November 2017

Cyber Deterrence against Cyberwar between the United States and China: A Power Transition Theory Perspective

Yavuz Akdag
University of South Florida, yavuz1@mail.usf.edu

Cyber Deterrence against Cyberwar between the United States and China: A Power Transition Theory Perspective

by

Yavuz Akdag

A thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Arts
School of Interdisciplinary Studies
College of Arts and Sciences
University of South Florida

Major Professor: Steven C. Roach, Ph.D.
Bernd Reiter, Ph.D.
Jongseok Woo, Ph.D.

Date of Approval:
September 19, 2017

Keywords: Cyberspace, Stuxnet, Level of satisfaction, Parity of Offensive Cyberwar Capability

DEDICATION

I would like to dedicate this work to my family and my friends who inspired and supported me along the way. My dad and mom, Remzi and Hacer Akdag, have supported me. In particular, I am very thankful to my older brother, Gokhan Akdag, for his guidance and financial assistance. He encouraged me to apply for the scholarship I am currently receiving to pursue graduate studies in the United States. My cousin, Suleyman Akdag, also deserves a profound appreciation for his endless effort to teach me math since my high school years, which played a significant role in where I am currently. I am so grateful to Dr. Nezir Akyesilmen for writing recommendation letters when I needed. He also inspired me to focus on cyber aspect of International Relations. I would also like to express my gratitude to Mrs. Linda Boyette, for her tremendous help with all kinds of issues facing me since I started my degree. Last but not the least, I would like to thank my friend, Marleni Castillo, for her encouragement during the thesis process. This accomplishment could never have been possible without support I received.

ACKNOWLEDGEMNTS

First, I would like to express my very profound gratitude to Dr. Steven Roach for being my thesis advisor and helping me navigate the writing process. He patiently corrected my writing/language mistakes and, then, gently encouraged me to see them on my own. He steered me in the right direction and helped me broaden my perspective. With his invaluable feedback and wisdom, I deeply believed that the quality of this work has substantially increased. He was also very perceptive, considerate, and helpful with the issues I came across along the way.

I would like to thank Dr. Bernd Reiter for being willing to be on the thesis committee and to help me with any sort of questions I had. He even let me borrow one of his research books so that I could have an additional insight into how to do research. I am very grateful to him for his help and contribution to this paper. I am also thankful to Dr. Jongseok Woo for being on the committee and his contribution to this project.

I must also express my gratitude to Ph.D. candidate Nathan Barrick for his writing edits and valuable comments on this thesis. His intellectual capacity ignited sparks in my thinking and stimulated me to raise some critical questions, helping me considerably enrich the argument. Thus, I am appreciatively indebted to him for his assistance and contribution to this study.

TABLE OF CONTENTS

LIST OF TABLES

ABSTRACT

In the last three decades, states and societies have increasingly been connected to each other through Information and Communication Technologies (ICTs) such as satellites and the Internet, thus expanding the sphere of influence of cyberspace. While offering numerous economic and security benefits, this increased global connectivity also poses various security challenges and threats at the national and international level. In particular, the threat of cyberwar has become one of the top national security issues in both the United States and China, as reflected in an increasing number of cyber disputes between the two nations recently. In the wake of this emerging threat, scholars have turned to the classical deterrence strategies of Cold War to counter these new challenges, inspiring the development of cyber deterrence theory.

However, numerous pundits in the cyber deterrence literature doubt the efficacy of cyber deterrence in hindering cyberwar. What theory or approach can offer the best explanatory framework for understanding the efficacy of cyber deterrence in forestalling cyberwar, specifically between the U.S. and China, is a question that remains unanswered. This study explores the effectiveness of cyber deterrence outside the bounds of classical deterrence and technological vulnerabilities in cyber systems and networks, and, then, offers Power Transition Theory (PTT) as an alternative approach to understanding whether cyber deterrence in the context of cyberwar between the rival antagonists can be successful. It answers the question of how PTT can allow us to better understand the effectiveness of cyber deterrence in the prevention of cyberwar between the United States and China. A cyber application of PTT argues that cyber deterrence is largely an

ineffective approach to preventing potential cyberwar between the U.S. and China, particularly if the latter achieves parity in offensive cyberwar capability with the former while concurrently remaining dissatisfied with the status quo in cyberspace.

INTRODUCTION

Background of the Problem and Question

This study examines the question: How can Power Transition Theory allow us to better understand the efficacy of cyber deterrence in preventing cyberwar between the United States and China? This question has become more relevant in recent years because cyberwar discourse has come to the forefront in the national political and security agenda of both China and the United States (Lindsay, 2013; Cai & Dati, 2015). In general, the above-question is also pertinent given that in the last three decades, nations and societies throughout the globe have become increasingly reliant upon information technologies due to the swift diffusion of information and communication technologies (ICTs) such as satellite, mobile phones, and the Internet. The most astonishing example of this growing global interconnectedness of ICTs is the Internet. In the early 1990s, there were only a handful of Internet users and websites. Today, the number is in the billions (Eriksson & Giacomello, 2006, pp. 221-222; Choucri, 2012, pp. 55-60).

The omnipresence of ICTs has become a striking symbol of this emerging global pattern. While seizing the economic, social, and security opportunities cyberspace offers, governments, societies, and corporations have not been able to comprehend the full implications and impacts of this increased global connectivity. Political decision-makers have struggled to grasp the compounding effects of this "fast-moving" and malleable cyber phenomenon upon conventional politics and strategy (Stevens, 2012, p. 148; Lindsay, 2015). As Nazli Choucri aptly puts it, "nontransparent" global interconnectivity defies "the traditional understanding of leverage and influence, international relations, and power politics, national security, borders, and boundaries-as well as a host of other concepts and their corresponding realities" (Choucri, 2012, p. 3).

Therefore, this rapidly evolving link between national security and the cyber domain or cybersecurity has become a central concern to governments. Most worrying to policy-makers is the potential threat posed by both states and non-state actors aggressively using the cyber venue to further their interests. In May 2009, President Barack Obama stated, "It's the great irony of our Information Age--the very technologies that empower us to create and build also empower those who would disrupt and destroy." Such concerns over the vulnerability of information networks and systems reflect the extent to which modern nation-states have become dependent upon ICTs and information networks to function properly (Stevens, 2012, p. 148).

In the late 2000s, there were several cyber developments that raised governments' concern and led cyber threats to be treated as a matter of national security, spurring increased momentum in the construction of cyber deterrence strategies (Stevens, 2012, p. 151). In 2007, Estonia experienced a series of cyberattacks, allegedly perpetrated by Russia, that targeted the various websites, such as those of the government and political parties, and forced them offline for short periods. This event is believed to have paved the way for the materialization of cyberwar discourse. Robert Kaiser, for instance, comments that the 2007 Estonia events were the basis for the formation of NATO's cyber defense policy in 2008 (Kaiser, 2015, p. 11-15). Georgia was the target of massive and more sophisticated cyberattacks, supposedly orchestrated by Russia, during the 2008 Georgia-Russia conflict. This war was also a wake-up call to governments with respect to the magnitude of the cyber threat. In this context, some commentators depicted the Georgia cyber-events during the armed conflict as "the maturation of the process" (Fritz, 2008, pp. 57-62). Undoubtedly, the most pronounced and resonating occurrence was the discovery of the Stuxnet worm in 2010, the most sophisticated cyber weapon on record, designed to target the nuclear facility in Iran (Farwell & Rohozinski, 2011; Rid, 2012; Lindsay, 2013; Lilienthal & Ahmad, 2015). Various scholars acknowledged that the worm, due to its destructive capacity, is likely to usher in a new epoch of interstate war: Cyberwar (Gross, 2011; Clayton, 2011).

As the aforementioned cyber incidents demonstrate, cyberspace and the use of cyber technology no longer exclusively operate as a form of "low politics" dealing with issues not vital to the very existence of a state. Rather, they have become a matter of the "high politics" of coping with issues crucial to national security. Common elements of high politics include, but are not limited to, violence, conflict, and warfare (Choucri, 2012, p. 3). For example, scholars note that full-fledged strategic attacks through cyberspace against the critical infrastructure of the United States can pose a great threat to its national security (Lynn, 2010; Clarke & Knake, 2010). According to the Department of Homeland Security, the critical infrastructure of the U.S., such as the nation's transportation and communication systems and power grids, supplies "the essential services that underpin American society and serve as the backbone of our nation's economy, security, and health." The department further notes that destroying or incapacitating these critical infrastructure systems would have a "debilitating" impact upon "security, national economic security, national public health or safety, or any combination of thereof" (The Department of Homeland Security, 2016). In 2010, in its *National Security Strategy,* the White House regarded cyber-threats as one of the most dangerous national security matters the country had to deal with. To draw attention to the seriousness of the danger, Leon Panetta, the former U.S. Defense Secretary, speculated in 2012 that another "Pearl Harbor" scenario with a cyber component attached to it may face Americans. With respect to that, China's increased cyber espionage on the U.S. government, private sectors, and military fueled considerable fear of this type of threat, leading to President Obama’s explicit accusation of China’s military involvement in such cyber operations in 2013 (Eun & Abmann, 2016, pp. 343-345).

That cyberwarfare threats have become a matter of high politics has provided impetus for the development of cyber deterrence theories to counter these new challenges. In the cyber deterrence literature, there are legitimate concerns about the feasibility of the cyber application of classical deterrence strategies and the efficacy of cyber deterrence (Libicki, 2009; Geers, 2010; Lupovici, 2016). This study provides an alternative approach to better informing cyber deterrence and examining its efficacy in preventing cyberwar between the U.S. and China because these challenges and threats to cybersecurity appear to be more acute in the case of the rivalry dyad between the two states (Lindsay, 2014, p.7). In this light, the main question in this study is how Power Transition Theory can enable us to understand the efficacy of cyber deterrence in preventing cyberwar between the United States and China.

Scholars writing about cyber deterrence tend to first provide the basics of classical deterrence theory (Libicki, 2009; Goodman, 2010; Morgan, 2010, p. 55; Geist, 2015; Bendiek & Metzger, 2015)--perhaps to help readers contextualize the subject, given that there is an extensive body of work written about deterrence theory. Following suit, this paper briefly describes the concepts of classical deterrence theory relevant to cyber deterrence against cyberattacks and cyberwar.

The Concepts of Classical Deterrence Applied to Cyberspace

Numerous scholars, security experts, think-thank researchers, policymakers, and military strategists have begun to study adversarial behavior in cyberspace. Governments and militaries in various nations began developing cyber strategies, constructing national cyber-policy to enhance cybersecurity of critical cyber infrastructure, creating military units to effectively counter the new threat, and finally integrating issues pertaining to the cyber terrain into their overall calculation of national security. For example, the Obama administration ordered the formation of Cyber Command within the U.S. armed forces in 2009 (Choucri, 2012, pp. 127-145; Domingo, 2016). Soon after Washington's announcement, China declared the creation of cyber units within its military in 2010 (Branigan 2010; Ball, 2011, p. 81; Singer & Friedman, 2014, p. 141). Most recently, Turkey announced its aspiration to create a cyber-military unit. According to a report by *Hurriyet Daily News,* Ahmet Aslan, Turkish Transportation, Maritime Affairs and Communication Minister, remarked that Turkey shall create a "cyber army" with the aim of combatting potential cyber threats in the wake of the latest WannaCry "ransomware" cyberattack compromising over 300,000 computers on global scale (Babacan, 2017).

Most important to the efforts to combat cyber threats was the generation of cyber deterrence strategies. Because cyberspace began to be considered as "an operational domain" or as "a war fighting domain" like other domains (such as the sea and the land), the urgent needs of cyberspace have necessitated the development of theories of cyber deterrence in the quest of national and global security. Thus, scholars sought to revitalize Cold War deterrence strategies to understand and combat the new threat from the cyber domain (Stevens, 2012, p. 148; Iasiello, 2014, p. 54).

Deterrence strategy can be traced back to the ancient Greeks. It has come to play an important role in understanding today's security issues (George & Smoke, 1974). The development of nuclear arsenals by the United States and the Soviet Union (USSR) provided them with the capability of annihilating the entire human race. This constituted a strong enough threat to prevent both sides from engaging in any full-scale attack, leading to nuclear deterrence. Kenneth Geers writes that Bernard Brodie, a strategist in the American military in 1946, stated that from that point forward, the chief objective of military establishments across nations switched from winning warfare to the prevention of it (Geers, 2010, p. 298).

Deterrence in international security studies refers to the strategic efforts to prevent other parties from taking detrimental actions by threating to cause--for retaliatory or punishment purposes- “unacceptable” damage on adversaries (Morgan, 2010, p. 55). To put it differently, deterrence is the persuasion of, or “inducement” to, a potential attacker that not taking a specific action will be in their best interest (Morgan, 1997, p. 22). The concept of deterrence refers to “a form of preventive influence that rests primarily on negative incentives” (Paul, Morgan & Wirtz, 2009, p. 2).

Nuclear deterrence theory is composed of three fundamental elements or variables: 1) capability; 2) credibility; and 3) communication (Paul, Morgan & Wirtz, 2009, p. 2). Deterrence’s success depends, if not exclusively, upon possessing means (weapons) for both defensive (deterrence-by-denial) and retaliatory (deterrence-by-punishment) purposes. P. M. Morgan notes that those means should be able to “reach” would-be attackers through delivery mechanisms in an effective fashion and incur “unacceptable” damage on them. Additionally, Morgan states that the command and control mechanisms as well as offensive tools of the defender should be resilient and “survivable” in order to respond after being attacked (Morgan, 2010, pp. 61-62). Credibility refers to the adversary’s assessment of the target’s capability, its “will” to conduct a counter-attack, and finally whether the measures to dissuade can be contestable by itself, meaning that the measures taken to deter “must be certain, severe, and immediate” (Goodman, 2010, pp. 106-107). The deterrer must also make sure that it succeeds in communicating its capability and the threat of retaliation to the potential aggressor (Paul, Morgan & Wirtz, 2009, p. 2). For many authors, this third condition for successful deterrence has greater importance because it pertains to conveying the message of how capable the deterrer is and its resolve to retaliate (Lupovici, 2011, p.51). “Deterrence is a psychological relationship; the goal is to shape an opponent’s perceptions, expectations, and ultimately its decisions about launching an attack” (Morgan. 2010, p. 56).

These three fundamental variables are indispensable for successful deterrence and must be present in all types of deterrence strategy (Paul, Morgan & Wirtz, 2009, p. 2). Deterrence strategies may differ based on the type of “conditional threats” and how they are best addressed (Freedman, 2004, p. 32). For L. Freedman, deterrence strategies fall into four significant categories. First is “narrow and broad” deterrence. “Narrow” means daunting a specific military operation during warfare, such as deterring the use of chemical weapons, while “broad” refers to the deterrence of war in general (e.g. NATO’s deterring the USSR). The second category is “extended and central” deterrence. Extended deterrence denotes safeguarding allies, or third-parties, whereas central deterrence aims at only the protection of one’s own territory. The third category is “immediate and general” deterrence. The former refers to deterrence in a state of emergency while the latter means deterring posture where no immediate threat exists. The fourth category is deterrence-by-punishment (retaliation) and deterrence-by-denial (defense) (Freedman, 2004), with the former deterring the potential offender from attacking by threatening to inflict inadmissible cost and the latter deterring the would-be-aggressor by turning its cost-benefit calculus into an unacceptable, “pyrrhic victory” (Morgan, 2010, p. 55).

Because the threat of cyberattacks and cyberwar lie outside of the classical deterrence framework, deterrence theory’s fundamental assumptions do not work effectively when applied to cyberspace (Morgan, 2010; Stevens, 2012). Deterrence theory assumes that nation-states are rational entities and, thus, act on a rational basis; they gauge the cost and benefit of taking an action or not taking it. If the cost of waging warfare against an adversary outweighs the benefit of it, a state will presumably be daunted from attacking its adversary. Insofar as nation states are deemed main agents in world politics, threats are produced by and confined to the rivalries or relations among states. In this way, each weapon type (e.g. nuclear or biological) represents a varying stratum in the states' calculation to deter--that is, there is "a symmetry between threats and weapons" (Paul, Morgan & Wirtz, 2009). However, nuclear threats posed by the powerful states have given way to risks posed by rogue states and terrorism. According to Freedman, these newly arising threats rendered the existing deterrence strategy of little use and, instead, gave rise to what he refers to as "a more appropriate alternative": "pre-emption." Defining the new strategy as dealing with the menaces prior to their actualization, Freedman also introduces the strategy of "prevention." The idea of prevention copes with a problem in advance so that it does not escalate into a crisis, whereas the strategy of pre-emption is employed when the threat is about to be actualized (Freedman, 2004, pp. 84-87).

