could potentially damage U.S. gas pipelines. This attack was coordinated against key personnel in these companies, sending e-mails with malicious links or file attachments allowing hackers into the networks (Clayton, 2013). The sensitive operational and technical data stolen make this cyber-attack particularly pernicious, with the potential to sabotage the pipeline infrastructure. At the time, nearly 30% of the United States power grid relied on natural gas (Clayton, 2013; Peixe, 2013). With the data that were stolen, an aggressor had the potential to blow up compressor stations. This destruction could be coordinated simultaneously, essentially holding the infrastructure of the United States hostage (Clayton, 2013). A retired scientist from the Gas Technology institute, William Rush, said the following:

> "Anyone can blow up a gas pipeline with dynamite. But with this stolen information, if I wanted to blow up not one, but 1,000 compressor stations, I could. I could put the attack vectors in place, let them sit there for years, and set them all off at the same time. I don't have to worry about getting people physically in place to do the job, I just pull the trigger with one mouse click" (Peixe, 2013).

In this breach, several kinds of sensitive files were stolen that could give the perpetrator the ability to control over or to change the operation of the pipelines. Some of this data included usernames, passwords, personnel lists, system manuals, and pipeline control system access credentials. Reports on the incident called the data files a part of a "sophisticated attack shopping list" (Clayton, 2013). To find the relevant data files, the hackers installed custom malware onto the systems, searching for any computer files with the letters "SCAD." Just like in the case of Stuxnet, these files monitored and operated the pipeline network and other essential (Clayton, 2013). These are the same type of files that Stuxnet took advantage of to inflict damage upon the Iranian facility. This information would allow hackers to reset computer-controlled systems along the pipeline, build up extreme pressures thereby causing explosions, or valve failures within the pipeline network (Peixe, 2013). By gaining access to these particular data files, it is clear that hackers were able to penetrate the computer systems of these pipeline companies rather deeply (Clayton, 2013).

Just like the case of Stuxnet, all indicators pointed to a team of educated, motivated, and well-funded designers behind the hack. This team clearly had specific purposes in mind for the cyber-attack (Clayton, 2013). The restricted report (titled Active Cyber Campaigns Against the U.S. Energy Sector) from the Department of Homeland Security

(DHS) documenting the cyber campaign did not mention the Chinese government in particular (Clayton, 2013; Gilbert, 2013). However, a preeminent and independent cybersecurity firm based near Washington D.C., called Mandiant, published a report in February 2013 that traced hacks of 141 companies around the globe to "Unit 61398" (Clayton, 2013; Gilbert, 2013). These hacks all occurred over a seven-year period (Gilbert, 2013). Unit 61398 worked out of a building in Shanghai, having strong ties to China's People's Liberation Army (Clayton, 2013; Gilbert, 2013). This group of hackers are known as some of the most sophisticated of the Chinese hacking groups (Sanger, Barboza, & Perlroth, 2013). They are known to many of their victims in the United States as the "Comment Crew" or "Shanghai Group" (Sanger *et al.*, 2013). Kevin Mandia, the founder and chief executive of Mandiant, said this about the group:

> "Either they are coming from inside Unit 61398 or the people who run the most-controlled, most-monitored Internet networks in the world are clueless about thousands of people generating attacks from this one neighborhood" (Sanger *et al.*, 2013).

Other security firms go so far as to suggest that the hacking group is state sponsored. In 2013 a classified National Intelligence Estimate, issued as a consensus document of all sixteen of the United States intelligence agencies, made a strong case that many of these hacking groups are either operated by army officers or are contractors working for the government (Sanger *et al.*, 2013).

The indicators of compromise (IOCs), or rather the online data signatures that indicate a person or place of origin, of those breaches were found to be the same as those involved in the pipeline attacks (Clayton, 2013). This strongly signals Chinese

involvement in the attacks on pipeline systems. China rejected any accusation of these cyber-attacks linked to its military. Geng Shuang, the spokesman at the Chinese Embassy in Washington D.C., wrote the following in an e-mailed statement to the Monitor:

> "Cyber-attacks are transnational and anonymous. Determining their origins is extremely difficult. We don't know how the evidence in this so-called report can be tenable. Chinese laws prohibit cyber-attacks and China has done what it can to combat such activities in accordance with Chinese laws and regulations" (Clayton, 2013).

The research director for the United States Cyber Consequences Unit, John Bumgarner, emphasized how natural gas pipelines are essential to national security in the United States (Clayton, 2013). In the restricted Department of Homeland Security report, a company, Telvent Canada, was among those hacked. This company not only has a significant role in the oil and gas industry, but also has a key role in the "smart grid" currently under development. This "smart grid," intending to coordinate energy distribution more efficiently, allows for both old and new software to work in concert with one another, communicating and controlling critical systems alongside each other. If the source code of these important and developing control-system technologies were captured, it would allow hackers to easily develop powerful and sophisticated cyberweapons—such as Stuxnet (Clayton, 2013). The Chinese government continued to deny all U.S. allegations of cyber espionage, maintaining that sustained allegations were "unprofessional" (Gilbert, 2013; Sanger *et al.*, 2013).

This event highlights much the same fears that Stuxnet highlighted previously. In this case, there was no damage to systems, but there was very deep infiltration into a network of facilities that have a high national security priority to the United States, China's

main competitor. Because there was no damage actually done to the network, it would be easy to say that this event is markedly distinct from Stuxnet. However, the perpetrators certainly had the means and the capability to accomplish much the same ends as Stuxnet in this case, they simply decided to not exercise that ability. If the perpetrators had decided to act in this case, lives would have been certainly lost as a result.

However, this case brings to mind another aspect of the Cold War: the Cuban Missile Crisis. During this event, it was not the act of firing a nuclear weapon that was abhorrent. It was the functional ability to fire one upon the United States with little to no effort or time for response. Functionally, the Chinese were allegedly in the same position. They allegedly had the functional ability to cripple the United States irreparably. Therefore, it would seem justifiable for this to be intolerable in a similar fashion. During the Cuban Missile Crisis, such an intolerable position would have been seen as a credible threat justifying a military response. This event calls into question if the same would follow during cyber warfare. Would the United States have been justified in responding militarily to such an intolerable threat? Because it never happened, this is all conjecture. However, the parallels are striking.