The Limits of Classical Deterrence for Cyber Application

Following the application of classical deterrence theory to cyberspace, the discussion on cyber deterrence seems to revolve around two poles. On one pole, some scholars and strategists believe that the nuclear and military deterrence fundamentals can be applicable to the cyber domain (Rice, Butts, & Shenoi, 2011). The study by the United States military, for instance, does not largely differentiate deterrence in kinetic space, such as land and sea, from deterrence in cyberspace (Philbin, 2013, p.16).

On the other pole, numerous scholars and experts raise concern over the feasibility of the concepts of classical deterrence to cyberspace or cyberwar. They identify several technological, political, and legal factors intrinsic to cyberspace which indicate that classical deterrence theory is ill-suited for cyberspace application. These factors include “technological volatility,” anonymity, perplexity, ambiguity, the ubiquity of computer networks and systems, and the asymmetric nature of cyberspace, as well as the limits of international law and norms. These distinctive characteristics of cyberspace impose significant restraints upon the core conditions indispensable for successful deterrence, namely credibility, capability, and communication, thereby subverting cyber deterrence (Geers, 2010; Lupovici, 2011, pp.49-51; Kello, 2013, p.33; Gartzke & Lindsay, 2015, p.320).

The “ambiguities” of cyber deterrence is notably at odds with the “clarities” of the deterrence strategies employed during the superpowers’ competition (Libicki, 2009, p. xvi). This vagueness mainly results from low barriers to entry into cyberspace, which diversifies cyber threat actors, ranging from states and non-state actors to individuals, as well as from the difficulty of attributing the source of an attack and the identity of the cyber perpetrator. The ambiguity problem is further exacerbated by the escalatory nature of the cyber venue, which is mainly caused by the difficulty of signaling intent or motivation, and identifying the location and identity of the attacker. Additionally, the question of how to respond proportionately is difficult, which undermines the credibility and communication of the defender (Kello, 2013, pp. 35-37; Bendiek and Metzger, 2015, p. 558).

Another problem is the asymmetric nature of cyberspace, which is not as big an issue in traditional deterrence. Asymmetry is inherent in cyber interactions. This fact makes it difficult for powerful states to project their cyber capability on relatively small targets or their counterparts that have few or no cyber assets to strike for retributory purposes, thus thwarting credibility (Libicki, 2009, p. 70; Schearer, 2016).

Technological volatility plays an important role in making impractical the application of conventional deterrence concepts to the cyber area. Due to the novelty of cyber weapons and the enigmatic nature of the vulnerabilities those weapons intend to manipulate, it is very difficult to assess their possible effects; cyber weapons are known for causing unintended, "collateral damage." To put it differently, "blowback" is likely, especially if the cyber weapons are poorly employed. Cyber offensive tools are also short-lived. Once revealed, they lose their effectiveness, which makes it implausible to demonstrate capability, thus undercutting credibility (Kello, 2013, pp. 33-34). Furthermore, owing to technological volatility, computer networks and systems previously defined as secure may not be secure the following day, which brings up the legitimate question of whether yesterday's cyber defenses will turn out to be outmoded tomorrow (The MITRE Corporation, 2010; Schneider, 2012; Kott, 2014).

An international legal framework regulating the cyber domain is lacking. Cyber-specific rules and norms to determine an appropriate code of cyber conduct is mostly non-existent. In addition, nations seem to be uneager to undertake cooperative relations with one another with respect to cross-border investigations of cyber-related issues. All of the above-factors complicate communication, thereby making it difficult to apply the strategy of deterrence by denial (Geers, 2010).

Given the distinguishing characteristics of cyberspace, scholars have made suggestions as to how to improve the efficacy of cyber deterrence against cyberattacks and cyberwar. Some have proposed the cyber application of serial deterrence, expanded deterrence, and tailored deterrence, which are extensions of conventional deterrence concepts (Libicki, 2009; Kugler, 2009; Morgan, 2010; Lupovici, 2016). Active cyber defense, deterring cyberattacks by resorting to kinetic means, and cyber deterrence against specific types of cyber weapons amenable to dissuasion are also under consideration (Graham, 2010; Mudrinich, 2012; Denning, 2015; Keen, 2015). Even, re-configuration of the very architecture of the internet has been offered as a means of increasing cybersecurity (Mudrinich, 2012). Other scholars have searched for solutions outside the technical domain of cyberspace. They suggest norm-based approaches under the strategy of deterrence by denial, with an emphasis on human factors in forming ideas and identities in cyberspace, and the social construction of perceived cyber threats (Stevens, 2012; Lupovici, 2016). The 2009 Tallinn Manual, a manual on international law that governs cyberwarfare, is illustrative of the efforts to create norms-based cyber deterrence (Schmitt, 2013, p. 1).

Nonetheless, the logical foundations of the study of deterrence in the previous decades seem to have been unable to address the uncertain and nontransparent threat of cyberattacks and cyberwar (Lupovicki, 2011). Scholars contend that the Cold War classical deterrence principles that played a significant role in the prevention of nuclear war cannot be transferred to cyberspace because corresponding strategies do not “carry the same value” when it comes to the cyber realm (Iasiello, 2014, p. 54). RAND Corporation, for example, maintains, “because cyberspace is so different a medium, the concepts of deterrence and war may simply lack the logical foundations that they have in the nuclear and conventional realms.” From this standpoint, cyberspace ought to be approached on its own merits (Libicki, 2009, p. 5). Consequently, scholars, experts, and government officials still have significant reservations about the effectiveness of cyber deterrence in meeting the challenges of cyberwarfare. What theory or approach can provide a better explanatory framework for informing cyber deterrence and understanding its effectiveness in countering cyber threats or preventing cyberwar, specifically between the U.S. and China, is a question that appears to remain unanswered in the literature. This study will focus on providing a relevant answer to this question in the context of cyberwar between the U.S. and China.

The Policy Gap and Central Argument

The studies regarding cyber deterrence have some commonalities (Lupovici, 2011, p. 49; Denning, 2015). Of those common elements, the most relevant one is that the studies overwhelmingly address the issue through a policy perspective and not through a theoretical perspective. For that reason, the bulk of pertinent works suffer from a lack of rigorous theoretical analysis, or they do not expressly or squarely refer to a theory in addressing cyber deterrence versus cyberattacks or cyberwar (Erikson & Giacomello, 2006; Lupovici, 2011, p. 49; Liff, 2012) Scholars articulate two reasons for the lack of theoretical analysis of the issue. Firstly, the history of cyber phenomenon entails a less than 30-year period. Consequently, there is an understandable lack of adequate historical cyber incidents to enable scholars to empirically evaluate "propositions" regarding cyberwar, making it difficult to develop a theory that can explain cyber phenomena (Lindsay, 2013, p. 368; Kosenkov, 2016, p. 2) and help better understand the efficacy of cyber deterrence. As Adams P. Liff aptly puts it, "Theorizing about a kind of warfare [cyberwar] that has not occurred necessitates a major caveat," which is, in this case, under-theorization of the pertinent studies (Liff, 2012, p. 403). Secondly, the "policy analysis community" dominates much of the work on global cyber security issues. Because the policy circles have largely addressed the issue through the lens of policy rather than theory, a theory-policy gap is pervasive in the study of cyber deterrence (Lupovici, 2016, p. 323).

This theory-policy gap is particularly acute in relation to cyber doomsday scenarios, such as a "digital Pearl Harbor" or "cyber 9/11" (Lindsay, 2015, p. 53), specifically in the context of cyberwar between China and the United States. Several researchers have provided some insights into how and why cyberwar between the U.S. and China, notably potential disputes over Taiwan, can occur as they have examined the applicability of classical deterrence wisdom to cyber deterrence (Libicki, 2009; Kugler, 2009, pp. 319-320). These insights, however, cannot go beyond mere speculation and “threat inflation” (Lindsay, 2013, p. 368), with only few exceptions (Domingo, 2016; Thomas, 2016). Most lack a rigorous theoretical framework or analyze cyber deterrence and its efficacy only within the confines of classical deterrence theory through analogy and technical vulnerabilities in cyber systems, as the above studies suggest. The main challenge or problem, then, lies in developing a new theory or using an existing theory that can address and help to better understand the efficacy of cyber deterrence against cyberwar between the U.S. and China. This study presents Power Transition Theory (PTT) and suggests that PTT can provide a theoretical framework to meet the challenge of better understanding whether cyber deterrence in the context of cyberwar between the U.S. and China can be successful.

A cyber application of Power Transition Theory argues that the analysis of the efficacy of cyber deterrence in the context of cyberwarfare between the U.S. and China should go beyond the limits of traditional deterrence theory and technical vulnerabilities in cyber systems and networks. Rather, the theory suggests that the political and strategic calculation of China and the U.S. in the cyber terrain will dictate the success and failure of cyber deterrence. In this respect, a cyber application of PTT maintains that the degree of satisfaction of China and its relative offensive cyberwarfare capability (parity of cyber-offense power) to that of the U.S. will determine the effectiveness of cyber deterrence between the two sides. This study argues that cyber deterrence is largely an ineffective approach to understanding how best to prevent cyberwar between China and the United States. Applying PTT indicates that China is likely to initiate cyberwar to alter the prevailing status quo in cyberspace in its favor, particularly if it approaches offensive cyberwarfare capability parity with the U.S. while simultaneously remaining dissatisfied with the cyber order.

Based on this thesis, there are two critical variables that play a decisive role in determining under what conditions cyber deterrence will be ineffective and whether cyberwarfare between the U.S. and China is likely to ensue. This study explains the level of satisfaction of China with the existing status quo in cyberspace by examining the rivalry dyad of the U.S. and China (Table 2) to determine whether the latter has been conflictual in its cyber relations to the former. Richard A. Clarke and Robert K. Knake's table (Table 1), wherein China and the U.S., along with three other nations, are compared based on their cyberwar capabilities, is the basis for the analysis of whether China has reached a parity of offensive cyber power with the U.S.

The relevancy of Power Transition Theory for assessing the efficacy of cyber deterrence between the U.S. and China is two-fold. First, the utility of this theory lies in its exploration of the trajectory of power diffusion between the United States and China and in its explanatory scheme as to when, how, and why the potential power transition war between the two states may occur (Tammen et al., 2000; Jackson, 2014, p. 338). Because this study aims to examine the effectiveness of cyber deterrence in preventing possible cyberwar between the U.S. and China, the application of PTT becomes most pertinent. Second, conventional and nuclear deterrence have been points of departure in developing an effective cyber deterrence against cyberwar through analogy. Power Transition Theory has been critical to some principles of the classical deterrence (Tammen et al., 2000; Kang & Kugler, 2015), and so it should be relevant to this discussion of cyber deterrence.

Power is a dynamic element; it is subject to change, as is the cyber-offense power of both parties (Nye, 2011). Similarly, China's level of satisfaction with the current status quo in cyberspace is liable to change over time, depending on its perception of whether the cyber order at the time is favorable enough. Since level of satisfaction and cyber-offense power are subject to change, so is the nature of the cyberwar threat between the two states. With cyber-offense power parity, peace in the cyber domain will likely prevail if China is satisfied with the status quo in cyberspace, whereas cyberwar will be likely if China is dissatisfied with the cyber order. This fact also indicates that the deterrence of cyberwar is flexible. Cyber deterrence between the U.S. and China can span an array of different responses at technical, economic, and political, as well as strategic, levels in order to prevent the simultaneous presence of the two critical variables: China's dissatisfaction and cyber-offense power parity.

This study suggests that making the current status quo in cyberspace favorable to the rising power China can profoundly diminish the possibility of an outbreak of cyberwar in the ensuing decades. In this sense, the flexible nature of deterrence against cyberwar between the U.S. and China lends to the more viable strategy of deterrence by economic, political, and strategic measures. The U.S. can play a crucial role in creating a satisfied China through integrating China into formal alliances or economic associations in cyberspace. In this sense, North Atlantic Treaty Organization (NATO)'s extended cyber deterrence policy can be a principal means of achieving such an objective. The manipulation of economic incentives to increase satisfaction is another effective way. Economic associations can open up new frontiers that may pave the way for political convergence with China on cyber-related issues, such as Internet governance, thus increasing satisfaction. By extension, the U.S. can spread satisfaction by utilizing globalization and ICTs in order to help the private ICT sector grow in China. In re-engineering cyber offensive warfare capability to remain ahead of China, the U.S. can increase resources at its disposal through the expansion of its alliance bloc by adding new members (Tammen et al., 2000).

Lastly, the global community should also bear responsibility for ensuring a peaceful *cyber* power transition, if it ever transpires, by taking conciliatory stances on cyber-disputes between the U.S. and China, promoting cooperative discourse and encouraging undertakings with China on cyber issues, such as cybercrime, and working in cooperation with the U.S. to lift barriers to a fair distribution of power in cyberspace.

It should be underlined that this study analyzes US-China bilateral cyber-relations in isolation from their overall relations in the kinetic world, thus necessarily making the analysis made here artificial. By extension, considering the wide extent of the bilateral cyber-relationship between China and the United States, ranging from security and economic to social and cultural relations, this study mainly focuses on the distribution of offensive cyberwar power between the two states and China's relative evaluation of the cyber order. Although narrow, this eclectic analytical approach can, nevertheless, be appropriate and beneficial.

Combining all together, this study provides a useful theoretical explanation and offers policy prescriptions and strategies to implement in order to hinder potential cyberwar. It informs policy-making by bringing new perspectives to the issue in question and offering guidelines for a peaceful re-distribution of power in the cyber venue.

Methodological Framework

This study utilizes qualitative research techniques that necessitate multiple methods and sources to corroborate the outcome. As a mode of observation, document analysis is used. Documents are social constructions. They are shared and utilized in an organized fashion. Thus, some scholars define documents as "social facts." Document analysis refers to a procedure for the review or evaluation of both electronic and printed documents that contain images and texts (words). Glenn A. Bowen notes that document analysis demands that the researcher examine and interpret data so as to "elicit meaning, gain understanding, and develop empirical knowledge". In this sense, documents can be helpful to the researcher in discovering insights pertinent to the research problem (Bowen, 2009, p. 27).

In addition, while document analysis has usually been used to complement other research methods, it has also served “as a stand-alone method.” In this context, Bowen highlights the growing number of journal articles and research reports that have, in recent years, used document analysis as a part of their preferred methodology (Bowen, 2009, pp. 27-29). Political scientists have found document analysis especially useful as a means of observing through texts or written records those political phenomena which are not conducive to direct observation (Johnson & Reynolds, 2012, p. 278).

The underlying reasons why document analysis was preferred in conducting this research are as follows. First, the documents analyzed provided substantive historical insight and background information. This helped define the root of the problem and the conditions that impact on the phenomena under scrutiny, contributing to answering the research question (Bowen, 2009, pp. 29-30).

Second, because the documents relevant to the research subject entail broader time periods, it helped observe differing methods and theories discussed and applied in the relevant literature (Johnson & Reynolds, 2012, p. 279). Furthermore, insofar as document analysis allows one to analyze varying drafts of a specific document, the researcher was able to compare them to track developments and changes (Bowen, 2009, p. 30). This helped identify what solutions in the pertinent literature were offered to increase the efficacy of cyber deterrence against cyberattacks and cyberwar. Third, collecting data from the running records is cost effective and time-saving (Johnson & Reynolds, 2012, p.279.

Fourth, the accessibility of the documents investigated in this research was another upside of this method. The relevant articles, books, reports, journal memos, and other documents were readily accessed through the library database and Internet. Fifth, and perhaps most importantly, analyzing documents from various sources could be used for the corroboration of arguments, thus reducing potential biases in a single study (Bowen, 2009, pp. 28-30). For example, examining various sources provided significant insights in understanding the offensive cyberwarfare capabilities of both China and the U.S., and this corroborated Richard A. Clarke's table where he compares the cyberwar strength of the U.S. and China along with other three states based on their offensive power, defensive power, and level of dependency on cyber systems.

This research uses secondary sources, including articles (from both academic and policy journals, and magazines), books, conference proceedings, notes, commentary, government documents, reports, and charts, for data collection. For instance, in examining China's level of satisfaction with the status quo in cyberspace, this study used a research study by Brandon Valeriano and Ryan C Maness featuring cyber incidents among rival states, including the United States and China, from 2001-2011.

The data relevant to the subject were mostly collected by browsing the library catalogs of the University of South Florida and utilizing Internet search engine queries, such as Google Scholar. In the search for documents, the following key terms and concepts were queried: *Cyberspace, cyber deterrence, cyberwarfare, Power Transtion Theory, cyberattack, cyber power, cyber capability, cyber conflict, cybersecurity, attribution problem, China, and the United States*. For the most part, academic articles along with books written by scholars who are prominent figures in regards to the subject were included in this study. In particular, some key studies on cyber deterrence and cyberwar were meticulously examined and drawn upon, especially *Cyberdeterrence and Cyberwar* by Martin C. Libicki and Cyber Deterrence by E.T. Jensen.

However, it should be noted that document analysis is not without limitations. A central limitation of this method may be that the relevant sources collected and examined can be picked up selectively, thereby rendering the finding or analysis made here highly biased (Bowen, 2009, p. 32).

The Study Design

This study is composed of four chapters and an introduction section. In the introduction section, the brief outline of the study is provided. The concepts of classical deterrence applied to cyberspace are touched upon, and the main problem, fundamental question, sub-questions, thesis statement, as well as the methodological framework are presented.

Subsequently, Chapter One discusses the theoretical framework upon which the analysis in this study is built. It presents Power Transition Theory and Classical Deterrence theory, elaborates on Power Transition Theory, and clarifies why the theory is pertinent and how it can offer more useful insights in understanding the efficacy of cyber deterrence in the context of cyberwar between the U.S. and China.

Chapter Two addresses the cyber deterrence literature to demonstrate the limits of classical deterrence and attempts to answer relevant sub-questions: How does conventional and nuclear deterrence wisdom apply to the relatively new environment of cyberspace? How does cyber deterrence vary from traditional deterrence? What are the key challenges of the cyber domain that impose significant restraints upon the applicability of conventional deterrence concepts to cyber deterrence? What are possible solutions that increase the efficacy of cyber deterrence?

Chapter Three lays the basis for contextual landscape and defines cyberspace and cyberwar. It alludes very briefly to the burgeoning literature on cyberwarfare and discusses what can be achievable with cyberwar, whether it can be a strategic means, and for what purposes nation-states resort to it. In this chapter, the case of Stuxnet is also addressed because it offers useful insights in understanding the nature of cyberwar and provides cogent justification of the definitional landscape in relation to cyberwar.

Finally, Chapter Four concludes the fundamental argument made in this paper. This chapter will shed light upon China’s relative assessment of the current status quo (level of satisfaction) in cyberspace and its relative cyberwar capability (parity of offensive cyberwarfare power) to that of the United States in order to understand the effectiveness of cyber deterrence against cyberwar between the two rivals. Lastly, the significance and implications of this study are addressed.

Chapter One: Theoretical Framework

1.0 Introduction to Chapter

This chapter addresses the theoretical framework utilized to answer the fundamental question and explain the central argument. It discusses contesting theories, namely Power Transition Theory and Classical Deterrence, for comparative purposes, and elaborates on the former since PTT is the main theory upon which the analysis is based. Comparing them will help to demonstrate how the two theoretical approaches differ in their clarification of conditions for peace and conflict in the international order, and why Power Transition Theory is relevant to the discussion of cyber deterrence and cyberwar. The main objective of the chapter is to indicate how PTT can provide a better perspective or approach to understanding whether cyber deterrence can be effective in precluding cyberwar between the United States and China.

1.1 Power Transition Theory

This study analyzes the efficacy of cyber deterrence against cyberwar between the U.S. and China using Power Transition Theory (PTT). In his piece *World Politics* in 1958, A.F.K. Organski initially deveoped the theory. In 1980, PTT was "redefined" and emprically validated by Jack Kugler and Organski in *The War Ledger* (Lee, 2015, p. 267). Power Transition Theory is defined as a "dynamic" theory because it is applicable to international politics across time; it systematically offers accounts of and baselines for how world politics should be explored. Not only is PTT prescriptive, but it is also a descriptive theory. It describes "the hierarchical relationships among power, satisfaction, and the choice of peace and conflict" and lays out the properties of the international structure. However, central to the theory is its explication of the critical dynamics in the international structure that play determining roles in when, how, and why war transpires (Tammen et al., 2000, pp. 5-6), thereby lending it to a "probabilistic theory of world politics" (Tammen, 2008, p. 318). Additionally, the theory also helps gain an empirical understanding of the "costs, intensity, duration, and consequences of war" and gives guidance in managing conflict arising in the international system (Tammen et al., 2000, p. 6).

Power Transition Theory posits that there is a hierarchical structure in the international order. One nation (the dominant power) sits at the peak of the hierarchy (usually the winner of the last major power war), and other nations are beneath the dominant one. Each nation has its place in the hierarchy commensurate with its relative power (Organski, 1968, p. 364; Rauch, 2016). That is, this hierarchical structure represents the relative diffusion of power among nations. Implicit in the argument is that nations instinctively recognize the uneven distribution of power and influence, as well as shifts in the relative power of nations within the hierarchical order (Tammen, 2008, p. 319).

Placing the United States at the hierarchical top of the international system, PTT defines the U.S. as the "dominant power." The dominant power is the nation exerting significant control over the international system. According to the theory, the nation that sets up the system reaps the most benefits from sustaining the status quo (Organski, 1968, pp. 364-370). The U.S. is the dominant power "by the virtue of the common recognition of its prominent position in world politics" (Tammen, 2008. p. 319). It should be noted that despite being by far the most powerful nation, the United States prefers to exert its influence upon other nations through cooperative actions rather than through the sheer use of force (Tammen, 2008, p. 318).

An essential part of PTT is the recognition of power disparity between the dominant power and those beneath it in the hierarchy. This power disparity ensures the leadership of the dominant power as well as the "stability" of the entire system (Organski, 1968. p. 365). Because the dominant power is the rule-maker and the preserver of the stability in the international system, it has to ensure the satisfaction of those aligned with it and wisely manage the rise of would-be-challengers (Tammen et al., 2000, p. 40). Based on empirical findings in the relevant literature, the theorists of PTT argue that the dominant power is "risk-averse" and unlikely to launch a war because it is committed to the maintenance of the status quo in the global order (Kim & Gates, 2015, p. 222). Lastly, the theory postulates that since it benefits most from it, the dominant power is also the nation most satisfied with the system, especially when not challenged (Tammen et al., 2000, p. 9).

Right beneath the dominant power are the great powers (Organski, 1968, p. 365). Japan, Russia, China, and Germany (or European Union) are classified as the great powers in the present world order (Tammen et al., 2000, p. 6). Distinguishing the dominant power from the great powers is that the former is more capable of exercising influence upon the conduct of others; by extension, it also reaps more benefits from the order than do the great powers. Nevertheless, the great powers also substantially benefit from the order and play, in most cases, a pivotal role in maintaining the status quo. Consequently, the theory states that it is largely in the great powers' best interests to side themselves with the dominant power to reap benefit from the existing international order. Of the great powers, it is, Organski notes, those aligning themselves with the dominant power that fall into the category of "the powerful and the satisfied" nations (Organski, 1968, pp. 365-366).

However, great powers may choose not to abide by the status quo dictated by the dominant power. A possible challenger to the regime always comes out of the layer of the great powers (Tammen et al., 2000, pp. 6-7). The advocates of PTT note that when a great power achieves a significant amount of power relative to that of the dominant nation, it can become a viable challenger to the status quo power. In this light, the theory asserts that China best suits the title of a potential challenger capable of taking on the dominant nation, in this case, the U.S., due to its rapid growing economic power (Tammen et al., 2000).

For PTT, power is subject to constant change due to varying growth rates (Rauch, 2016). Organski refers to power as “the ability to influence the behavior of others in accordance with one’s own ends” (Organski, 1968, p.104). The theory maintains, “a country’s power is a function of population, productivity, and relative political capacity.” In other words, PTT defines national capability as endogenous elements comprised of a productive economy, a fertile and large population, and high political capacity adept at the extraction of resources, such as human and material capital. According to PTT, to the extent that these three crucial components of power are successfully managed, a nation can expand its influence beyond its borders (Tammen et al., 2000, pp. 15-20). Important to emphasize here is that changes in these essential components of national power may mean a shift in the distribution of power among nations in the hierarchy. This can be a source of instability in the international order due to swift changes in the aforementioned elements of national power (Organski, 1968, p. 338). Consequently, PTT argues that the preconditions for peace and war in the international system result from shifts in a nation’s relative power in the hierarchical order (Tammen et al., 2000).

The theory contends that the ascendancy of challengers achieving a relatively high economic growth rate is inevitable in the world order (Tammen et al., 2000). PTT underscores that what happens inside the state plays a crucial role in understanding the occurence of conflict in the global system. It is the internal developments in a state, such as a rapid industrial expansion, explosion in population size, and “political modernization” that can increase a nation’s capacity and, thus, explain the underlying reasons why a rising power challenges the status quo (Kim, 2015, p. 252). While the United States currently possess a substantial advantage over China in terms of overall national power, this power preponderance will not, according to the PTT theorists, prevail indefinitely (Tammen et al., 2000). The U.S. has a "mature" economy that has for decades been growing at about a 3% ratio, while China's economy has achieved a few decades of rapid growth at roughly a 9% rate. Implicit in this swift economic growth ratio is the ultimate translation of economic power into regional and, then, global power (Tammen, 2008, p. 320).

It is worth noting that the ongoing power transition between the U.S. and China does not, for PTT's proponents, vary from the previous challenges to the dominant powers of different eras. For example, Germany challenging the United Kingdom in the early 20th century bears similarity with the current process unfolding between the U.S. and China, and yet more important is that the theory aims to shed light upon whether China's potential challenge to the U.S. will lead to a power transition war or occur peacefully (Tammen et al., 2000, p. 18).

As articulated above, Power Transition Theory neatly clarifies preconditions for power transition war in the international system. It offers three critical variables through which the probability of war is anticipated: Power parity between the rising challenger and the dominant power; overtaking; and level of satisfaction of the contender (Kugler & Lemke, 1996).

First, core to the argument regarding *power parity* is that stability in the status quo is maintained when there exists a power preponderance of the dominant nation over possible contenders. Instability, however, likely ensues when a challenger catches up in power with the prominent country. In other words, the theory argues that one of the main causes of a wide-scale war is not the disparity of capabilities among the dominant power and the potential challanger, but, rather, it is mainly due to the would-be challenger reaching power parity with the dominant nation (Lee, 2015, p. 267). Essential to underline is that China has swiftly and steadfastly been growing with a larger population; it may surpass the U.S., which has already reached a sustained economic growth rate (Tammen et al., 2000). PTT argues that as the challenger China approaches power parity with the dominant power U.S., the odds of war substantially rise (Lim, 2015, p. 284).

What does this mean for the U.S-China relationships? How can the dominant power manage the time periods prior to the challenger achieving power parity? Power Transition Theory argues that because the U.S. already has a saturated economy, it has to find "external resources" to obtain significant relative gains in order to make up for China's rapid internal economic growth. This can be done through the expansion of its alliance bloc and its "economic reach," or simultaneous application of both. To add a new member, including previously discontent nations, to the alliance means an additional resource to "the power base of the alliance" that could be leveraged in times of crisis. The purpose of expanding the alliance is to "acquire overwhelming preponderance of power and the resources sufficient to head off any fast-growing challenger" (Tammen el al., 2000, p. 38). In this context, PTT suggests that the U.S. should foster European countries to combine their resources with those of the U.S. against any common threat. The theory also argues that the dominant power ought to encourage the integration of Russia into NATO. According to PTT, not only would Russia's European integration increase the pool of resourses available to the dominant power to maintain its preponderance, but also it would contribute to Russia remaining a satisfied nation, denying China "the opportunity to reestablish an anti-American alliance with Russia." The same strategy would also likely apply to India. PTT envisions that India has the potential to overtake the U.S. in the future. For that reason, it suggests that integrating India into the pool of satisfied U.S. allies would serve the purpose of increasing resources at the Western alliance's disposal, preventing, or further delaying, power parity between

China and the United States. This would, in turn, diminish the odds of a potential conflict between the two rivals through redistribution of power (Tammen el al., 2000, pp. 175-176).

The theory further suggests that if forging such formal alliances is not feasible, the dominant power can resort to further forming economic-based alliances in order to reengineer power diffusion. Economic agreements have binding effects on ratifying countries by producing mutual areas of “self-interest,” which may contribute to both sides resolving political disagreements. The U.S. policy in Europe in the aftermath of World War II is an excellent example of successfully reengineering power distributions through economic associations. With that in mind, the theory contends that corresponding “manipulation of economic incentives remains one of the most powerful policy tools the United States can wield in its relationship with China” (Tammen et al., 2000, p. 38).

The second crucial variable in explaining the odds of a major power transition war is the concept of *overtaking*. The potential challenger may intend to displace the dominant power in its position of world leadership and can accomplish this through internal developments, such as a significant increase in political and economic capacity. Overtaking is actualized once the rising challenger outstrips the relative power capability of the dominant power, which markedly increases the odds of war occurring (Tammen et al., 2000, p. 21). It is worth highlighting that how swiftly the rising challenger approaches the power parity with the declining dominant defender and how fast the overtaking is realized will substantially impact the prospects of a system-wide war; the faster the overtaking occurs, the more likely it is to lead to a power transtion war (Kim, 2015, pp. 252-253).

The third critical variable in determining the possibility of power transition war is the degree of *satisfaction* of a potential challenger with the prevailing status quo. This variable is believed to be central to the theory in its explication of why conflict occurs in the international system (Rauch, 2016). Based on PTT, the likelihood of war increases upon the existence of differentials in how the challenger and the dominant power perceive the existing international order and rules guiding the hierarchy (Tammen & Kugler, 2006, p. 40). In other words, the challenger is likely to wage war if its national interests and preferences are considerably distinct from that of the dominant power. If that is the case, then, it frequently follows that the rising challenger is dissatisfied with the status quo. Importantly, even if power parity is achieved and overtaking occurs, preconditions for war have not been met unless the challenger is dissatisfied with the order. If satisfied, then, the challenger will supersede the dominant power peacefully; if not, it may become a risk-taker and will inexorably seek to bring about changes in the status quo in its favor. Therefore, the theory concludes that the discontent challenger will be more willing to wage war than the dominant power. However, in either case, the discontent challenger will modify the system, peacefully or not (Tammen et al., 2000).

What does this mean for the U.S-China relationship? How can the dominant power manage satisfaction? And what is the role China can/should play in managing satisfaction? Power Transition Theory argues that to manage satisfaction, the U.S. and its allies' foreign policy objective must be to create a "satisfied" China (Tammen et al., 2000, p. 34). This can be accomplished through multiple means. The U.S. can subtly and indirectly increase satisfaction using globalization as a means to extend its "commercial and cultural systems." ICT (Information and Communication Technology) is also a very effective tool or "a principal vehicle" for the creation and diffusion of satisfaction. By utilizing ICT, the dominant power can "penetrate borders, open new markets, distribute information, create constituencies, and tie together common interests, [serving] the purposes of a status quo dominant power" (Tammen et al., 2000, pp. 38-39).

The dominant power can foster satisfaction by integrating China into an alliance or offering opportunities that may facilitate China's socialization into the current international order, which would make it more willing to abide by the existing international rules and norms. In this sense, the theory maintains that China's integration into NATO may enhance China's satisfaction level and may pave the way for a peaceful transition if that ever takes place. PTT also asserts that binding economic organizations, such as the European Union and World Trade Organization, are meant to create economic utilities to increase the satisfaction of nations in the U.S.'s bloc. Such economic associations with China may produce economic benefits and catalyze Chinese economic growth, increasing satisfaction. More specifically, the theory suggests that Washington should prioritize assistance to the private sector in China and encourage foreign investment in China. Although political decision-makers dominate "the domestic power hierarchy," private enterprises are the second most effective players. Consequently, the interest of business community usually has great impact upon the calculus of national security interests. A Chinese business sector integrated with the global economy would be a disincentive for the Communist party to pursue an aggressive trajectory in its foreign policy.

However, PTT argues that for the private sector in China to grow, the regional authorities must play a greater role in the allocation of national resources in China. This necessitates the decentralization of Chinese government. In addition, China must be committed to abiding by international rules in relation to trade and commerce, and encourage "free enterprise and democratization," which are likely to remain significant challenges for China (Tammen et al., 2000, pp. 157-179).

At this point, one may ask the question of why the dominant power does not use its power preponderance over the challenger and initiate an early war to dispel the threat and ensure its position at the top of the pyramid. Power Transition Theory maintains that the leader nation does not attempt to initiate a preemptive war because the conflict may disrupt the system of norms and rules which it has set up. The prevailing status quo provides not only economic gains but also security benefits to both itself and its satisfied allies. Launching a preemptive war would cause havoc in the order and lead to uncertainty among the satisfied system advocates, resulting in a significant decline in their support for the status quo. When the legitimacy of the status quo diminishes in the eyes of the satisfied nations, so does the power preponderance of the leader nation. That is why PTT claims that a dominant power is likely to be risk-averse and unlikely to start a war (Tammen et al., 2000, p. 27).