F-35 strike fighter theft

In June 2013 at a Senate subcommittee hearing, defense acquisitions chief Frank Kendall claimed he was reasonably confident that all classified information of and relating to the development of the F-35 jet remained protected. Kendall admitted that unclassified information on hacked, contractor networks may not have been as well-protected (Alexander, 2013; Freedburg, 2013). Kendall was primarily concerned with maintaining

the secrecy of the design and production of the fighters. If those particular aspects of the program had been compromised, then the United States and her allies would lose a substantial advantage over her competitors (Alexander, 2013). The "fifth-generation" aircraft is meant to be able to evade radar and integrated air defense systems. The F-35 is the most expensive weapons program in United States history. The United States is collaborating with eight international partners, intending to purchase 2,450 of the aircraft upon the completion of development. Such an arsenal would cost the United States almost $400 billion (Alexander, 2013). This admission in 2013 was not news to those who had been paying close attention. Six years previously, BAE systems (a F-35 subcontractor) was hacked by a mysterious party (Freedburg, 2013). United States officials claimed that no classified information was stolen in 2009; however, in 2011 China announced its intentions to build a fifth-generation stealth fighter of its own with similar capabilities of the F-35. In 2012, the J-31 was capable of flight (Weisgerber, 2015).

Kendall's remarks came only a month after the Pentagon released its annual China report (Alexander, 2013). In this report, the Pentagon claimed that China was using cyber espionage to acquire and advance her military technologies, within her already fast-paced military modernization program. This was the first report that directly charged the Chinese government and military with cyber intrusions into United States government and computer systems (Alexander, 2013). While both China and Russia have both skilled hackers and their own fifth-generation stealth jet fighter programs, the Chinese were considered the more viable hacker. China's program appears to be strikingly similar to the

United States' program, whereas the Russians were not accused of such direct copying (Freedburg, 2013).

It has been said that the security breach saved China "twenty-five years of research and development" (RT.com, 2015). It's been speculated that approximately fifty terabytes (the equivalent of five Libraries of Congress) was stolen, an estimate much higher than the original "several terabytes" estimated (RT.com, 2015). The data stolen included engine schematics and radar designs, along with files that would make it easier to not only manufacture advanced weaponry but also design counter-measures to their opponents' weaponry (RT.com, 2015; Freedburg, 2013).

In 2016, the United States sentenced Chinese national Su Bin for being a part of the hacking of United States military secrets. The 51-year-old businessman was captured in Canada in 2014 and extradited to the United States (PressTV.ir, 2016). Su plead guilty for his involvement in the scheme (Gertz, 2016). For his involvement in the scheme, Su was sentenced to four years in federal prison and fined $10,000 (PressTV.ir, 2016). This marked the first successful prosecution of a Chinese hacker for stealing defense secrets (Gertz, 2016).

The 2014 indictment alleged that Su used his China-based aviation company as a cover to assist two unidentified, Chinese co-conspirators to access defense secrets (PressTV.ir, 2016). Between 2009 and 2013, the co-conspirators hacked into Boeing's computer systems and the networks of other defense contractors in both the United States and Europe (Bender, 2014). While the theft of data relating to the F-35 and the F-22, both fifth-generation jet fighter programs, was by far the most intrusive, Su and his co-

conspirators allegedly stole from thirty-two different United States projects. It is believed by the United States government that this small team attempted to sell the stolen data files to Chinese state-owned companies. Su wrote in an email to his alleged co-conspirators the goal to help China "stand easily on the giant's shoulder's" (Bender, 2014).

New technical specifications about China's own fifth-generation jet fighter program, the J-31, was released on a Chinese blog in September 2015 (Weisgerber, 2015). The J-31 is being designed as a rival to the F-35 Joint Strike Fighter, but both seem to be strikingly similar in appearance. Military experts claim that while the two fighters look similar, the F-35 has better computer software and defense technology hardware. However senior Pentagon officials see indicators that the superiority of United States' defensive technology is shrinking. It is becoming increasingly unclear that the military capabilities of the United States will remain unmatched, unlike previous decades. In 2007, the Pentagon attempted to urge defense companies to better protect their networks. While United States' defense companies have been trying to shore up their cybersecurity, there's been a gap in security talent. Some private cybersecurity companies suggested in 2015 that as much as 90% of defense companies in the United States were not equipped to deal with cyber espionage (Weisgerber, 2015).

Beijing repeatedly denied all accusations that they perpetrated any sort of cyber-attack against United States' military resources (RT.com, 2015; PressTV.ir, 2016). Their Foreign Ministry spokesman, Hong Lei, told reporters:

> "The so-called evidence that has been used to launch groundless accusations against China is completely unjustified … According to the materials presented by the

> relevant person, come countries themselves have disgraceful records on cyber security" (RT.com, 2015).

That being said, the Chinese media has heralded Su Bin as a hero to the Chinese people (PressTV.ir, 2016). The Chinese newspaper *Global Times* wrote:

> "We have no reliable source to identify whether Su has stolen these secrets and transferred them to the Chinese government. If he has, we are willing to show our gratitude and respect to his service to our country. On the secret battlefield without gunpowder, China needs special agents to gather secrets from the US. As for Su, be he recruited by the Chinese government or driven by economic benefits, we should give him credit for what he is doing for the country" (Global Times, 2016).

This is a case where military espionage was used to stay in the same league as an opponent. This phenomenon is not a new one, or even all that surprising. This was common not only during the Cold War, but also throughout the rest of military history. If a state cannot understand the technology their opponent is using against them, then it cannot defend against it. What makes cyberespionage distinct from other forms of espionage is that the lines between cyberespionage and cyber warfare are less well-defined. In previous forms of warfare, espionage largely dealt with gathering intelligence related to troop movements, military technological innovations, and tactical plans. Rarely if ever did this kind of intelligence gathering allow an opponent to have any kind of control over a military operation or government system. This kind of espionage simply did not help an opponent gain access to the mechanisms necessary to gain that sort of control; however, sabotage was possible in some cases. Yet all of these techniques required great personal risk from the saboteurs and spies. There were norms developed over what would constitute a reasonable, proportional response to espionage.