Distinguishing dissatisfied states from satisfied ones is based on to what extent cooperative actions guide them in their relations to one another. PTT is at odds with the realist theorists of International Relations who argue that power relations among nations dictate conflict and peace in the international system. PTT suggests that differentiation in preferences is, in conjunction with power parity, central to determining whether conflict occurs or peace prevails (Tammen & Kugler, 2006, pp. 40-41). Due to the perception that they do not accrue benefits from the existing status quo as much as satisfied nations do, dissatisfied states will aspire to bring about changes in the order given the opportunity. As such, they will assertively and forcefully try to make some modifications in the web of relations among nations in the international hierarchy as a way of reaping more benefits from the order. Therefore, PTT argues that nations discontented with the status quo are more likely to engage in non-cooperative relations with their satisfied rivals. This, coupled with power parity, considerably increases the probability of a major war (Tammen et al., 2000, p. 109).

By extension, the theory postulates that while satisfied states are predisposed to cooperate with each other in a bid for maximizing their "absolute gains," the relations between content and discontented nations are characterized by endeavors for the maximization of their "relative gains" through non-cooperative actions. Thus, according to the advocates of PTT, the bottom line is that the relationship between a satisfied and dissatisfied nation will, in a great measure, be conflictual since their interests lie in conflict (Tammen et al., 2000, pp. 110-111). This point is important to note because it constitutes the logical basis of why this study analyzes the rivalry dyad of China and the U.S. to ascertain whether the former has been non-cooperative and conflictual in its cyber engagements with the later. This analysis will indicate China's level of satisfaction with the cyber system.

For PTT, the probability of war is at its apex when the potential challenger reaches power parity while, at the same time, remaining dissatisfied with the status quo (Tammen, 2008). Based on that, the degree of satisfaction and the power dis/parity are the two most critical variables that dictate the odds of a potential wide-scale power transition war in the international system (Tammen et al., 2000). It is these two important variables that this study uses in order to analyze the efficacy of cyber deterrence against cyberwar between China and the U.S. and, for that matter, whether cyberwar is likely or unlikely. The other variable, *overtaking*, is not subject matter of the analysis in this study because there are divergent views among the advocates of PTT as to whether a power transition war transpires before or after the contender surpasses the dominant power, thus making the variable controversial (Lim, 2015, p. 284).

Having laid out the most important tenets of PTT, it is imperative to very briefly outline the precepts of classical deterrence theory for comparative purposes. This comparison will clarify how the two contesting theoretical frameworks explain the conditions that foster peace and induce conflict in the international order. In comparing PTT with classical deterrence, the advocates of PTT refer to the structure of deterrence as "the interaction between two competitors" (Tammen et al., 2000, pp. 84-85). This position is also consistent with this study because the paper attempts to examine the efficacy of cyber deterrence against cyberwarfare between two contenders, namely the United States and China, through the lens of Power Transition Theory.

1.2 Alluding to Classical Deterrence Theory

Although there are various theoretical perspectives and extensions of classical deterrence, the proponents of Power Transition Theory appear to focus on classical nuclear deterrence as a point of departure for "comparative purposes" since it derives from the balance of power theory and, therefore, allows more precise comparisons and contrasts with Power Transition Theory. So, in this study, classical deterrence chiefly refers to classical nuclear deterrence (Tammen et al., 2000, pp. 84-85).

In the Cold War era, classical nuclear deterrence theory was conceived to prevent nuclear war (Schelling, 1979). K. Kang and J. Kugler point out that according Bernard Brodie, the first proponent of the theory, global stability is ensured by the potential menace of losing masses of population from punitive retaliations between the nuclear weapons-holding states (Kang & Kugler, 2015, p. 284). This idea is a derivative of the realist theory of International Relations (IR), according to which, the global order exists in an anarchical environment and can only be maintained through the balance of power (Tammen et al., 2000, pp. 85-87).

Similar in logic to the balance of power theory, classical deterrence posits that a balance of power (power parity) is not a sufficient condition for the assurance of peace; the presence of nuclear power balance (parity) is vital to the avoidance of conflict and preservation of peace in the international system given the assumption that nation-states act on a rational basis (Tammen et al., 2000, pp. 85-90). In other words, the main premise of this approach is that if nuclear proliferation expands and Mutually Assured Destruction (MAD) is accomplished, a potential nuclear war between contesting international actors possessing a destructive "second-strike retaliation" capability is much less likely to occur. This is because under MAD conditions, the costs of warfare turn out to be irrational and "unthinkable." Related to this, John J. Mearsheimer, a prominent figure of realist theory of IR, comments, "the more horrible the prospect of war, the less likely it is to occur" (as cited in Kang & Kugler, 2015, p. 284).

According to the proponents of classical deterrence theory, given that "payoffs to hostile" actions by any actor are even, a reciprocal destructive outcome emerges if war erupts. In consequence, nuclear powers tend to be risk-averse because they are presumably rational actors. Therefore, the likelihood of purposeful conflict is virtually ruled out. This is the theoretical basis of "the stability of deterrence equilibrium." However, classical deterrence postulates that there may be conditions under which the acquisition of nuclear power and nuclear equality do not guarantee the stability of the global order. According to the classical deterrence theorists, there are two conditions under which the theory fails: In an "irrational" decision-making mechanism; or through unintended or accidental initiation (Kang & Kugler, 2015, pp. 285-286).

Classical deterrence also argues that under nuclear preponderance, conditions for an anarchic international environment fade away. The theory assumes that a nuclear nation will opt for the continuation of the status quo and, thus, will be unwilling to launch a war unless challenged. However, for classic deterrence, general deterrence is "tenuous." For example, the theory asserts that general deterrence is insubstantial under Israel's nuclear dominance because what holds Israel back from attacking its adversaries is "the unwillingness to strike first"; yet classical deterrence contends that this fact significantly changes once MAD and nuclear parity are achieved by Israel's opponents. Under MAD, both Israel and its adversaries would be deterred due to the fear of reciprocal annihilation. At variance with classical deterrence theory, PTT maintains that with a satisfied and nuclear preponderant Israel in the region, there is a higher chance of general deterrence succeeding because Israel will seek not to disrupt the existing order from which it significantly benefits (Tammen et al., 2000, pp. 96-97).

The most contentious argument of classical deterrence is associated with nuclear proliferation. In this line of thought, disputing countries may be armed with nuclear arsenals to achieve nuclear parity across the entire system, which would eliminate conflict and ensure stability. With respect to that, Kang and Kugler point to Kenneth Waltz's argument that because there is nuclear disparity in the Middle East, with only Israel in possession of nuclear weapons, the region is unstable. Some countries in the region, such as Turkey, Saudi Arabia, and, more importantly, Iran, should be assisted in developing nuclear weapons in order to achieve nuclear power balance and bring stability to the region (Kang and Kugler, 2015, p. 285).

1.3 Power Transition versus Classical Deterrence

Having laid out some of the basics of classical detrrence theory, it is important to note that the advocates of PTT question classical deterrence theory's empirical validity, which makes the theory revelant to this study. According to Power Transition Theory, the emergence of nuclear weapons did not shift the underlying casues of conflict, war, and peace. Unlike classical deterrence, PTT does not view any outbreak of a nuclear war as accidental; instead, it contends that a nuclear war, if it ever occurs, would be a result of "goal-seeking behavior" (Kang & Kugler, 2015, p. 286). In contrast to the classical deterrence theory's view of an anarchic world, Power Transition Theory depicts a hierarchical world order, with each nation sitting in a different place in accordance with their national power. PTT suggests that it is not power parity but power preponderance that induces stability in the international system. According to PTT, while dissatisfied nations seek to alter the status quo, the satisfied preponderant power and its allies seek the preservation of the international order (Tammen et al., 2000).

At odds with the classical deterrence' perspective that under nuclear parity (MAD), stability in the world order is ensured, PTT argues that the odds of wide-scale war increase under balance of nuclear power (parity). The theorists of PTT specifically direct criticisms at classical deterrence's neglect of a nation's satisfaction level in their assessment of the system's stability. In this light, significantly distinguishing PTT from classical deterrence is that PTT maintains that stability is ensured by the presence of a satisfied defender that has nuclear preponderance while it is threatened by the presence of a dissatisfied contender with significant nuclear power in comparison with the dominant power (Tammen et al., 2000, pp. 91-100). According to PTT, the dissatisfied challenger is driven by the motive of gaining a greater share of the benefits. Consequently, the discontented challenger may deem the prospect of conflict as an "opportunity," not a "danger". Therefore, as stated by Power Transition Theory, in spite of the existence of the risk of MAD, the discontented challenger will opt to engage in war, thus rendering the deterrence power of nuclear weapons tenuous (Kang & Kugler, 2015, p. 287). Based on that, central to PTT's argument is that in sharp contrapose to the classical deterrence view, the prospect of nuclear warfare is more likely under nuclear parity (MAD) provided one of the nuclear nations is in the state of dissatisfaction with the existing status quo. In other words, nuclear parity can only ensure stability if the nuclear powers are content with the prevailing status quo (Tammen et al., 2000).

The significance of dissatisfaction level of the contender is underscored by the PTT's theorists. They maintain that once a dissatisfied challenger reaches the nuclear capacity of the declining dominant power, the challenger is likely to leverage its capability to demand a new, favorable order. In contrast to classical deterrence theory, which argues that "the Cold War remained cold" due to the prohibitive costs of nuclear war, or MAD, PTT suggests that the Cold War did not turn into a hot one in that "the USSR could not credibly challenge the U.S. or NATO allies.". Important to note that the proponents of PTT anticipate that when China approaches conventional power equivalence with the U.S. and simultaneously remains dissatisfied, the future relations between the two will be more perilous than the relations between the USSR and the U.S. during the Cold War (Tammen et al., 2000, pp. 90-92).

The importance of the level of dis/satisfaction is also manifest with respect to the idea of proliferation. PTT and classical deterrence theories contrast on this issue. Classical deterrence theory contends that nuclear proliferation will ensure peace because wide-scale nuclear proliferation among nations will make war too costly, decreasing the odds of war occurring. On the contrary, PTT suggests that while proliferation of nuclear weapons to discontented nations will increase the prospect of nuclear warfare, arming satisfied nations with nuclear arsenals will likely promote peace. Thus, essential to the PTT's argument is that one should not link the odds of nuclear war to the degree of "destruction" but to the degree of "dissatisfaction" (Tammen et al., 2000, pp. 97-100).

Reinforcing the point pertaining to proliferation, PTT theorists question classical deterrence's empirical validity. They pose a provocative question, demanding answer for the underlying motive of the United States' development and deployment of ballistic missile defense systems in East Asia if MAD can ensure stability. They contend that it is conspicuous that the U.S.

acts with the purpose of achieving “a nuclear advantage,” not of preserving MAD, thereby bringing the classical deterrence view’s validity into question (Kang and Kugler, 2015, p. 285).

PTT also contends that the classical deterrence`s argument that nuclear proliferation plays a stabilizing role cannot be acknowledged by the actions of the global community. To corroborate this argument, they, again, pose a critical question of why the international community attempts to hinder North Korea from acquiring weapons of mass destruction (WMD) whereas classical deterrence seems to be mute on the development of nuclear arsenals with the Middle East with “impunity” (Kang and Kugler, 2015, p. 285). The PTT theorists, for example, draw attention to the fact that the U.S. has made major efforts to preclude Iran from acquiring nuclear weapons while supporting Israel in its quest for a nuclear arsenal. They argue that this is because “U.S. preventive actions are directed only at the dissatisfied nations,” which corroborates the validity of the PTT’s argument that it is not the degree of destruction but the level of dis/satisfaction that dictates conditions for peace or conflict (Tammen et al., 2000, p. 90).

In summary, Power Transition Theory asserts that nuclear deterrence is insubstantial at best. It postulates that if a dissatisfied contender achieves nuclear parity or conventionally overtakes the satisfied dominant power, the prospect of war dramatically increases. Conversely, under nuclear disparity, peace is likely to be ensured by a satisfied status quo power. To put it differently, contrary to classical deterrence theory that associates peace or stability with MAD, PTT argues that the probability of a major war ought to be associated with nuclear parity and level of satisfaction. Lastly, PTT greatly opposes proliferation of nuclear weapons, arguing that acquisition of nuclear weapons by discontented nations poses a grave danger to the stability and peace of the existing international system (Tammen et al., 2000, p. 101).

1.4 The Application of Power Transition Theory to Cyber Deterrence against Cyberwarfare

According to the advocates of Power Transition Theory, it was mainly the above-mentioned deficiencies of classical deterrence theory that encouraged them to develop an alternative perspective and offer alternative explanations for the probability of potential power transition war in the kinetic realm (Kang and Kugler, 2015, p. 286). Similiar in purpose to that, this study suggests that a cyber application of Power Transition Theory can provide an alternative theoretical framework to classical deterrence, arguing that PTT can enable us to better inform cyber deterrence and understand its efficacy in preventing cyberwar between the U.S. and China.

PTT is pertinent to the analysis here for two main reasons. First, PTT is meant to explain how, why, and when a power transition war between the U.S. and China can likely occur in the physical world. This relevance will meet this study's objective to understand the efficacy of cyber deterrence against cyberwar between the U.S. and China. Second, PTT casts considerable doubt on classical deterrence theory in explaining conditions for the stability of the present international system. Because classical deterrence is the basis for cyber deterrence, a cyber application of Power Transition Theory argues that cyber deterrence will, at best, be tenuous in thwarting potential cyberwarfare between the U.S. and China. PTT would suggest that an analysis of the effectiveness of cyber deterrence between the U.S. and China should go beyond the limits of classical deterrence theory and technical vulnerabilities in cyber systems. Instead, a cyber application of the theory asserts that China's relative assessment of the status quo in cyberspace (whether satisfied or not) and its relative cyber-offense capability (power parity) to that of the U.S. should constitute the foundation for such an analysis.

At this point, some important questions should be raised: Why should an alternative theory or approach be used to better examine the effectiveness of cyber deterrence between the U.S. and China? Why does the cyber application of classical deterrence fall short of meeting the challenge of cyberattacks and cyberwar? And what are these challenges to or limitations of cyber deterrence that render it ineffective? The next chapter intends to answer such questions comprehensively.

Chapter Two: Academic Discussion on Cyber Deterrence

2.0 Introduction to Chapter

This chapter defines cyber deterrence and its relevant concepts, sheds light upon the pertinent literature, and identifies the gap therein. The main purpose of the chapter is to examine the efficacy of cyber deterrence within the confines of classical deterrence and technical vulnerabilities in cyber systems and networks, and to lay out the limitations of classical deterrence in informing cyber deterrence against cyberattacks and cyberwar. To this end, the chapter answers important questions: Why is there a need to develop or use an alternative theory to better inform cyber deterrence and explore its efficacy in the prevention of cyberwar between the U.S. and China? How does conventional and nuclear deterrence wisdom apply to relatively new cyberspace? Why does classical deterrence fall short of meeting the challenge of cyberwar? What are the restraints that cyberspace or cyberwar impose upon classical deterrence that render cyber deterrence ineffective? And what are possible solutions already available to increase the efficacy of cyber deterrence?

2.1 Cyber Deterrence

The link between cyberwarfare and deterrence strategy has increasingly become a focal point of numerous scholars. Many began exploring new ways to implement the basics of classical deterrence theory to the cyber area so as to successfully deter cyberattacks and cyberwarfare

(Lupovici, 2011, pp. 49-51). This provided impetus for the development of what Goodman, and various other scholars, refer to as "cyber deterrence theory" (Goodman, 2010).

The origins of cyber deterrence date back to Operation Desert Storm in 1991, when the idea of a "Revolution in Military Affairs" gained popularity. During the early stages of the operation, the U.S. waged "information warfare" (IW), described by D. Betz as "a potential weapon in its own right" (Betz, 2006, p. 508), against the Iraqi government, paralyzing its military communications networks. This situation revealed the significance of cyber deterrence. In the 1990s, scholars provided firm foundations for the study of deterrence and IW, and concentrated more upon "the use of perception management than with digital attacks on information infrastructures." After the cyber occurrences in the late 2000s, such as the cyberattacks on Estonia in 2007, scholars' attention turned to deterring cyberattacks, or "cyberwar," that have strategic and political ends (Stevens, 2012, pp. 149-151).

At this point, there is utility in defining cyberattack because the notions of *cyberwar* and *cyberattack* are usually used interchangeably, prompting a great deal of controversy. In this study, cyberattack refers to the utilization of computer codes by adversaries for the purposes of interfering with "the functionality of a computer system" or network, including those of governments and military services, to achieve strategic and political advantages by disrupting those networks and systems, such as knocking them offline, or entirely destroying them. (Stevens, 2012, p. 151; Kello, 2013, p. 19; Eun & Abmann, 2016, p. 347). The adopted definition of cyberwar in this study will be provided in chapter three. For now, cyberwar refers to "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption" (Clarke & Knake, 2010, p. 6).

The term “cyber deterrence” entails two components. First, the notion of “cyber” needs to be clarified. Joseph S. Nye defines the concept “cyber” as “a prefix standing for electronic and computer related activities” (Nye, 2011, p. 122). The second component, “deterrence,” is already addressed above. With that in mind, W. Goodman provides a useful definition of “cyber deterrence.” For him, just as in other deterrence forms, cyber deterrence is to dissuade attackers from taking aggressive actions in cyberspace (Goodman, 2010, p. 107). T. Stevens offers a more specific description of cyber deterrence, with an emphasis on the deterrence strategy generally perceived among states or its components. The purpose of deterrence is the hindrance of cyberattacks through persuasion of the potential challenger that such attacks would yield unfavorable outcomes (Stevens, 2012, p. 151). Urging the need to include cyber mediums in defining cyber deterrence, Lupovici offers a definition of the term, with an emphasis upon the use of means--both kinetic and cyber--in order to deter cyberattacks (Lupovici, 2016, p. 325). Lupovici’s description is at odds with the adopted principle of “retaliation in kind” since the kinetic means is involved for retributory purposes. The significance of this principle is acknowledged in Richard J. Harknet’s observation that, “At its core, deterrence theory rests on the principle of retaliation in kind…” (Harknet, 1996, p. 102).

As with classical deterrence, communication, credibility, and capability are three essential components of cyber deterrence theory. Firstly, nation-states employ the strategy of deterrence for the protection of an interest. In order to deter adversaries from posing threats to the interest, a nation-state announces its “deterrent declaration” (Goodman, 2010, p. 105). The deterring party must be able to effectively communicate this declaratory deterrence strategy to other nations, especially its opponents, by unequivocally demonstrating what its redlines are and, therefore, what is acceptable and what is not. Important to cyber deterrence is also the ability of the defender to properly signal intent and capability, not only in times of war but also in peacetime. Secondly, operating in conjunction with communication is credibility. The deterring party does not just draw redlines and urge others not to cross them. It must certainly take a punitive action against an adversary if a declared redline has been crossed. Failure to do so will result in a loss of credibility not only in the eyes of its adversaries but also of the international community (Iasiello, 2014, p. 56). Lastly, capability is the deterrer's means of either punishing the challenger or denying the benefits it can accrue from the attack, or both (Goodman, 2010, pp. 105-106).

With that being stated, the authors studying cyber deterrence appear to overwhelmingly concur that cyber deterrence, as with classical deterrence theory, usually have two main strategic components to be implemented by nation-states so as to deter adversaries: A) *deterrence by denial;* and B) *deterrence by punishment or retaliation* (Libicki, 2009, p. 7; Geers, 2010, p. 299).

2.1.1 Deterrence by Denial

Deterrence by denial means the deprivation of the would-be offender of possible gains or benefits to be attained through cyberattacks or the persuasion of the putative challenger that cyberattacks will not yield desirable outcomes (Kugler, 2009, p. 327). While cyber deterrence by punishment rests upon the fear of retaliation (Glaser, 2011, p. 2), deterrence by denial, on the other hand, aims at lowering the benefits an attacker seeks to gain via enhancing defensive measures to protect computer systems and networks (Jasper, 2015, p. 69). Thus, the purpose of deterrence by denial is the persuasion of adversaries that due to the robust defensive measures in place, they will not gain benefits equivalent to the cost of aggression (Philbin, 2013, pp. 2-5). Deterrence by denial is regarded as the defensive facet of the strategy of deterrence and is, according to Goodman, composed of two fundamental elements: futility and prevention. While the former is to demonstrate that the aggression will not have “the desired effect on the target,” the latter is to show that the defense-based measures will cause the disruption of the cyber offense, thus hindering it from achieving its objectives (Goodman, 2010, p. 106).

Given the challenges, to be addressed below, such as the single-use feature of cyber weapons and the problem of attribution, that complicate the strategy of deterrence by retaliation, some scholars emphasize the importance of the strategy of deterrence by denial and, thus, see more prospect of success with it (Adams, 2001; Lynn, 2010; Elliott, 2011). Drawing attention to the significant role defensive cyber capabilities can play, Lieutenant Colonel Scott W. Beidleman points out that not only do defensive measures lessen the severity of consequences of cyberattacks, but they also enhance a state’s ability to resist attacks and fortify the security of cyber infrastructure (Beidleman, 2009, p. 18). By the same token, Libicki remarks that effective cyber defenses can enhance deterrence posture by adding credibility. “The better one’s defenses…the less often a cyberdeterrence policy will be tested.” He lists several benefits of good cyber defenses. First, a good cyber defense makes an attack less effective. Second, a robust cyber defense establishes credibility of the threat of punishment. Third, good cyber defenses can distinguish third-party cyberattacks from relatively more sophisticated state-executed ones, thus facilitating attribution (Libicki, 2009, pp. 73-74). These benefits listed above lead the defensive facet of cyber deterrence to become the central approach (Jensen, 2012, p. 807).

Across the literature that discusses deterrence by denial, one can find differing conceptualizations and typologies. Some scholars divide deterrence by denial into “deterrence-by-resistance” and “deterrence-by-resilience.” Deterrence by resistance is, by nature, “defensive” (Thijssen, 2016, p. 6); its efficacy lies in “the pre-event as defense” (Bendiek & Metzger, 2015, pp. 560-561). It is meant to convince the potential cyber attacker that aggressive actions will not be effective (Thijssen, 2016, p. 6). K.A. Taipale, however, argues that defensive measures increasing the cost of an attack and lowering the potentiality for significant gains represent conventional cyber-defense posture, which has "residual deterrent effects" (Taipale, 2010, p. 36). Although always improvable, defensive parameters cannot be perfected. That is, the deterrer may make it difficult, in terms of the amount of time and effort required, for an aggressor to intrude into networks, yet it cannot preclude the attacker from breaching a system eventually (Solomon, 2011, p. 20). For that reason, various scholars and experts accentuate the imperative to switch from a "fortress" to a "resilience" posture in deterring cyberattacks and cyberwarfare (Bologna, Fasani, & Martellini, 2013, p. 53). For example, William J. Lynn, the former U.S. Deputy Secretary of Defense, maintains that the U.S. does not have the luxury of retreating behind a "Maginot Line of firewalls" because cyberwarfare bears resemblance to "maneuver warfare" (Lynn, 2010, p. 99). According to J. L. Caton, the importance of shifting to the resilience approach is also evident in both the White House cyber deterrence policy and the most recent NATO Policy for Cyber Defense (Caton, 2013, pp. 155-156).

Deterrence by resilience denotes the durability of a state's cyber systems; it supplies alternative capabilities and systems, and enables systems to recover swiftly (Tran, Campos-Nanez, Fomin, & Wasek, 2016, p. 29). In counterpoint to the preventive, passive defense measures, such as antivirus software, firewalls, and patches (Mudrinich, 2012, p. 181), deterrence by resilience is a "holistic" approach adaptable to various type of cyberattacks (Bologna, Fasani, & Martellini, 2013, p. 53). Because deterrence by resilience is "a latent deterrent" that allows one to combat across "a degraded environment" (Trujillo, 2014, p. 47), it stipulates "response, recovery, and restorative action" (Bologna, Fasani, & Martellini, 2013, p. 54). From Taipale's standpoint, cyberattacks on a resilient system will be futile. This futility can be actualized by two sub-strategies employed under deterrence by resilience.

The first sub-strategy is *redundancy*. A redundant system prohibits cyber attackers from rendering the entire system non-functional. Even though cyberattacks could be able to succeed in shutting down some fragments of the system, redundancy will allow the system to function through substitute systems (Taipale, 2010, pp. 36-37). For example, it is said that the U.S. is prepared for potential cyberattacks that may have crippling effects on both industrial sectors and government by reserving bandwidth for strategic purposes (Jensen, 2012, p. 815).

The second sub-strategy is *recovery* (Taipale, 2010, p. 36). Some scholars also refer to it as “reconstitution” or “antifragility” (Jensen, 2012, p. 815; Schearer, 2016, p. 8; Thijssen, 2016, p. 15). Potential cyber aggressors would be deterred if the system is capable of rapidly recovering its capabilities and any cyber infrastructure damaged or destroyed in the first cyberattack. Implicit here is that the attack will have negative effects upon the victim; and yet the potential benefits the would-be-attacker sought to gain will be diminished through the victim’s ability to recover swiftly (Taipale. 2012, pp. 37-38).

At this point, it is worth noting that the idea of active defense is incorporated into cyber defense strategies. Central to the concept of active defense is “the proactive detection, analysis and mitigation of network security breaches in real-time combined with the use of aggressive countermeasures deployed outside the victim network.” Active defense spans various proactive measures, such as honeypots (to be discussed below), and encompasses a wide range of strategy. In Scott Jasper’s view, for the private sector in the U.S., active defense means cooperation with cybersecurity providers for the detection of cyber intrusions (Jasper, 2015, p. 73). However, various pundits note that active defense carries a high risk of escalation and causes ethical problems due to its potential impact upon innocent third parties. Hence, this strategy has been subject to valid criticisms, leading many scholars and experts to conclude that the application of immediate deterrence through active defense is ill-suited (Libicki, 2009, p. 61; Morgan, 2010, p. 66; Mudrinich, 2012, p. 182; Caton, 2013; Bendiek & Metzger, 2015, pp. 562-563). In place of active defense, it is suggested that deterrence by resilience for the defense of critical cyber infrastructure ought to be focal point of decision-makers (Caton, 2013).

Deterrence by denial also entails the strategy of making networks and systems interdependent. The would-be challenger would fear the odds that it would harm itself by attacking systems and networks upon which it also relies (Taipale, 2010, p. 39). For example, E. T. Jensen writes that while the Bush administration considered executing crippling cyberattacks on financial networks used by Saddam Hussein in the course of the invasion of Iraq in 2003, this idea was abandoned. The U.S. was deterred from carrying out cyberattacks on these networks because of the fear of the potential cascading effects of such attacks on global financial networks. This deterrence strategy not only works well between trading partners but also between possible cyber opponents. For instance, China recently has become a significant trading partner of the United States. A significant portion of financial transactions between the two states is through computer-networked systems. This economic interdependence, according to Jensen, greatly deters China from conducting crippling cyberattacks on the U.S. economy, but does not dissuade China from conducting cyber espionage on the private sector in the United States (Jensen, 2012, pp. 820-821).

Here, it is important to open a parenthesis to emphasize that this study does not offer deterrence by economic and political entanglement in the above context. China is likely to carry out cyberattacks on the U.S. upon the simultaneous presence of the two critical variables: China’s dissatisfaction and its reaching a parity of offensive cyberwar power with the Unites States. Rather, this paper suggests deterrence by economic and political means in the sense that such strategies will likely lead to political convergence, thus marginalizing the areas of disagreement between the two parties, which will, in turn, increase the level of satisfaction of China with the existing status quo in cyberspace.

Returning to the discussion of deterrence by interdependency, Taipale notes that in the kinetic world, the interdependency approach was apt for “the generally symmetric state-on-state conflicts;” however, in the cyber environment where actors are highly networked to each other, the strategy of dependency provides numerous opportunities and offers a higher prospect of success (Taipale, 2010, p. 39). In this regard, Jensen points to the ’recognition of the Department of Defense (DoD) of the importance of creating digital interdependency and interconnectedness with other countries since such dependency can pave the way for “situational awareness” across nations. This may encourage states to collectively defend themselves and deter potential aggressors (Jensen, 2012, p. 820).

2.1.2 Deterrence by Punishment or Retaliation

The other main deterrence strategy is *deterrence by punishment or retaliation*. This method is the offensive facet of deterrence (Goodman, 2010, p. 106) and, thus, refers to the use of credible threats of the imposition of intolerable losses, costs, and risks upon the aggressor. Its chief purpose is to persuade the opponent that the cost from retaliation would exceed “expected” benefits sought through cyberattacks (Kugler, 2009, p. 327).

R. L. Kugler articulates “deterrence by offering incentives for adversary restraint” as a third strategy along with denial and punishment in pursuit of deterrence. This third strategy rests upon the persuasion of the opponent that not taking deleterious action will culminate in “an acceptable, attractive outcome" (Kugler, 2009, p. 327). Similarly, Goodman mentions the notion of "reassurance" as an important component of an effective deterrence strategy. Reassurance can be in many forms. It can be mutual security assurances or in the form of various types of assistance (Goodman, 2010, p. 107). It should, however, be noted that this study, as have many other studies, regards deterrence by denial and deterrence by punishment as the two integral components of an effective cyber deterrence and categorizes other forms of deterrence strategies into sub-strategies employed under deterrence by denial or deterrence by punishment.

Just as in classical deterrence theory, cyber deterrence requires that punitive measures be immediate, certain, and severe. In other words, consequences of retributory actions must be "incontestable." While immediacy, or "celerity," connotes the promptness of retribution, certainty means how likely the potential attacker will be punished. Ultimately, severity refers to how costly the counter-attack will be to the potential offender. That is, in order to deter effectively, the deterrer must make sure that the cyber culprit is persuaded that it will be "identified," "caught," and, then, "punished" in a prompt and severe manner. However, owing to the difficult-to-deal with problems caused by the intrinsic characteristic of the cyber domain, such as the attribution problem, the ambiguity of attackers' motivations, and its unbounded and abstract essence, the employment of "orthodox" concepts of classical deterrence theory to the cyber venue will confront significant challenges, thus problematizing cyber deterrence (Taipale, 2010, p. 18).

The classical deterrence concepts of "interdependency" and "counterproductivity" were also incorporated into cyber deterrence by punishment. Interdependency refers to the commonality of interest between the attacker and defender. The cost of an attack will increase if the deterring and attacking parties have more shared interests. Counterproductivity is the deterrer's persuasion of the attacker that attacks aiming at accomplishing tactical objectives may result in the frustration of broader normative or strategic objectives. As an illustration, Goodman states that terrorists might be dissuaded from carrying out suicide attacks if the U.S. adopted a policy of punishing the families of these terrorists. However, not only would this policy be detrimental, or “normatively counterproductive,” to the U.S., but it also would adversely affect larger U.S. objectives--that is, “strategically counterproductive” (Goodman, 2010, p. 106).

Deterrence by denial and deterrence by retaliation can be applicable singly or simultaneously in cyberspace. Libicki maintains that cyber deterrence can be more effective when both strategies are employed concurrently (Libicki, 2009; Kugler, 2009, p. 327). Beidleman suggests that for deterrence to work, the U.S. must adopt a cyber deterrence strategy encompassing at least the simultaneous employment of both offensive and defensive cyber capabilities (Beidleman, 2009, p. 2). Correspondingly, Kugler writes that in a bid for deterring cyberattacks, the United States could develop a robust cyber defense and, at the same time, utilize its cyber-offense power to carry out cyberattacks on the aggressor’s digital networks. However, he also urges that neither cyber offenses nor cyber defenses should be contained to the technical domain of cyberspace, such as an adversary’s information networks, but that one should also use economic and political instruments (Kugler, 2009, pp. 327-328). This point is important to stress because it directly reinforces the argument of this study that cyber deterrence has a flexible nature and includes a wide array of response options from political and economic to strategic ones.

The assumption of rationality is also important to cyber deterrence. Underscoring the significance of *rationality* as one of the assumptions needed for a successful deterrence, Richard J. Harknett states that a would-be offender’s’ decision calculus is presumably made on a rational basis. In theory, the potential cyber aggressor is deterred if the cost-benefit calculation of attacking favors the former or if the benefits of restraining from an aggressive cyber action exceed its costs.

For that reason, crucial to deterrence is “the proper communication of those potential costs to the challenger” (Harknett, 1996, p. 97). Even though potential costs are properly communicated to would-be challengers, Goodman cautions that not all decisions to conduct or restrain from cyberattack are taken rationally due to the lack of flawless information about the possible conflict scenario (Godman, 2010, p. 107). This fact may lead to miscalculation and, as a result, the failure of deterrence (Harknett, 1996, p. 97).

In this paper, cyber deterrence refers to, as Patrick M. Morgan puts it for deterrence in general, “a matter between states” (Morgan, 1997, p. 20). This feature of deterrence is consistent with this study since it aims at exploring the efficacy of cyber deterrence in preventing cyber warfare between two states, namely China and the United States. Martin Libicki provides a useful rationale for this reductionist approach to cyber deterrence, noting that for retaliation in kind to succeed, the deterring state ought to be able to hold the offender’s valuable information networks at risk. Corporations as non-state actors have seldom been accused of being cyber culprits, thus rendering them of little importance in an analysis of this sort (Libicki, 2009, pp. 25-26). However, one caveat is that this assumption may be challenged since cyberspace enables non-state actors to be significant players in the playground.

Having laid out the main elements of cyber deterrence, crucial questions in the cyber deterrence literature remain to be answered: Whether cyber deterrence informed by the study of the nuclear and military deterrence can successfully be applied to the cyber domain; and, if so, how. If they cannot be applied, then what are the key challenges of the cyber domain that impose significant restraints upon the applicability of classical deterrence concepts to cyber deterrence? How can one differ cyber deterrence from classical deterrence? What are possible ways of increasing the efficacy of cyber deterrence?