With cyberespionage, the physical risk can be negligible or nonexistent to cyberspies. Additionally, there is much more to gain from cyberespionage. In successful cyberespionage operations, it is possible to gain all of the same kind of intelligence as with previous forms of espionage. They can also get access to greater degrees of information once a system is successfully infiltrated and can even gain control of parts of that system. In order to gain access to particular files, such as the files related to the F-35 strike fighter, a cyberspy must have penetrated secure systems deeply. These deep system invasions have greater potential damage to the greater system than conventional espionage operations. This makes reacting to a cyberespionage attack particularly precarious. If there is potential to greatly damage or takeover a system, a state would want to be allowed to significantly discourage this kind of aggressive action. This would imply that a strong reaction would be desired. But in a true cyberespionage attack, no real damage has occurred and only information has been taken. This makes a large response seem unjustified, but any other kind of response might not be taken seriously. In the case of the F-35 strike fighter theft, years of expensive development and technological innovations were high jacked by the Chinese, but without proof that the Chinese government was directly involved, there is little the United States can do reasonably do in response. There is no clear proportional response with cyberespionage. What is clear is that China sees cyberspace as a battlefield and that it is at war with the United States upon that battlefield. This particular case is important to understand because it serves as an unequivocal example of cyberespionage being a key part of the Chinese cyber warfare strategy.

Attack on GitHub

In March 2015, a popular coding site called GitHub, based out of San Francisco, CA, was attacked (Stone, 2015; Dou, 2015). GitHub was the world's biggest host of open-source projects (Goodin, 2015). GitHub is very popular in China, as the website itself is encrypted, allowing the sensitive content it links to work around the barriers in place on the Chinese Internet (Cendrowski, 2015). The entire GitHub site itself was blocked by Chinese censors in 2013, but Chinese coders dissented its brief absence (Cendrowski, 2015). The 2015 attack appeared to be targeted at two GitHub projects in particular, GreatFire and CN-NYTimes, both aimed at subverting Chinese government Internet censorship (Stone, 2015). GreatFire is an organization that develops and reports on methods to work around the Great Firewall (Hern, 2015). The New York Times' Chinese mirror, CN-NYTimes, tries to give Chinese citizens access to the newspaper, even when the website is blocked by Chinese censors (Hern, 2015).

The attack itself was a DDoS attack, evolving as GitHub tried to update its defenses (Stone, 2015). This was accomplished by inserting a malicious strain of JavaScript into millions of users' Internet browsers when they visited a China's most popular search engine, Baidu (Stone, 2015; Dou, 2015). When users would visit Baidu, their browser would submit a request to both anticensorship programs (Stone, 2015). While Baidu is the largest search engine within China, the attackers only used web traffic from users overseas, making it harder for GitHub to defend against the attack (Dou, 2015). The GitHub sites were so overwhelmed with online requests, that the websites were knocked offline (Stone, 2015). This new offensive system has been called the "Great Cannon" (Temperton, 2015).

Researchers from the University of Toronto, University of California-Berkley, the International Computer Science Institute, and Princeton University had startling claims over the capabilities of the Great Cannon (Temperton, 2015). They suggested that China could not only intercept any foreign web traffic coming in and out of Chinese websites, but also plug in malicious code into that traffic, and use it to attack the Internet more broadly. The researchers also suggested that this cyberweapon could be altered to attack particular users rather than a particular website. If this were the case, this would mean that anyone hosting a website in China or running Chinese advertising or analytics code could be targeted with this system. In addition, there is a possible "man-in-the-middle" configuration. This would entail "intercepting unencrypted emails a targeted IP address, replacing legitimate attachments with malicious ones" (Temperton, 2015). This possibility was particularly troubling for researchers, representing a "potent cyber-attack capability." Researchers noted that:

> "The operational development of the Great Cannon represents a significant escalation in state-level information control: the normalization of widespread use of an attack tool to enforce censorship by weaponising users" (Temperton, 2015).

The outages GitHub experienced demonstrated that the Internet—intended to be decentralized—relies heavily on key pieces of Internet infrastructure (Hern, 2015).

It was alleged that the Chinese government was responsible for the attacks on GitHub, but the Chinese government denied any involvement in the attack on GitHub (Stone, 2015). Baidu claimed it not only had no involvement in the attack, but also its systems were not infiltrated after conducting an internal inspection (Dou, 2015). Initial

reports showed a link between the Great Cannon and the Great Firewall, China's Internet filter (Temperton, 2015). A lead cybersecurity researcher, Mikko Hyponen, said that the attacker "had to be someone who had the ability to tamper with all the Internet traffic coming into mainland China" (Stone, 2015). There were technical details linking the attack to the Chinese, most notably the malicious code traced to China Unicom, the same telecom company caught aiding the Great Firewall previously (Goodin, 2015). It was found that the machine that attacked GitHub was located either near or on the Great Firewall, strongly implicating the Chinese government. During the same week this evidence was uncovered, both Google and Mozilla made it clear that their web browsers would no longer trust digital certificates issued by the China Internet Network Information Center (Goodin, 2015).

The attack on GitHub came on the heels of Beijing blocking many virtual private networks, a popular tool for Chinese citizens to work around Chinese censorship and gain access to an unfiltered view of the Internet (Stone, 2015; Dou, 2015). Additionally, a 2015 document from China's People's Liberation Army acknowledged the existence of hacker grounds within the PLA (Cendrowski, 2015). One researcher, Bill Marczak, found the brazenness of the attack particularly striking. Marczak stated that "[the attack on GitHub] was a very public demonstration of the capability" of the Great Cannon, adding that it was likely that China wanted people to know they had such capabilities (Weissman, 2015).

In a way, the Great Cannon serves the same purpose as a nuclear weapon. When the nuclear bomb was deployed in World War II, only one state—the United States—had the capability to use it. The Great Firewall allows China to weaponize its Internet traffic in a manner unlike any other state. It is uncertain and unclear how other states can go about

either attacking in this manner or defending from a weapon like the Great Cannon. For this reason, this method of attack has the potential to be used as an Internet deterrent, but it remains unclear how a state can threaten its use without providing a demonstration of force, such as the one China displayed in this case. Unlike a nuclear weapon where just physically having one serves as a deterrent, this weapon would have to be used in order to show a state has the capability to use it. This would imply that a state would need to use it in an unreasonable or disproportionate fashion, in order to use it as a threat later. This would go against international laws as they stand.