2.2 Hurdles to Effective Cyber Deterrence

The bulk of the studies exploring the efficacy of cyber deterrence appear to conclude that the application of classical deterrence theory to the cyber domain faces salient challenges, significantly limiting the effectiveness of cyber deterrence (Denning, 2015, p. 11). For example, Stevens writes that cyber deterrence does not accommodate Patrick Morgan's six criteria of classical deterrence theory. Firstly, states are not in severe military conflict in the cyber venue. Secondly, the assumption of rationality in classical deterrence theory does not apply to cyberspace because of the multitude of non-state entities operating in the cyber domain. Thirdly, the credibility of threat of retaliation diminishes due to the problem of attribution. Fourthly, no state can be sure that it can incur "unacceptable damage" on one another in the cyber area owing to the inability to put an opponent's assets at risk in a repetitive way. Fifthly, credibility is undercut for several reasons, such as the likelihood of collateral damage. Lastly, stability is hampered due to the increased chance of escalation in cyberspace (Stevens, 2012, p. 152). While many challenges with regards to deterrence of cyberattacks stem from technical issues inherent in cyber space (e.g. the attribution problem), some are not entirely new and, thus, pose "comparable challenges." As an illustration, conveying threatening messages about one's capability and credibility faces significant challenges in the kinetic world just as it does in the cyber sphere; and yet these challenges are more perplexing and even further amplified in the cyber domain due largely to the increased number of non-state cyber threat actors, such as individuals (Bendiek & Metzger, 2015, pp. 556-557).

Lupovici aptly observes that the difficulties mentioned above are associated with the three most significant conditions necessary for deterrence to work in an effective fashion--that is, how credible the threat is; capability; and communication (Lupovici, 2011, p. 49). If these three essential components of deterrence cannot be employed properly and effectively, neither deterrence by denial nor deterrence by retaliation can succeed simply because the successful application of these two deterrence strategies relies upon them. Having stated that, the bulk of literature tends to study the impediments to an effective cyber deterrence by separately examining the obstacles to deterrence by retaliation and by denial (Geers, 2010; Jensen, 2012). For the sake of clarity and simplicity, this paper, too, follows the same pattern to shed light on the cyber deterrence literature.

2.2.1 Impediments to Deterrence by Punishment or Retaliation

Some scholars and experts note that the internet is a global infrastructure that a massive number of individuals rely upon. Because the internet was designed to promote collaboration and constant expansion of accessibility, security concerns were deemed secondary. As a result, it is said that offense technically has a greater advantage over defense in cyberspace. For example, Lynn III asserts that savvy hackers will always be able to detect vulnerabilities and surmount security measures taken to prevent intrusions into systems. Thus, the ability of the U.S.' opponents to exploit vulnerabilities in its networked-systems may always be one step ahead of the U.S.` ability to protect its systems. Core to the argument is that "in an offense-dominant environment, a fortress mentality will not work" (Lewis, 2010, p. 57; Lynn, 2010 p. 99). By extension, cyber defense is regarded more problematic than conventional military defense strategy in that executing cyberattacks is inherently "costless," thus encouraging cyber attackers to inexorably test cyber defenses (Glaser, 2011, p. 2).

However advantageous offense in the cyber venue seems to be over defense, it is not without problems. Many scholars list numerous major challenges to deterrence by retaliation that significantly lessen the effectiveness of cyber deterrence. Those challenges are: The attribution problem regarding the source of the attack and anonymity of the attacker; the difficulty of signaling capability and intention; the uncertainty about scale and severity of the damage done through cyberattacks; the asymmetric nature of cyberspace; diminishing return on consecutive cyberattacks; the impracticality of cyber disarmament; third parties engaging in cyberattacks; the difficulty of establishing threshold to retaliate; legal issues (proportionality and "dual-use" objects); and ultimately the escalatory nature of cyberwarfare or cyberattacks. Each of these factors will be individually addressed below.

2.2.1.1 Attribution Problems

Of those scholars enumerating the challenges to cyber deterrence, Libicki stands out. He makes a "sophisticated" contribution to the study of cyber deterrence (Stevens, 2012, p. 151) and contends that cyber deterrence must be approached "on its own merits" as it greatly differs from nuclear or military deterrence. Thus, it may not work in the way that classical deterrence theory did during the Cold War epoch. With that aim, he lays out nine problems that may render cyber deterrence by retaliation futile, with three problems being critical and the rest six being "ancillary" (Libicki, 2009). Of the critical three, the attribution problem holds center stage in the discussion of cyber deterrence by retaliation (Jensen, 2012, p. 785).

The internet was designed in a way that neither the identification of the server where the cyberattack was launched nor the cyber aggressor can, in most cases, be known. Due to the architecture of the internet and its being a "borderless medium" (Goldsmith & Wu, 2006, p. vii), the anonymity of the cyber offender does not appear to be a "transient problem" (Hollis, 2011, p. 378). John Markoff points out that for some cyberwarfare scholars, the internet refers to a "wilderness of mirrors" (Markoff, 2009, p. 5). In consequence, the attribution problem tends to be portrayed, in the literature, as a crucial limiting factor for an effective cyber deterrence, specifically for deterrence by retaliation. In the cyber domain, the offender expects a certain level of "impunity." Therefore, it is believed that no cyber deterrence strategy may be effective in the prevention of cyberattacks that are viewed as "free rides" (Kugler, 2009, p. 326) because of the uncertainty of the identity of attacker, which will undermine credibility of the threat by retaliation, irrespective of how capable the retaliator is, thereby making deterrence ineffective (Geers, 2010).

Because the general tendency in the literature is to present the attribution problem as a major hurdle to deterrence, it is imperative to cover it in detail. In cyberspace, the uncertainty in attributing the source of an attack can complicate deterrence in various ways (Lynn, 2010, p. 99). To begin with, the nuclear strategy adopted by the U.S. assumes that the origin of a nuclear attack on the U.S. soil can be traced through the delivery mediums of attackers (Elliott, 2011, p. 37). In other words, it would have been generally evident "who did it" during the nuclear standoff between the superpowers (Libicki, 2009, p. 40). To the contrary, in cyberspace, the source of malicious cyber actions, or who is liable for them, often remains unknown (Lin, 2016, p. 77); "whereas a missile comes with a return address, a computer virus does not" (Lynn, 2010, p. 99). The attacker can be mostly anonymous (McReynolds, 2015). Because "deterrence is a state of mind" (Beidleman, 2009, p. 16), the cyber culprit must be certain that the target will correctly detect it and, therefore, fear retaliation, for deterrence to be successful. This plays a critical role in a successful retaliation (Libicki, 2009, p. 41). However, due to the technical difficulties intrinsic to the cyber domain, cyber aggressors can readily conceal their identities, minimizing the credibility of the deterring party, which, in turn, renders cyber deterrence ineffective. Even if the deterring party has been able to identify the origin of the attack and the identity of the cyber offender through technical mediums, such as an internet protocol (IP) address and a user name, these technical means may not lead to a "smoking gun" indicating the actual attacker. This may be because the cyber aggressor may have employed "deceptive or misleading attack signatures," such as the use of compromised computers in a botnet diverting the source of the attack, thereby effectively concealing identity (Solomon, 2011, p. 5). It may also be the case that the target may not have even realized that it was under cyberattack but may have, instead, incorrectly ascribed the problem to "error or malfunction" in computer systems (Hollis, 2011, p. 378).

Moreover, cyberattacks can be launched from anywhere and by anyone (Certoff, 2010). Thus, in contrast to nuclear warfare strategy, cyberwarfare increases the likelihood of successfully conducting a surprise attack (Geers, 2010, p. 300). For example, cyberattacks can emanate from the hijacked computer of a third party and even from a library with a Wi-Fi connection. They can also be orchestrated by a multitude of cyber actors as opposed to the very limited nuclear threat actors active during the Cold War era (Libicki, 2009, pp. 42-44). According to E. Iasiello, it is anticipated that over 140 states aspire to possess cyber capability and that over 30 states are in pursuit of forming cyber units within their militaries (Iasiello, 2014, p. 54). Consequently, Libicki aptly observes that it is, unlike the Cold War era, hard to demonstrate "a *single* dominant threat." Not only states but also non-state actors should also be under consideration as potential cyber threat actors; hackers sponsored by states or individual hackers can also execute cyberattacks, which, in turn, muddles efforts to detect cyber perpetrators (Libicki, 2009, pp. 42-44). To illustrate, there is still no persuasive proof that Russia was involved in the cyberattacks against Georgia while the two states were in a military conflict in 2008 (Deibert, Rohozinski, and Crete-Nishihata, 2012,

p. 17). To mitigate the negative effects of the multiplicity of cyber threat actors and "provocations" on attribution, some scholars offered "tailored deterrence," defined as a strategy considering "the specific predilections of each individual adversary and its conduct" (Kugler, 2009, p. 325). In other words, deterrence strategies are tailored to specific circumstances, threat actors, capabilities, and lastly communications (Bunn, 2007, p. 1).

Further complicating and deepening the attribution problem is the possibility of misattribution of an attack and, thus, the punishment of innocent states, as well as the necessity of persuading third parties that the retaliation is not an act of aggression but, in fact, is a justified act of defense (Libicki, 2009, pp. 42-45). First, the obfuscation of one's identity is possible in the cyber terrain. For example, the cyber attacker may have routed cyberattacks via hijacked computers in its adversary state with whom the deterrer also has strained diplomatic ties. In this case, the actual attacker is likely to assert that its computer has been compromised and, therefore, has nothing to do with the attack. This is called "plausible deniability" (Geers, 2010, p. 301). The unwillingness of the third party to cooperate with the deterrer over the investigation of a given cyber occurrence may be interpreted as a sign of "guilt," thereby causing the misattribution, which, in turn, diminishes the effectiveness of cyber deterrence. Libicki notably draws attention to the odds of undermining the efficacy of deterrence by misattributing an attack and, as a result, punishing a wrong party, which, in turn, may create a new adversary. More importantly, he views "false-flag operations" as "the more serious threat to a successful retaliation" (Libicki, 2009, pp. 43-44).

Contrary to the Cold War era nuclear standoff between the USSR and the U.S., convincing third parties prior to reprisal has grown in importance. Knowing that it had attacked, the cyber aggressor may not question the legitimacy of the retaliation. The deterrer is also mindful of the situation, but third parties are not aware of what has occurred (Libicki, 2009, p. 42). The deterrer state must be in possession of a certain level of evidence prior to taking any retributory action against the putative cyber offender, evidence which could be very challenging to acquire (Shamsi, Zeadally, Sheikh, & Flowers, 2016, p. 2890). Cyber tools, or weapons, can readily traverse several "jurisdictions," making the acquisition of forensic proof following cyberattacks an onerous task in the absence of effective cross-border cooperation (Kello, 2013, p. 33). Ironically, in efforts to provide the aggressor and the international community with evidence that indicates "conclusive attribution," the deterrer is believed to serve the aggressor by informing it of how to conceal its identity in a more effective way next time around (Hare, 2012, p. 128). As a consequence of this, in the words of Geers, "cyber investigations typically end at a hacked, abandoned computer, where the trail goes cold," thereby foiling deterrence (Geers, 2010, p. 301).

There also exists a time dilemma concerning the attribution of cyberattacks. In a short time, even with well-equipped and organized teams, examining "a well-executed" cyberattack and determining the best course of action thereafter may face profound difficulties due in part to the pace of political developments and pressure upon decision-makers. Thomas Rid and Ben Buchanan suggest that more time should be available for a more accurate attribution (Rid & Buchanan, 2014, p. 32). However, ironically, the more time passes to collect evidence, the less legitimate the retaliation becomes insofar as the execution of retributive action may not be regarded as "self-defense" but as "armed reprisal," which is proscribed by international law (Lupovici, 2016, p. 329). Therefore, not being able to provide persuasive attributive evidence in a timely enough fashion to retaliate may weaken the legitimacy of the defender, limiting available options upon the deterrence's failure (Kello, 2013, p. 33). This is, to a great extent, not the case in the kinetic realm.

As formidable as the problem of attribution is portrayed by a considerable number of pundits, that is not to say that attribution never occurs and that all cyber aggressors remain anonymous. The source of attack can, for instance, be attributable due to "dumb mistakes" of cyber perpetrators (Hollis, 2011, p. 399). Cyber aggressors may have conducted a cyberattack through an IP address associated with the state, thus revealing their identity. A source of an attack can also be attributable because of a state executing a large number of Computer Network Exploitation (CNE) operations, leading to the disclosure of its "modus operandi," which, in turn, unfolds its identity. Additionally, the cyber offender may simply divulge itself or may confess that it carried out the attack, which also ends the attribution problem (Libicki, 2009, pp. 48-51). Besides, Kugler notes that the problem of attribution may be trivial upon the application of cyber deterrence to "attributable" cyber aggressors of the U.S., such as China (Kugler, 2009). However, David Elliott seems skeptical of this position and argues that inferring an attacker's identity based on "the global-security situation at the time" is not a strong point of departure for attribution and retaliation (Elliott, 2011, p. 38).

Some authors assert that the problem of attribution is not about technical issues inherent in the very design of the internet whatsoever, but rather, that the problem stems from "the space of law, regulation, multi-national negotiation, and economics" (Clark & Landau, 2011). Emilio Iasiello writes that focusing merely on technical analysis may be a misstep in attributing an attack. Instead, melding the analysis of cognition, behavior, and technique of the cyber offender can be an ideal way to begin a successful attribution (Iasiello, 2014, p. 58). Similarly, other scholars take a constructive approach and seek a solution to the attribution problem outside the technical domain (Stevens, 2012; Rid & Buchanan, 2014; Lupovici, 2016). For instance, Rid and Buchanan maintain that beyond technical difficulties, the problem of attribution is "what state makes of it." Human factors, such as the quality of leadership, play a crucial role in attributing the source of cyberattacks. It is also up to governments to determine "how to do attribution" and when doing attribution is beneficial and when it is not (Rid & Buchanan, 2014, p. 30).

With the opposing voices hinted at, the bulk of scholars studying the problem of attribution, assert that it remains a major hurdle to a successful employment of cyber deterrence. In parallel to this line of thought, Libicki remarks that attribution may not become easier in the future (Libicki, 2009, p. 49).

2.2.1.2 The Problem with Signaling Intention and Capability in the Cyber Venue

The emphasis upon the significance of signaling intentions and capabilities to one's opponents in cyberspace is pervasive in the cyber deterrence literature (Libicki, 2009; Jensen, 2012, p. 787; Iasiello, 2014, p. 57). By nature, signaling encompasses interplays between a rivalry dyad across space and time. These interplays can take many forms. For example, in order to signal its discontent to the USSR in the Cold War epoch, the U.S. put its strategic bombers at a higher alert since it knew that Soviet Russia's intelligence means would detect this activity and accurately construe it (Rice, Butts, & Shenoi, 2011, p. 58). Here, to what extent a defender can effectively and clearly signal its capabilities and intentions to protect an interest in times of peace and conflict will strongly influence the effectiveness of deterrence (Jensen, 2012, p. 787). Despite the fact that some authors promote the viability of applying the sorts of conventional signaling strategies employed during the Cold War period to cyberspace (Rice, Butts, & Shenoi, 2011), it is widely held by various scholars and experts that signaling in cyberspace is more perplexing and problematic than signaling in the kinetic realm for several reasons.

For deterrence to work, it is imperative that the deterrer can demonstrate its capacity to use force (Bendiek & Metzger, 2015, pp. 558-559). For instance, in the kinetic world, only after the demonstration of the devastating effect of nuclear weapons at Hiroshima and Nagasaki in the 1940s could the world be convinced of the scale of destruction of which nuclear weapons were capable (Elliott, 2011, p. 36). A corresponding display of cyber capabilities is not, however, a viable option insofar as cyber means rely upon what is called "zero day" vulnerabilities in computer-oriented systems. Publicly revealing those cyber weapons to demonstrate capability to use force will render them useless when and if the vulnerabilities to be exploited by cyber tools are closed (Lindsay, 2015, p. 53). This brings us to "use and lose" dilemma, meaning that demonstration of cyber capabilities cannot dissuade "because convincing evidence of the capacity to inflict harm is itself useful information in nullifying the threat" (Gartzke, 2013, p. 60). In consequence, the short-lived nature of cyber offensive tools complicates signaling, a necessary element for deterrence by retaliation (Lindsay, 2015, p. 53).

Secondly, it is believed that instead of revealing themselves to demonstrate their capability to deter, cyber actors tend to stay anonymous simply because of the problem of attribution helping them avoid being retaliated against. This fact diminishes the utility of displaying capability. Also, notifying an opponent that its specific cyber systems are going to be targeted or have already been infiltrated will be counterproductive since such signaling will mobilize the opponent to take necessary measures, such as moving its servers to another platform to safeguard its systems or networks. Thus, it is rarely regarded as a useful strategy to signal an intended target in the cyber sphere (Jensen, 2012, pp. 788-789).