CHAPTER 6: SIGNIFICANCE

The confusion and anxiety in international relations stemming from cyber warfare is dramatic. Since the term's introduction, policy makers the world over have shifted increasing weight and concern towards cyber warfare. However, it seems that much of this anxiety comes with new technological and sudden technological advancements regardless of it being in cyber warfare or not. More studies would have to be conducted in order to compare all of these trends, but this paper has focused on comparing the emergence of cyber warfare to the emergence of nuclear weaponry and the conflicts of the Cold War. This paper suggests that the mentality and ethics of the Cold War has largely not been lost, rather it has shifted to the new domain of cyberspace.

Both the United States and China draw heavily upon values in their rhetoric surrounding cybersecurity. As previously stated, this rhetoric is often directed to a domestic audience in order to rally support for their nation's cause. But these values, particularly those portrayed by the United States, are incredibly polarizing. The delineate what is good and evil action in international relations, necessarily setting those that act contrary to the perceived "good" action as "evil." During the Cold War, it was the United States versus the Soviet Union. These two actors spoke of having such different values and different approaches to life, but as time goes by it has become more and more clear that both the United States and the Soviet Union acted in similar fashions regardless. Both

the United States and China have overarching themes in their foreign policy unrelated to security. For the United States, there seems to be a concern for individual rights, civil liberties, and universal human rights. For China, there is an emphasis on collective development and win-win relations between states. While not mutually exclusive, these two schemas of rhetoric often run contrary to one another. By focusing on individual rights over collective development, the United States can accuse China of not protecting its people. By focusing on win-win relations over universal human rights, China can accuse the United States of impeding the progress of developing nations around the world by holding developing nations to unreasonable expectations. In both arguments, there is a "good" side and an "evil" side. But both the United States and China are acting in similar manners, placing the importance of security over the concerns of their rhetoric.

In the case of the United States, Stuxnet demonstrated that even in situations that have strong evidence that a state carried out a cyber-attack against an opponent, there is little that the international community can do in response. Without direct evidence to accuse a state of conducting cyber-operations, a state can successfully attack another state without garnering any repercussions from the international community. The manner that the United States acted in this case is much as it did during the Cold War, so it would seem reasonable to apply the same ethical norms on cases like this one. However, these norms were largely based on Just War theory, specifically the idea of proportionality. Stuxnet undermines proportionality because Iran could not simply unlease Stuxnet on the United States as a reasonable response. At least at the time, Iran was not capable of such a feat. It did not understand how Stuxnet functioned nor had personnel with sufficient knowledge

to carry out such an operation. In such as situation, the only means Iran had access to were conventional, but there is no clear answer for what Iran should have attacked in this case. In conventional warfare, if a state such as the U.S. were to attack and destroy a facility, a reasonable response would be for a state such as Iran to attack and destroy something of similar strategic value.

In the case of China, the attack on the natural gas pipelines and the theft of F-35 strike fighter innovations raised many of the same questions as Stuxnet. The main difference between these cases is that the attack on the natural gas pipelines and the theft of F-35 designs did not result in any perceivable damage to the system whereas the Stuxnet attack did. In many regards, this makes the question of proportionality even that much more difficult in these cases. Because there was no perceivable damage and espionage is not usually a cause for proportional retaliation, the case of the F-35 strike fighter theft is particularly troubling. As stated previously, the hackers had to have deeply breached the security apparatus of the United States in order to access all of the files necessary to create their own strike fighter. This would seem to be cause for some kind of proportional retaliation, but it is unclear what kind of retaliation would be reasonable in this case. A state cannot proportionally react to actions that were possible due to the infiltration if those actions were never taken. Because there was no perceivable damage and the targets were not overtly military or defensive in nature, it is arguable if any form of retaliation is reasonable in the first place. Unless rules and norms surrounding proportional responses to cyber-attacks are developed, the troubles often associated with proxy wars and other forms of Cold War engagements may enter modern military strategies unchecked.

The implications of the other Chinese actions are slightly more varied. Where Stuxnet demonstrated the possibility of modern engagements similar to proxy wars between states, China has demonstrated how to use international corporations as a means for modern engagements similar to proxy wars. Operation Aurora used international corporations as a means to access security information of the United States. In doing so, China is redefining and blurring the lines between civilian and military targets. If these trends were to continue, then much of the progress made in the past century regarding humanitarian law during conflict could either develop loopholes or could be overwritten. If this were to occur, this would be a regression for human rights. Much of these humanitarian measures are based on Just War theory principles and while Just War theory is problematic during cyber warfare, Just War theory has done much to better manage the humanitarian consequences of conflict.

As previously stated, much of international law does not seem applicable to cyber warfare. There are significant problems with attribution and proportionality in cyber warfare, as demonstrated in the cases of the United States and China. This is one of the main reasons that both academics and state officials are so weary of cyber warfare. The last time a new technological weapon (nuclear weapons) came on to the international scene, norms formed and restrictive legislation followed. The norm that carried the day was deterrence. What makes cyber warfare so troubling in international relations today is that deterrence, which has been a tried and true source of stability among developed nations, is fundamentally based on the rule of proportionality. A state can respond to an attack in a reasonable fashion, rather than rapidly escalate the conflict, by following the principles of

proportionality. Additionally, deterrence requires there to be a credible threat. While it is still unclear what precisely would constitute a credible threat in cyber warfare, the Great Cannon is a definite possibility of a credible threat in cyber warfare. It is a cyberweapon that can be used multiple times and to which there is little to no defenses to such an attack. However as things stand, there are no clear rules of deterrence and engagement and the United States and China seem to be reverting back to old Cold War frames of action.

Because of the constraints of this research paper, it would have been very difficult to examine how several recent developments will effect or have effected cyber warfare. There are two recent developments in particular which could warrant research in the future: the U.S.-China Cyber Agreement (signed in September 2015) and the Presidential Policy Directive – United States Cyber Incident Coordination (released in July 2016). Regarding the U.S.-China agreement, it is simply too soon to judge if the agreement has been effective in curtailing cyber-operations going on between each state. Due to the secretive nature of cyber warfare, the public generally learns about cyber-operations with a significant lag time. This would mean that more time is necessary to find out if this agreement had any effect. As for the 2016 presidential policy directive, it opens a window into the perspective of the White House. However, it was released towards the end of research. It would be difficult to say the direction it would be trending for similar reasons it would be difficult to analyze the U.S.-China agreement.