Lastly, the defender's resolve to respond necessitates an indubitable signaling of the interest that will be protected, but signaling in the cyber sphere becomes problematic given the multiplicity of cyber actors. Unlike the Cold War era, when potential threat actors were mainly limited to the major powers, cyberspace presents multiple potential challengers, including individuals and private sector actors, thereby making signaling more complicated, which, in turn, hampers deterrence (Bendiek & Metzger, 2014, p. 559).

2.2.1.3 Other Major Challenges to Cyber Deterrence by Retaliation

2.2.1.3.1 The problem of uncertainty about severity and scale of damage from cyberattacks

During the Cold War, neither the scale of attack nor how severe it was as ambiguous as are they in the cyber domain. To illustrate, a car bomb undoubtedly inflicts less harm than does a truck bomb, or following a nuclear blast, the damage done could be calculated. In essence, in the kinetic world, the battle damage evaluation of a specific type of attack was possible, and counter measures could be taken in accordance with the projected harm to be suffered (Taipale, 2012, p. 19).

In contrast to the physical world, in cyberspace, retaliation faces the difficulties of assessing the intended battle damage (scale and scope) in advance due to the "unbounded and abstract" characteristics of cyberspace, which complicates efforts to signal the capability and intention of the deterrer effectively (Libicki, 2009, p. 52; Taipale, 2012, p. 19).

First, in the kinetic world, the calamitous result of nuclear weapons remained unchanged (Taipale, 2012, p. 19; Geist, 2011, p. 51). By contrast, in cyberspace, "a radical new cyber weapon with never-before-seen effects could appear overnight" (Geist, 2015, p. 51). Due to the nature of cyberspace that permits reciprocal influences and encourages interdependency by the virtue of the availability of information and the opportunity for exchanges (Morgan, 2010, p. 61), potential reprisals may result in crippling or corrupting more computers of the targeted system than intended. A cascading, subversive effect in any cyberattack is highly possible (Libicki, 2009, p. 53), which may lead to a cyberattack on the scale of an "electronic Pearl Harbor" scenario (Jensen, 2012, p. 790). For example, the case of Stuxnet provided evidence that engineering a potent cyber weapon that did not present risks of infecting the computers of third parties is a difficult task (Geist, 2015, p. 51). Use of a cyber weapon which damages third parties could result in condemnation from third parties and may be perceived by the state subject to the retaliation as a "disproportional" response, which may lead to legal problems as well as to unnecessary "counterescalation," thereby undermining deterrence (Libicki, 2009, p. 53).

Second, because cyber systems may chance from one second to the next, uncertainty as to whether the pre-existing loopholes to be exploited by the retaliator are closed is pervasive (Libicki, 2009). It is said that even though the retaliator has been able to discover vulnerabilities in the networked system of the attacker, these pre-existing vulnerabilities could have been closed soon after the putative attacker had discovered them. The discovery of these vulnerabilities can be in multiple ways. Vulnerabilities in systems may have been discovered by the target, depending partly on the skill of its administrators (Libicki, 2009, pp. 55-57). These loopholes can also be closed by chance--for example, patches may have been installed without the retaliator knowing it (Bendiek & Metzger, 2010, p. 559). Consequently, the retaliator may be fooled into thinking that it successfully exploited these loopholes and retaliated when, in fact, it did not, thus rendering the deterrent posture ineffective since the chief objective of retaliation is to "communicate displeasure" with a desired effect on the attacker (Libicki, 2009, p. 54).

2.2.1.3.2 The problem of the asymmetric nature of cyberspace

The existence of asymmetry between cyber actors is another factor that erodes the credibility and capability of cyber deterrence by retaliation (Geers, 2010, p. 302). While noting that no conventional warfare could entirely be symmetric, Libicki highlights that cyberwarfare is comparatively much more asymmetric, thereby differentiating it from any other conventional war practices (Libicki, 2009, p. 70).

With the wide dissemination of computers and the mounting interconnectedness of information networks across the world, both nation-states and non-state actors, such as hackers, corporations, and terrorist groups, may be in possession of the required technology and skills to engage in a new form of conflict in the cyber area (Wang & Stamper, 2002, p. 171). While for a nation to develop nuclear capability requires spending massive amounts of time and resources, gaining cyber capabilities to strike is much easier and cheaper. To illustrate, with only $700, a hacker with malicious intent can readily make an online purchase to acquire a cyber weapon such as the "Zeus Trojan" or one of its variants, the very viruses that infected more than 70,000 computers in more than 190 countries around the world (Lan & Xin, 2010, p. 1). For that reason, individual hackers and terrorist groups as non-states actors with little time and money spent can possess cyber tools to carry out cyberattacks and cause disruption and damage, including financial damage worth of billions of dollars, thus making cyberspace a highly asymmetric war-fighting zone (Geers, 2010, p. 302). This fact has led many scholars to conclude that offense is inherently more advantageous over defense due in part to the availability of cyber weapons to everyone (Wang & Stamper, 2002, p. 171), a reflection of the "low-cost" and "low-risk" characteristics of cyberspace (Lan & Xin, 2010, p. 1).

Just because states and non-state actors have easy access to cyber weapons does not necessarily mean that they also have computer-based network systems or any “identifiable” cyber infrastructure worth being struck by their targets for retributory purposes (Geers, 2010, p. 302). The degree to which each cyber agent relies upon the networked system or the Internet can markedly differ. For example, some states are relatively more wired than others. Kugler underlines the U.S. vulnerability to cyberattacks owing to its increased dependence on information technology and networks, ranging from military operations to all sorts of public services, such as banking and education (Kugler, 2009, p. 313). Based on that, some commentators argue that less powerful nations, such as China, may benefit from the asymmetric advantages cyberwarfare provides to exploit the U.S. dependence on information systems. To reinforce this argument, they point to the formation of “information warfare units” in China’s military (Kesan & Hayes, 2012, p. 443). With that being noted, core to the point is that the opponent must have valuable cyber assets to lose when retaliated against in kind; provided it does not, the credibility of the threat of retaliation is trivialized, which renders deterrence “inconsequential.” To illustrate, the would-be-cyber challenger may consist of a group of hacktivists, such as Anonymous, scattered across the globe, or the potential cyber offender may be “a cellular-structured terrorist” group situated in various parts of the world. If so, Iasiello poses a meaningful and legitimate question: “[W]hat value point can be leveraged that will have sway over the actions of the entire group?” (Iasiello, 2014, p. 65; Klein, 2015). As Libicki, too, aptly notes, while the distributed denial-of-service attacks (DDoS) incapacitated many government institutions of the digitally connected population of Estonia in 2007, the cyberattacks on less-wired Kyrgyzstan in 2009 did not have the same crippling effect. Then, it follows that unlike in conventional warfare, the asymmetric nature of cyberattack and cyberwarfare makes cyber deterrence through cost-imposition (punishment) problematic by diminishing the credibility of the threat through retaliation because the target may not have valuable cyber assets, or nothing at all, to be hit back (Libicki, 2009, p. 70).

Underscored in the literature is that if targets, such as lone hackers or terrorist groups, have little, or nothing, to lose to retaliation in kind, how can they be deterred? This fact brings up a contentious issue to be addressed below: Retaliating against a cyberattack through kinetic means.

2.2.1.3.3 The problem of diminishing returns on successive cyberattacks

In the Cold War period, mutually assured destruction (MAD) ensured that waging nuclear war against another nuclear weapon-holder would mean the obliteration of all parties (Powell, 1990). This situation cannot be reproduced in cyberspace; MAD concepts are ill-suited to cyberattacks and cyberwarfare (Rash, 2016). In contrast to a nuclear reprisal offense, there is no such cyberattack that is so devastating that all possible cyber aggressors would not take the risk of suffering retaliation (Libicki, 2009, p. 56). Cyberattacks on Georgia and Estonia, for instance, had disruptive rather than destructive effects on targets (Elliott, 2011, p. 36). For that reason, scholars appear to underline the necessity of punishing would-be cyber offenders in a repetitive fashion until the cyber culprits are sure that the chance of accomplishing their goals is very slim, and, as a result, see scaling down their goals in a gradual manner as in their best interest (Blank, 2001, p. 128).

The idea of repeated cyber retaliation derives from the conventional strategy of *serial deterrence*, in which both sides attempt to punish each other until one party learns its lesson. Incorporating an old strategy into cyber deterrence in a novel way, Morgan seems to believe that with the strategy of serial deterrence in effect, cyberattacks can be “manageable” if the defending party inflicts repetitive pain on the aggressor for a long time, prompting the initial attacker to suspend the attack, either permanently or temporarily (Morgan, 2010, pp. 56-59); but in the cyber domain, the efficacy of this strategy is disputable since it faces significant challenges.

First, unlike most of the conventional warfare forms, in cyberspace, the repetitive use of force faces the problem of the diminishing returns on consecutive cyberattacks. The level of impact the first cyber punitive strike had upon the target is most likely to diminish upon the second use of the same cyber tool because cyber offensive tools, contrary to their kinetic counterparts, leverage vulnerabilities in cyber systems permeable to exploitation (Solomon, 2011). These vulnerabilities in the computer-based system of the target are highly likely to have been removed or patched in an expeditious way, particularly in the aftermath of the discovery of a malware already penetrating the system and inflicting damage on it. As such, the problem lies in the ambiguity as to whether the victim successfully fixed "its hitherto-vulnerable systems" following the first retaliatory strike and what a second strike will accomplish. Consequently, as Libicki puts it, "a trick [cyber weapon] taken out of a bag cannot always be put back for use another day," thereby creating the quandary of either use it or lose it (Libicki, 2009, pp. 58-59). For instance, once experts discovered the "zero-day exploits" that Stuxnet leveraged, those defects were studied, possible "antidotes" were generated, and ultimately vulnerabilities in systems were fixed, thus prohibiting Stuxnet from using the same exploits in the future and rendering its use a second time ineffective. The problem of cyber weapons being short-lived mediums is also closely associated with the strategy of signaling one's intention and capability to the potential opponent in cyberspace (Libicki, 2009; Jensen, 2012, p. 788).

Second, another important point pertaining to the problem of repeatability is made by Iasiello. Stressing the escalatory nature of repetitive punitive cyberattacks, he points to the increased risk of the target viewing the retaliatory attack not as "a direct result of the offending action" but as an act of offense. Hence, he cautions that the failure of the target to understand the legitimacy of the reprisal may lead the retaliator to resort more impactful and conspicuous methods in a series of retributory attacks; this act may cause the target to misinterpret the punitive actions, which may, in turn, result in the escalation of the crisis into "a greater cyber conflict," inspiring more attacks instead of deterring attacks (Iasiello, 2014, pp. 65-66).

2.2.1.3.4 The impracticality of the disarmament of would-be cyber attackers

In the literature, scholars broadly concur that classical deterrence is in a sharp contrast with cyber deterrence when it comes to the ability of cyber means or cyberwarfare, as opposed to nuclear weapons or conventional warfare, to disarm potential cyber aggressors (Davis, 2014, pp. 345-346). The impracticality of disarming potential cyber culprits results from the less severe consequences of cyberattacks, and the ubiquity of the Internet and potential hackers (Libicki, 2009, p. 59), as well as the relative ease of acquiring offensive cyber means. For instance, offensive cyber tools can be obtainable through inexpensive online-downloading and be purchasable from "cybercrime markets" (Gartzke & Lindsay, 2015, p. 321).

Furthermore, the cyber domain is not conducive to the sort of disarmament treaties that were effective in the kinetic world because "the very actors that are most threatened by cyber war in one moment benefit from exploitation and espionage in the next." In this light, disarmament of the attacker in cyberspace seems to be "impractical" (Gartzke & Lindsay, p. 321). This impracticality of cyber disarmament has several far-going implications for the success of cyber deterrence.

First is the threat posed to the stability of cyber deterrence. Knowing that the adversary is not capable of carrying out cyberattacks that might lead to the disarmament of the victim may incentivize cyber attackers. Due to the covert nature of preparing for cyberattacks (Morgan, 2010, p. 72) and the fear stemming from the uncertainty of whether the adversary will attack first, both parties have incentives to rush into striking first. This is because the contending sides may see utility in attacking prior to the other party taking protective measures, such as reconfiguring its network. That mutual fear of an unexpected attack is what Paul K. Davis refers to as "the perceived cost of going second." This favors offense over defense, thus destabilizing deterrence (Davis, 2014, pp. 345-346). Furthermore, incentives to strike first through cyberattacks are amplified given the impracticality of mutually assured destruction (MAD) which was a feature of nuclear deterrence (Crosston, 2011, p. 100). MAD is not applicable to far less severe cyber responses, and, as a result, the cost of attacking is significantly diminished, thus altering the equation of offense-defense in favor of the former (Bendiek & Metzger, 2014, p. 559), which, in turn, jeopardizes the stability of cyber deterrence.

Second, some scholars note that the impracticality of disarming cyber challengers renders the strategy of preemption, or preventive, strike an irrational "motive" (Libicki, 2009, p. 61; Gartzke & Lindsay, 2015, p. 319). Even though a preemption attack might appear to succeed, the damage inflicted through cyberattacks would, unlike the apocalyptic damage inflicted by nuclear weapons, mostly be limited to information infrastructure and networks (Cimbala, 2014, p. 281), and even to a few computers, which are easily replaceable (Libicki, 2009, p. 61). Even if a punitive attack destroyed the entire platform from which the attack had been initiated, the actual aggressor can readily continue its misconduct through relocation to a different offense platform with a differing offense "pathway" using a varied network. That fact appears to lead Jonathan Solomon, a technology and system analyst, to conclude that in cyberspace, "symmetrical counterforce deterrence" is not handy (Solomon, 2011. p. 13).

Given the inapplicability of disarming would-be attackers, Libicki emphasizes the importance of persuading the aggressor to stop attacking. He discards the idea of "rushing into retaliation." That is, it is not the swiftness of retaliation that should be prioritized, but, rather, more focus should be given to efforts to persuade the cyber perpetrator not to do what it has been doing. In the light of that, the strategy of active defense discussed in the relevant literature becomes a contentious issue. In a narrow sense, the core of the strategy of active defense is to automatically target the attacking computers in retaliation (Libicki, 2009, pp. 61-62). However, this raises serious concerns among pundits and experts. For example, Morgan states that automatic retaliation, although establishing credibility, may hit a target from which the attack originated accidently or "erroneously," thereby bearing the risk of escalating an "incident" into a war (Morgan, 2010, p. 66).

2.2.1.3.5 The problem of third parties engaging in cyberattacks

The articulation of the problem of a third party's involvement in cyberattacks and cyberwarfare is prevalent in the relevant studies (McReynolds, 2015). Third parties can be nation-states, non-state actors, such as individual hackers, massed patriot hackers, terrorist groups, non-governmental organizations, or corporations. While in the physical domain, non-state actors are known for their non-combatant characteristic and minimal influence, this situation is the exact reverse in the cyber domain (Rattray & Healey, 2011, pp. 67-70). To put it differently, in the Cold War era, only a very limited number of actors that could pose a nuclear threat existed. In the cyber domain, the number of possible threat actors is, by contrast, "astronomically" high. In addition, not only does this diversity of actors increase swiftly, but it also continuously differ in character, thus causing ambiguity and hampering communication as well as stability of deterrence (Sterner, 2011, p. 66). The increased number of threat actors in cyberspace is due partly to low entry barriers to cyberspace, the ease and low cost of acquiring cyber tools for malicious uses, and vulnerabilities or weaknesses in systems, all of which makes offense easier than defense in the cyber sphere (Rattray & Healey, 2011, pp. 67-70). Having noted that, the question of how third parties can muddle cyber deterrence needs to be answered.

First, in cyberspace, neither the original attacker nor the retaliator can confidently be certain that consecutive cyberattacks and counterattacks come from each other given the possibility of a third party interjecting itself into the conflict, thus complicating deterrence (Solomon, 2011, p. 17). From Libicki's standpoint, the problem is likely to arise provided that cyberattacks and counterattacks between the original cyber perpetrator and the retaliator are public knowledge. For example, a fight between two states in cyberspace may have mobilized a group of patriotic hackers over which the contending governments may not have control. As a result, even though the original offender and the retaliator ceased cyberattacks and counterattacks against each other, the patriotic hackers might take up the fight where they left off and continue to conduct cyberattacks on the target, thereby leading to confusion between the original opposing parties (Libicki, 2009, pp. 62-63).