These documents and others like them should be looked at in future research. I believe that it is important to continue to pursue this kind of research as cyber warfare evolves. Another case study that would give insight into cyber warfare is Russia. To

investigate a third case would have been too much for the confines of this research, but Russia is the third major actor in cyber warfare as it currently stands. Without looking at the actions and rhetoric of Russia, this research can only provide an incomplete picture of cyber warfare. While this is a weakness of this research, it is an opportunity for future investigations. It is possible that future research could resolve many of the issues surrounding proportionality and attribution that were brought up by this paper. It seems clear is that new ethical norms must be established in order to not revert back towards old models of warfare, adapted to new technologies. As the world becomes increasingly connected via the Internet, the world becomes more at risk to cyber-attacks. States would be able to engage in conflict more frequently and with greater reach in this new era, making the need for new norms of proportionality and attribution essential in the modern information age.

GLOSSARY OF TERMS

BIOS	Basic system necessary to startup a computer
Botnet	Network of computers that become slaves to a hacker
Conventional warfare	Warfare waged through kinetic means; warfare engaged outside of cyber warfare
Cyber warfare	Warfare waged over electronic information and communication technologies
Cyber attack	Attack via virtual means
Cyberweapon	Virtual weapon
Digital information system	Computers and computer systems
Hacker	Person who illicitly invades computer systems or goes beyond their level of clearance on a system in order to gain access to that computer system
Malware	Malicious piece of software
Nonlethal	Not intended to kill its target
Operating System	System that allows a computer to function
Self-replicating	Attribute of a program where is can duplicate itself
Trojan (horse)	Malware that is either hard to detect or does no perceivable harm
Virus	Malware that travels by attaching itself to
Worm	Malware that is a standalone program
Zero-day vulnerability	Previously unknown weakness in the security of a computer program or operating system, that allows for zero response time to a threat

RESOURCES

Alexander, D. (2013, June 19). Theft of F-35 design data is helping U.S. adversaries - Pentagon. *Reuters*. Retrieved from http://www.reuters.com/article/usa-fighter-hacking-idUSL2N0EV0T320130619

Asia Cooperation Dialogue. (2016). About ACD. Retrieved from http://www.acd-dialogue.org/about-acd.html

BBC. (2012, January 10). United States of America timeline. Retrieved from http://news.bbc.co.uk/2/hi/americas/country_profiles/1230058.stm

BBC. (2016, January 21). China profile - timeline. Retrieved from http://www.bbc.com/news/world-asia-pacific-13017882

Bender, J. (2014, July 16). FBI: A Chinese hacker stole massive amounts of intel on 32 US military projects. *Business Insider*. Retrieved from http://www.businessinsider.com/chinese-hackers-stole-f-35-data-2014-7?IR=T

Blodget, H. (2010, May 23). China surprisingly rattled by Google's clever pullout. *The Huffington* Post. Retrieved from http://www.huffingtonpost.com/henry-blodget/china-surprisingly-rattle_b_509428.html

Bowers, S. R., & Mielnik, P. A. (1998). Making warfare acceptable: Nonlethal strategies. *The Journal of Social, Political, and Economic Studies*, *23*(1), 17–32.

Brenner, S. W. (2007). "At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare. *Journal of Criminal Law & Criminology*, *97*(2), 379–475.

Broad, W. J., Markoff, J., & Sanger, D. E. (2011, January 15). Israeli test on worm called crucial in Iran nuclear delay. *The New York Times*. Retrieved from http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

Brownlee, L. (2015, September 25). New report of malicious Chinese cyber attack on a U.S. government agency. *Forbes Magazine*. Retrieved from http://www.forbes.com/sites/lisabrownlee/2015/09/25/new-report-of-malicious-chinese-cyber-attack-on-a-u-s-government-agency/#acac1fa309bf

Buchanan, M. (2010, January 15). Google hacked the Chinese hackers right back. Retrieved from http://gizmodo.com/5449037/google-hacked-the-chinese-hackers-right-back

CCTV.com. (2015, July 2). China to UN: Cyber security is multi-party responsibility. *CCTV.com English*. Retrieved from http://english.cntv.cn/2015/07/02/VIDE1435837809198235.shtml

Cendrowski, S. (2015, March 30). China pursues cyberpolitics by other means again with Github attack. *Fortune Magazine*. Retrieved from http://fortune.com/2015/03/30/china-pursues-cyberpolitics-by-other-means-again-with-github-attack/

Central Intelligence Agency. (2016, July). The World Factbook: China. Retrieved from https://www.cia.gov/library/publications/the-world-factbook/geos/ch.html

CivilRights.org. (2016). Tribal Sovereignty. Retrieved from http://www.civilrights.org/indigenous/tribal-sovereignty/?referrer=https%3A%2F%2Fwww.google.ie%2F

Clayton, M. (2010, November 30). Stuxnet: Ahmadinejad admits cyberweapon hit Iran nuclear program. *The Christian Science Monitor*. Retrieved from http://www.csmonitor.com/USA/2010/1130/Stuxnet-Ahmadinejad-admits-cyberweapon-hit-Iran-nuclear-program

Clayton, M. (2013, February 27). Exclusive: Cyberattack leaves natural gas pipelines vulnerable to sabotage. *The Christian Science Monitor*. Retrieved from http://www.csmonitor.com/Environment/2013/0227/Exclusive-Cyberattack-leaves-natural-gas-pipelines-vulnerable-to-sabotage

Coppernoll, M.-A. (1999). The nonlethal weapons debate. *Naval War College Review*, *52*(2), 112.

Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches*. Los Angeles: Sage.

Crowcroft, O. (2016, May 09). How China is winning its war against internet freedom. International Business Times. Retrieved from http://www.ibtimes.co.uk/behind-great-firewall-china-winning-its-war-against-internet-freedom-1558550

Davenport, K. (2016, July). Biological Weapons Convention signatories and states-parties: Fact sheets & briefs. Retrieved from https://www.armscontrol.org/factsheets/bwcsig

Delpech, T. (2012). Space and Cyberdeterrence. In *Nuclear Deterrence in the 21st Century* (pp. 141–158). RAND Corporation. Retrieved from http://www.jstor.org/stable/10.7249/mg1103rc.11

Dipert, R. R. (2010). The Ethics of Cyberwarfare. *Journal of Military Ethics*, *9*(4), 384–410. http://doi.org/10.1080/15027570.2010.536404

Dombrowski, P., & Demchak, C. C. (2014). Cyber war, cybered conflict, and the maritime domain. *Naval War College Review*, *67*(2), 70.

Dou, E. (2015, March 29). U.S. coding website GitHub hit with cyberattack. *The Wall Street Journal*. Retrieved from http://www.wsj.com/articles/u-s-coding-website-github-hit-with-cyberattack-1427638940

Dunham, J. (2016, April). *Press Freedom in 2015: The battle for the dominant message* (Rep.). Retrieved https://freedomhouse.org/report/freedom-press/freedom-press-2016

Economist. (2010, September 30). A worm in the centrifuge. *The Economist*. Retrieved from http://www.economist.com/node/17147818

Everts, S. (2015a, February 09). When chemicals became weapons of war. Retrieved from http://chemicalweapons.cenmag.org/when-chemicals-became-weapons-of-war/

Everts, S. (2015b, Spring). A brief history of chemical war. Retrieved from https://www.chemheritage.org/distillations/article/brief-history-chemical-war

Falcone, R., & Miller-Osborn, J. (2015, September 23). Chinese Actors use '3102' malware in attacks on US government and EU media (Rep.). Retrieved

http://researchcenter.paloaltonetworks.com/2015/09/chinese-actors-use-3102-malware-in-attacks-on-us-government-and-eu-media/

Falcone, R., Grunzweig, J., Miller-Osborn, J., & Olson, R. (2015, June 16). Operation Lotus Blossom (Rep.). Retrieved https://www.paloaltonetworks.com/resources/research/unit42-operation-lotus-blossom.html

Flyvbjerg, B. (2006). Five Misunderstandings About Case-Study Research. In P. Atkinson, & S. Delmont (Eds). *SAGE Qualitative Research Methods.* (Vol. 12, pp. 220-1). Thousand Oaks, CA: SAGE Publications, Inc. Retrieved from http://srmo.sagepub.com.mutex.gmu.edu/view/sage-qualitative-research-methods/SAGE.xml

Freedburg, S. J., Jr. (2013, June 20). Top official admits F-35 stealth fighter secrets stolen. Retrieved from http://breakingdefense.com/2013/06/top-official-admits-f-35-stealth-fighter-secrets-stolen/

Gertz, B. (2016, March 24). China hacked F-22, F-35 stealth jet secrets. *The Washington Free Beacon*. Retrieved from http://freebeacon.com/national-security/china-hacked-f22-f35-jet-secrets/

Gibson, T. (2015, December 17). 2015 a pivotal year for China's cyber armies. Retrieved from http://thediplomat.com/2015/12/2015-a-pivotal-year-for-chinas-cyber-armies/

Gilbert, D. (2013, March 01). Chinese hackers target US gas pipelines in die hard-style attack. *The International Business Times*. Retrieved from http://www.ibtimes.co.uk/energy-infrastructure-targeted-chinese-hackers-441095

Gilbert, S. G. (2014, June 9). Chemical weapons. In *Toxipedia*. Retrieved from http://www.toxipedia.org/display/toxipedia/Chemical+Weapons

Global Times. (2016, March 24). Su Bin deserves respect whether guilty or innocent. Retrieved from http://www.globaltimes.cn/content/975876.shtml

Goldberg, J. (2016, April). The Obama Doctrine. *The Atlantic*. Retrieved from http://www.theatlantic.com/magazine/archive/2016/04/the-obama-doctrine/471525/

Goodin, D. (2015, April 02). DDoS attacks that crippled GitHub linked to Great Firewall of China. *Ars Technica*. Retrieved from http://arstechnica.com/security/2015/04/ddos-attacks-that-crippled-github-linked-to-great-firewall-of-china/

Guyatt, D. (1997, December). Killing me softly. Retrieved July 12, 2016, from http://www.deepblacklies.co.uk/killing_me_softly_pr.htm

Hern, A. (2015, March 30). GitHub cleans up after cyber-attack. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2015/mar/30/github-cleans-up-cyber-attack

Huhtinen, A.-M. (2015). The Double Edge of the Information Sword. *International Journal of Cyber Warfare and Terrorism*, *5*(2), 21–30. http://doi.org/10.4018/IJCWT.2015040102

Hurley, J. S., McGibbon, H. M., & Everetts, R. (2014). Cyber Readiness: Are We There Yet? *International Journal of Cyber Warfare and Terrorism*, *4*(3), 11–26. http://doi.org/10.4018/ijcwt.2014070102

InsideGov.com. (2016a). 2014 United States budget. Retrieved from http://federal-budget.insidegov.com/l/117/2014

InsideGov.com. (2016b). 2015 United States budget. Retrieved from http://federal-budget.insidegov.com/l/118/2015

InsideGov.com. (2016c). 2016 United States budget estimate. Retrieved from http://federal-budget.insidegov.com/l/119/2016-Estimate

Janczewski, L., & Colarik, A. M. (2008). *Cyber warfare and cyber terrorism*. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.670.9033&rep=rep1&type=pdf

Kelley, M. B. (2013, November 20). The Stuxnet attack on Iran's nuclear plant was 'far more dangerous' than previously thought. *Business Insider*. Retrieved from http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11?IR=T

Krotofil, M. (2014). Cyber Can Kill and Destroy Too: Blurring Borders Between Conventional and Cyber Warfare. *International Journal of Cyber Warfare and Terrorism*, *4*(3), 27–42. http://doi.org/10.4018/ijcwt.2014070103

Kushner, D. (2013, February 26). The real story of Stuxnet. *IEEE Spectrum*. Retrieved from http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

Kutsch, T. (2013, August 28). Timeline: A recent history of US interventions. *Al Jazeera America*. Retrieved from http://america.aljazeera.com/articles/2013/8/28/timeline-a-recenthistoryofusinterventions.html

Lawrence, S. V., & Martin, M. F. (2013). Understanding China's Political System (Rep.). Congressional Research Service.

Lewer, N. (1999). Nonlethal weapons. *Forum for Applied Research and Public Policy*, *14*(2), 39–45.

McDowell, M. (2013, February 6). Security tip (ST04-015): Understanding denial-of-service attacks. Retrieved from https://www.us-cert.gov/ncas/tips/ST04-015

Medhurst, M., Ivie, R., Wander, P., & Scott, R. (1997). Cold War Rhetoric: Strategy, Metaphor, and Ideology. Michigan State University Press. Retrieved from http://www.jstor.org/stable/10.14321/j.ctt7zt8nn

Mezher, T., El Khatib, S., & Sooriyaarachchi, T. M. (2015). Cyberattacks on Critical Infrastructure and Potential Sustainable Development Impacts. *International Journal of Cyber Warfare and Terrorism*, *5*(3), 1–18. http://doi.org/10.4018/IJCWT.2015070101

Mitra, A., & Schwartz, R. L. (2001). From Cyber Space to Cybernetic Space: Rethinking the Relationship between Real and Virtual Spaces. *Journal of Computer-Mediated Communication*, *7*(1). http://doi.org/10.1111/j.1083-6101.2001.tb00134.x

Morgenthau, H. (1967). *Politics among nations: the struggle for power and peace* (4th ed.). New York: Knopf.

Morris, C., Morris, J., & Baines, T. (1995). Weapons of mass protection: Nonlethality, information warfare, and airpower in the age of chaos. *Airpower Journal*. Retrieved from http://www.iwar.org.uk/iwar/resources/airchronicles/morris.htm

Nakashima, E. (2015, June 4). Chinese breach data of 4 million federal workers. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/889c0e52-0af7-11e5-95fd-d580f1c5d44e_story.html

National Bureau of Statistics of China. (2014). China Statistical Yearbook-2014. Retrieved from http://www.stats.gov.cn/tjsj/ndsj/2014/indexeh.htm

National Bureau of Statistics of China. (2015). China Statistical Yearbook-2015. Retrieved from http://www.stats.gov.cn/tjsj/ndsj/2015/indexeh.htm

Obama, B. (2011, October 07). Executive Order 13587 - Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information. Retrieved from https://www.whitehouse.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net

Obama, B. (2013, February 12). Executive Order - Improving Critical Infrastructure Cybersecurity. Retrieved from https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

Obama, B. (2015, April 01). A new tool against cyber threats. Retrieved from https://medium.com/the-white-house/a-new-tool-against-cyber-threats-1a30c188bc4#.bw63529ib

Pagano, M. (2009). United States of America. In Steytler N. & Kincaid J. (Eds.), *Local Government and Metropolitan Regions in Federal Countries* (pp. 364-392). McGill-Queen's University Press. Retrieved from http://www.jstor.org/stable/j.ctt8020h.16

Patterson, E. (2005). Just War in the 21st Century: Reconceptualizing Just War Theory after September 11. *International Politics*, *42*(1), 116–134. http://doi.org/http://dx.doi.org.mutex.gmu.edu/10.1057/palgrave.ip.8800100

Patterson, R. (2015). Silencing the Call to Arms: A Shift Away from Cyber Attacks as Warfare. *Loyola of Los Angeles Law Review*, *48*(3), 969–1015.

Peixe, J. (2013, February 28). US gas pipelines at risk after Chinese military cyber attack. Retrieved from http://oilprice.com/Latest-Energy-News/World-News/US-Gas-Pipelines-at-Risk-after-Chinese-Military-Cyber-Attack.html

Peterson, A. (2015, March 27). Someone hijacked the Google of China to attack anti-censorship tools. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2015/03/27/someone-hijacked-the-google-of-china-to-attack-anti-censorship-tools/

Press Reference. (2016a). United States. Retrieved from http://www.pressreference.com/Sw-Ur/United-States.html

Press Reference. (2016b). China. Retrieved from http://www.pressreference.com/Be-Co/China.html

PressTV.ir. (2016, July 14). Chinese man jailed in US for stealing F-35 data. Retrieved from http://www.presstv.ir/Detail/2016/07/14/475206/F35-China-US-military-hack

RT.com. (2015, January 21). 50 terabytes! Snowden leak reveals massive size of F-35 blueprints hack by China. Retrieved from https://www.rt.com/news/223947-snowden-pentagon-china-hack/

Russia's Presidency in BRICS. (2014). Brief introduction to the Shanghai Cooperation Organisation. Retrieved from http://en.sco-russia.ru/about_sco/20140905/1013180761.html

Sanger, D. E. (2009, January 10). U.S. rejected aid for Israeli raid on Iranian nuclear site. *The New York Times*. Retrieved from http://www.nytimes.com/2009/01/11/washington/11iran.html?scp=1&sq=january%202009%20sanger%20bush%20natanz&st=cse

Sanger, D. E. (2012, May 31). Obama order sped up wave of cyberattacks against Iran. *The New York Times*. Retrieved from http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=1&seid=auto&smid=tw-nytimespolitics

Sanger, D. E., & Markoff, J. (2010, January 14). After Google's stand on China, U.S. treads lightly. *The New York Times*. Retrieved from http://www.nytimes.com/2010/01/15/world/asia/15diplo.html?ref=technology

Sanger, D. E., Barboza, D., & Perlroth, N. (2013, February 18). Chinese army unit is seen as tied to hacking against U.S. *The New York Times*. Retrieved from http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?_r=0

Schmidt, M. S. (2012, August 2). Cybersecurity bill is blocked in the Senate by G.O.P. filibuster. *The New York Times*. Retrieved from http://www.nytimes.com/2012/08/03/us/politics/cybersecurity-bill-blocked-by-gop-filibuster.html?_r=0

Schwartz, M. J. (2013, May 21). Google aurora hack was Chinese counterespionage operation. *Information Week: Dark Reading*. Retrieved from http://www.darkreading.com/attacks-and-breaches/google-aurora-hack-was-chinese-counterespionage-operation/d/d-id/1110060?

Shah, A. (2012, January 28). Media in the United States. Retrieved from http://www.globalissues.org/article/163/media-in-the-united-states

Simons, H. (2009). Evolution and Concept of Case Study Research. In *Case Study Research in Practice* (pp. 12–28). London, United Kingdom: SAGE Publications, Ltd. Retrieved from http://srmo.sagepub.com/view/case-study-research-in-practice/SAGE.xml

Spetalnick, M., & Brunnstrom, D. (2015, June 05). China in focus as cyber attack hits millions of U.S. federal workers. *Reuters*. Retrieved from http://www.reuters.com/article/us-cybersecurity-usa-idUSKBN0OK2IK20150605

Stevens, T. (2013). Information Warfare: A Response to Taddeo. *Philosophy & Technology*, *26*(2), 221–225. http://doi.org/http://dx.doi.org.mutex.gmu.edu/10.1007/s13347-012-0070-y

Stone, J. (2015, March 30). Chinese government suspected in GitHub hack, evidence links DDoS attack to censorship push. *The International Business Times*. Retrieved from http://www.ibtimes.com/chinese-government-suspected-github-hack-evidence-links-ddos-attack-censorship-push-1863556

Symantec Security Response. (2010, January 15). Hydraq - An attack of mythical proportions. Retrieved from http://www.symantec.com/connect/blogs/hydraq-attack-mythical-proportions

Taddeo, M. (2012a). An analysis for a just cyber warfare. In *Cyber conflict (CYCON), 2012 4th international conference on* (pp. 1–10). IEEE. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6243976

Taddeo, M. (2012b). Information Warfare: A Philosophical Perspective. *Philosophy & Technology*, *25*(1), 105–120. http://doi.org/http://dx.doi.org.mutex.gmu.edu/10.1007/s13347-011-0040-9

Tarr, G. (2005). United States of America. In Kincaid, J., Tarr, G., & Kincaid, J. (Eds.), *Constitutional Origins, Structure, and Change in Federal Countries* (pp. 382-408).

McGill-Queen's University Press. Retrieved from http://www.jstor.org/stable/j.ctt80vfv.17

Temperton, J. (2015, April 10). China's 'Great Cannon' could hack anyone, researchers warn. *Wired Magazine*. Retrieved from http://www.wired.co.uk/article/china-great-cannon-github-hack

The White House. (2009). Cyberspace policy review (Rep.). Retrieved https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

The White House. (2013, February 12). Presidential Policy Directive - Critical Infrastructure Security and Resilience. Retrieved from https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

The White House. (2014, January 17). Presidential Policy Directive - Signals Intelligence Activities. Retrieved from https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities

The White House. (2016). Foreign policy cyber security. Retrieved from https://www.whitehouse.gov/issues/foreign-policy/cybersecurity

Tweed, D. (2015, October 16). China's cyber spies take to high seas as hack attacks spike. *Bloomberg News*. Retrieved from http://www.bloomberg.com/news/articles/2015-10-15/chinese-cyber-spies-fish-for-enemies-in-south-china-sea-dispute

Tyler, P. E. (2001, July 16). Russia and China sign 'friendship' pact. *The New York Times*. Retrieved from http://www.nytimes.com/2001/07/17/world/russia-and-china-sign-friendship-pact.html?pagewanted=all

U.S. Census Bureau. (2015). Population estimates, July 1, 2015, (V2015). Retrieved from http://www.census.gov/quickfacts/table/PST045215/00

U.S. State Department. (2011, November 29). Dependencies and areas of special sovereignty. Retrieved from http://www.state.gov/s/inr/rls/10543.htm

U.S. State Department. (2016). U.S. collective defense arrangements. Retrieved from http://www.state.gov/s/l/treaty/collectivedefense/

Wang, Q. (2011, October 20). Work to build a peaceful, secure and equitable information and cyber space. Speech presented at the First Committee of the 66th Session of the GA on Information and Cyberspace Security, New York. Retrieved from http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t869580.shtml

Wang, Y. (2015, September 16). For China-US friendly cooperation, for global peace development. Speech presented in the Lanting Forum. Retrieved from http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1297164.shtml

Wang, Y. (2016, February 26). A changing China and its diplomacy. Speech presented in the Center for Strategic and International Studies. Retrieved from http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1345211.shtml

Weisgerber, M. (2015, September 23). China's copycat jet raises questions about F-35. Retrieved from http://www.defenseone.com/threats/2015/09/more-questions-f-35-after-new-specs-chinas-copycat/121859/

Weissman, C. G. (2015, April 13). Meet the team who just exposed China's insanely powerful hacking tool. *Business Insider*. Retrieved from http://uk.businessinsider.com/the-great-cannon-chinese-hacking-tool-exposed-2015-4?r=US&IR=T

Xi, J. (2015a, September 22). Full transcript: Interview with Chinese President Xi Jinping [Interview]. Retrieved from http://www.wsj.com/articles/full-transcript-interview-with-chinese-president-xi-jinping-1442894700

Xi, J. (2015b, September 28). Working together to forge a new partnership of win-win cooperation and create a community of shared future for mankind. Speech presented at the General Debate of the 70th Session of the UN General Assembly, New York.

Zetter, K. (2010a, January 12). Google to stop censoring search results in China after hack attack. *Wired Magazine*. Retrieved from https://www.wired.com/2010/01/google-censorship-china/

Zetter, K. (2010b, January 14). Hack of Google, Adobe conducted through zero-day IE flaw. *Wired Magazine*. Retrieved from https://www.wired.com/2010/01/hack-of-adob

Zetter, K. (2010c, January 14). Google hack attack was ultra sophisticated, new details show. *Wired Magazine*. Retrieved from https://www.wired.com/2010/01/operation-aurora/

Zetter, K. (2013, March 25). Legal experts: Stuxnet attack on Iran was illegal 'act of force'. *Wired Magazine*. Retrieved from https://www.wired.com/2013/03/stuxnet-act-of-force/

Zetter, K. (2014, November 3). An unprecedented look at Stuxnet, the world's first digital weapon. *Wired Magazine*. Retrieved from https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

BIOGRAPHY

Brenna L. Fitzpatrick graduated from Ocean Lakes High School, Virginia Beach, Virginia, in 2011. She received her Bachelor of Science in Sociology and her Bachelor of Arts in Philosophy from Virginia Tech in 2015. She received her Master of Science in Conflict Analysis and Resolution from George Mason University and her Master of Arts in Mediterranean Security from the University of Malta in 2016.