Second, cyber actors possess a differing degree of "risk tolerance" in comparison to their counterparts in the kinetic world (Trujillo, 2014, p. 49). The success of deterrence relies upon the assumption of rationality of actors making cost-benefit calculations and acting accordingly; and yet not all non-state actors act on a rational basis. Hacktivists or terrorist groups may not have a rational world sentiment. Consequently, they are not as propitious to deterrence as nation-states are (Iasiello, 2014, p. 64). For example, individual hackers may carry out cyberattacks simply to have fun or win prestige, making them resistant to deterrence (Lakhani & Wolf, 2005). This irrationality problem is further magnified given the “perceived anonymity, invulnerability, and global flexibility” in the cyber venue (Trujillo, 2014, p. 49). This leads Solomon to conclude that deterring third party non-state actors in the cyber terrain can be challenging, if not impossible (Solomon, 2011).

Third, as previously mentioned, third parties may significantly interfere with efforts to correctly and confidently attribute the source of a cyberattack. In addition to that, Libicki also highlights that the odds of a third party’s engagement obstruct the retaliator’s and the original aggressor’s understanding of “the relationships among attack, retaliation, and counterretaliations.” In this light, third party hackers can jeopardize the restoration of the order prior to the breakout of cyberwarfare between the actual aggressor and the retaliator, thus destabilizing cyber deterrence. Taking all together, the original fighting sides must always keep in mind the prospect of a third party meddling in the fight. For Libicki, this fact undercuts an implicit logic of deterrence: “if you stop, we stop,” thereby limiting the efficacy of cyber deterrence (Libicki, 2009, p. 63).

2.2.1.3.6 The problem of establishing a threshold to retaliate and the cyber application of conventional deterrence concepts of “broad” and “narrow” deterrence to cyberspace

In the literature, drawing redlines or determining thresholds for any potential harm inflicted through cyberattacks is presented as a major hurdle (Kugler, 2009, p. 338). The challenges residing in the establishment of “simple” and “recognizable” thresholds that permit a full understanding of “all immediate consequences” primarily stem from several factors peculiar to cyberspace (Goldstein, 2013, pp. 133-138). First, the inadequacy of an international legal framework defining what constitutes cyberattack and, thus, merits retaliation, makes it difficult to determine thresholds (Solomon, 2011, p. 12). Second is the ambiguity of the magnitude and consequences of cyberattacks, and the difficulty of understanding the underlying intention of the attacker. The aforementioned factors may lead to miscalculation, misinterpretation, surprise, and escalation between fighting parties, thus causing deterrence to fail (Goldstein, 2013, pp. 133-138).

The limits of the international legal framework in terms of defining what constitutes cyberattack and, thus, deserves reprisals, complicates efforts to determine thresholds (Solomon, 2011, p. 12). There are several approaches to determining how deleterious a cyberattack must be to merit punishment. Of these, the approach that prioritizes the effect and scale of the offense stands out (Jensen, 2012, p. 791). The Tallinn manual, a manual on the law that is intended to regulate cyberwar by drawing analogies from existing international law, is an example of this approach since it places emphasis upon the effects and scale of cyberattacks in establishing thresholds for reprisals. It should be noted, though, that it is not a binding document (Schmitt, 2013, pp. 1-45). According to Guy-Philippe Goldstein, the answer to the question of what consequences of cyberattacks are deemed to cross a redline for the deterrer should encompass what is "tolerable" and, thus, can be neglectable, and what is "intolerable" and, therefore, can directly instigate retaliation, both in kind and kinetic (Goldstein, 2013, p. 134). Drawing an analogy from the law of armed conflict with respect to *jus ad bellum* in the 1949 Geneva Convention, the Tallinn Manual regards significant human casualties resulting from cyber misconduct as "armed attacks" and justifies the use of force or any potential military retaliations in self-defense. Additionally, the Manual also justifies retaliation, both in kinetic and non-kinetic, in the wake of significant economic loss due to cyberattacks that can endanger the political integrity of the independent nation-state, so long as the consequences of those actions are recognizable. Thus, those cyber actions responsible for the loss of human life and considerable economic damage can be categorized as intolerable and, thus, deserve reprisals (Goldstein, 2013, pp. 134-136). However, some argue that despite being a good starting point, the Tallinn Manual is still inadequate and not likely to be effective in the foreseeable future. Hence, some scholars call for the development of internationally recognized rules which reflect the consensus of the global community (Geers, 2010; Bendiek & Metzger, 2015, p. 564).

The question of what is tolerable is also associated with the question of "narrow" deterrence by punishment (Bendiek & Metzger, 2012, p. 563). Libicki admits the viability of a narrow deterrence posture that distinguishes what to deter. He agrees on the degree of clarity that the loss of human life from cyberattacks will bring in determining thresholds for reprisals. Libicki, however, raises concerns about the justification of retaliation based on such criterion. Unlike armed attacks in the kinetic world, cyberattacks can, he states, cause human casualties not as a "primary" but as a "secondary" consequence (Libicki, 2009, p. 67). That is, to gauge indirect or "delayed" effects in cyberwar is very hard to do upon the application of the principle of proportionality (Jensen, 2013, p. 207); even if human life is lost from a cyberattack, which has yet to occur, it would probably be due partly to an "accident." Therefore, justifying reprisal in accordance with the criteria mentioned above will not be "simple" because of the uncertainty about the immediate consequences of cyberattacks and the ambiguity of the real intention of the offender (whether the deaths were an accident or deliberate.) Furthermore, while accepting the existence of a high potentiality of proportional retaliation, Libicki, nevertheless, has some reservations about establishing thresholds based on economic criteria, too. First, he argues that such an approach faces the difficulty of pricing. For example, it is hard to establish a price for "lost privacy" in cyberspace (Libicki, 2009, pp. 67-68). Second, whereas small scale cyberattacks are expected to cause minor damage, large scale cyberattacks are more likely to inflict tremendous damage on computer systems (Nishikaze, Ozawa, Kitazono, Ban, Nakazato, & Shimamura, 2015). However, this is not always the case with cyberattacks. An aggressor with a modest intent may inadvertently have exceeded the determined threshold, which is likely because of the high probability of a cyber offensive having cascading effects on the target. This may lead the cyber attacker to regard as unwarranted what the deterrer may have considered to be a “proportionate” reprisal, thus increasing the risk of escalation (Libicki, 2009, pp. 66-68). Hence, it is difficult to determine thresholds for retaliation due to the unclarity of magnitude and consequences of cyberattacks, and the difficulty of understanding the underlying, true motive of the cyber perpetrator (Goldstein, 2013, pp. 133-138).

Having addressed what is considered intolerable in cyberspace, practices falling into the tolerable category can, Goldstein writes, be considered cyber espionage, classified under Computer Network Exploitation (CNE), because the international community views that as simply a new form of the old practice of keeping an eye on governments (Goldstein, 2013, p. 134; Bartos, 2016). Speaking of small scale, tolerable cyber aggression which inflicts minor damage, Libicki casts doubt on “broad” deterrence strategy. He, in this sense, strongly opposes the policy of “zero-tolerance,” which means retaliation for every single act of cyber misconduct, regardless of its scale, scope, or whether it is repeated. He asserts that if the U.S. adopts a “zero-tolerance” policy, it will be unwise and troublesome, mainly for three reasons. First, such policy may constantly face “the potential for a *casus belli*.” Thus, he advises that small scale cyberattacks should be subject to prosecution of the cyber culprit rather than to a direct retaliation. Second, the attacker may misinterpret the signaling through retaliation since the deterring state is, in contrast to retaliation in the kinetic world, likely to retaliate based on “the occasional discovery rather than the constant activity” of investigating every intrusion into her systems. This can, for Libicki, prompt the attacker to pose the question of “Why me, why now?” and, as a result, to interpret the message by punishment in a wrong way. Third concerns whether the retaliation is proportional. If the punishment is not proportional in the eyes of the target, both parties run the risk of escalation, thus hampering deterrence (Libicki, 2009, p. 65-66). The issue of proportionality deserves more attention since the pertinent literature devotes significant commentary on it.

2.2.1.3.7 The legal Issues: The problem of proportionately responding to cyberattacks by both cyber and kinetic means, and "dual use" entities

There exists a body of international law governing the rules of engagement and conventional war practices in the kinetic world, but conflict in the cyber realm lacks such legal framework and, thus, "does not fall squarely within the bounds of law enforcement or traditional warfare" (Sterner, 2011, p. 76). This legal vacuum in cyberwarfare brings up various problems with deterrence by retaliation. Of those, the issue of "proportionality" attracts the attention of many scholars studying cyber deterrence. To fill this gap, some steps were taken. One of those is NATO's initiative of the Tallinn manual, applying existing customary and conventional principles to cyberattacks and cyberwarfare (Payne, 2016). In accordance with the Manual, a punitive reprisal against a cyber attacker must be proportional in the sense that it must amount to the first wrongdoing while not being equivalent to an escalation. In the event of a retaliation against state actors, the importance of proportionality becomes a more sensitive issue. As crucial as it is to punish the would-be cyber aggressor proportionately, various scholars, however, concur upon the existence of the significant challenges to do so (Iasiello, 2014, p. 59; Sterner, 2011).

First, the projected effect and magnitude of cyberattacks is, as underlined above, hard to determine (Limnell, 2016, p. 10). Ironically, there is a high prospect of small attacks, even if not meant to, leading to dramatic consequences or collateral damage, due to the high level of interdependence of global networks, while large attacks of malicious intent can, specifically if poorly carried out, cause much less severe consequences. As a result, it is difficult to respond proportionately owing to the difficulty of projecting the second order effects and magnitude of cyberattacks (Sterner, 2011, p. 73).

Second, in some cases, the needed information for the determination of the battle damage caused by cyberattacks may not be attainable (Limnell, 2016, p. 10). For instance, the private sector's role in the operation and constitution of the cyber venue is, as opposed to its role in the kinetic realm, immense (Mudrinich, 2012, p. 183). Therefore, the reluctance of privately owned enterprises to share information regarding intrusions and the damage wreaked by cyberattacks with the authorities, due partly to "business confidentiality," may hamper the assessment of the battle damage, making it hard to retaliate proportionately (Limnell, 2016, p. 10).

The third problem complicating proportionate responses to a cyberattack concerns the speed of the reprisal. Assessing the entire battle damage done to one's computer-oriented systems and networks can be burdensome since it usually takes weeks to soundly fathom the magnitude of the damage. For that reason, the retaliator may not be able to be prompt in retaliation, and this may lead the attacker to misinterpret the late retributory action, thereby increasing the risk of escalation (Limnell, 2016, p. 10). According to Goodman, because of the uncertainty of the consequences and magnitude of cyberattacks, as well as the anonymity of cyber attackers, the deterrence strategies of "severity" and "immediacy" in punishment measures are not applicable to the cyber domain; and yet he notes that cyber deterrence only accentuates "certainty" in punitive measures (Goodman, 2010, p. 108).

The fourth problem pertains to what type of retaliation it will be, whether kinetic or non-kinetic (Sterner, 2011). Taking a glance at the cyber deterrence literature, in retaliation to a cyberattack, nation-states are offered a range of response instruments. For deterrence purposes, state-actors can leverage military and diplomatic tools, as well as economic, legal, and cyber instruments. Even, nuclear arsenals can be used to deter cyberwarfare and cyberattacks (Jensen, 2012, p. 793; Limnell, 2016, p. 10). This wide spectrum of response options at states' disposal is not constrained by the existing international law governing use of force since the law does not provide a specific prescription of what means states can leverage in self-defense, and yet the response ought to be proportional. In other words, a deterring state can strike back through both kinetic and cyber means (Dal & Ozyurt, 2014, p. 312). For example, according to B. Thijsen, as of 2012, the White House made it clear that kinetic response to cyberattacks would be on the table (Thijsen, 2016, p. 11). The example of kinetic response to cyber misbehavior is manifest in the Obama' administration's sanctions on Russia following Russian' interference with the 2016 U.S. presidential election. The U.S. resorted to kinetic means and expelled 35 Russian operatives in retaliation for Russia's cyber misconduct (Jackson, 2016). Corresponding strategy has also been adopted by other international actors. For example, NATO announced that the use of kinetic force in response to cyberattacks is not off the table (Thijsen, 2016, p. 11). However, potential kinetic retaliations to cyberattacks raise various valid concerns (Sterner, 2011, p. 72; Jensen, 2012, pp. 794-795).

Firstly, unlike reprisals in the physical world, it is hard to point a finger at someone or identify the sources of attacks with full confidence in cyberspace (Cebrowski, 2002, p. 6). Thus, a kinetic retaliation to the assumed cyber aggressor bears significant risks if the attribution is not done accurately. Secondly, resorting to kinetic means for reprisals may be too late to deter the cyber perpetrator from inflicting damage on computer networks given the relative speed with which cyberattacks can transpire (Jensen, 2012, p. 795). Thirdly, and most importantly, Sterner urges that employing kinetic means in response to a cyberattack may be too risky on the accounts that the likelihood of causing human casualties significantly outweighs the damage a cyberattack may inflict upon systems. In this light, he draws a conclusion that kinetic response is likely to be "disproportional" (Sterner, 2011, p. 72). This fact, along with the others already described above, may profoundly increase the chance of escalation as discussed below.

Lastly, also problematic are "dual-use" targets occupied by both civilians and governments or militaries (Hollis, 2007). This closely concerns the problem of the distinction between civilian and military entities. (Wedgwood, 2002, p. 224) In accordance with the law (*Jus in bello*), a fighting party can target an opponent's military facility in which civilians are working. In other words, this facility may qualify for a legitimate target based on the "dual-use" rule. However, when it comes to cyberspace or cyberwarfare, the issue of dual-use objects can apply to almost every computer-networked system. To draw attention to the importance of the dual-use issue in the cyber venue, Duncan B. Hollis writes that by 2000, over 90% of the United States Army's information and communication traffic occurred through networks utilized by civilians. As a corollary of this, any attack targeting a government's communication networks through cyber systems would mean an interference with the utilization of the same infrastructure by civilians, or non-combatants (Hollis, 2007). Such effects on civilians are prohibited in accordance with Geneva Conventions IV of 1949 (Ambach, Bostedt, Dawson, Kostas, & Bostedt, 2015, p. 75). Then, the trouble is that in the event of cyberwar, dual-use facilities are more likely to be targeted owing to the high interconnectedness of the cyber realm (Geiß & Lahmann, 2012), thus raising legal problems, which, in turn, complicates cyber deterrence by retaliation.

2.2.1.3.8 The problem with the increased chance of escalation in cyberspace

Drawing an analogy from the escalation ladder of Cold War era nuclear-strategy, scholars studying cyber deterrence try to ascertain whether cyberattacks and counterattacks may lead to a higher chance of escalation during a particular conflict level (Davis, 2014, pp. 347-348). Libicki provides, in order of the severity of belligerence, an escalation ladder of response, with responding through nuclear instruments being at the top, preceded by kinetic force and, then, by cyber response, and with economic and diplomatic responses at the bottom of the ladder. He points out that because wielding a nuclear weapon in retaliation to an attack would be the ultimate level of escalation in a given conflict, neither side would have any further need to fear provoking the other to resorting to a more devastating form of attack. Libicki stresses the serious possibility that counterretaliation by the original cyber aggressor may escalate into "the violent and even nuclear realm" for several reasons (Libicki, 2009, pp. 29-69).

For Libicki, the likelihood of escalation depends mainly on: 1) if aggressors view cyber retaliation as unmerited; 2) if cyber perpetrators are under domestic pressures to retaliate in a conspicuously "painful" fashion; and 3) if they are convinced that countering in other domains, such as land and sea, where they have more advantages, will help them win the fight. It should, however, be noted that the underlying reasons of escalation in cyberspace may be multiplied. For instance, "inadvertent" and "accidental" escalation may occur in cyberspace as it can in the kinetic world, or even if retaliation is proportional, the original attacker may not perceive it as so (Libicki, 2009, p. 69). Providing a speculative escalation ladder assessment for cyberattacks, Paul K. Davis, in this respect, poses a provocative question to underscore the significance of attackers' perception of retaliation in the escalation ladder. He points out that for some, striking civilian infrastructure through large counterattacks may seem to be escalatory, yet he wants us to assume that China and the U.S. were in conflict and that the U.S. already started hitting some targets in China. "Would Chinese cyber attacks on the U.S. homeland be escalatory?" According to him, it might be seen so on the part of the U.S. while not being deemed escalatory by the Chinese (Davis, 2014, p. 348). It, then, follows that the higher the chance of perception differentiation between cyber actors as to the justification of reprisals, the higher the chance of escalation.

Another reason for escalation in cyberspace may be the problem of "temporality." Cyberattacks do not give an early warning sign, which may lead to confusion in the escalation ladder. During the Cold War period, there existed "observable" sets of sequential events, such as developing a weapon and testing it. Those events did not occur suddenly. Thus, they functioned as "early warning signs" and provided the disputing parties with clearer ladders of escalation to follow. Owing to these visible series of events, Cold War actors could adjust "triggers" and redlines in accordance with how threats were unfolding. However, this is not the case in the cyber sphere. The very infrastructure and cyber tools that account for cyberspace and that are utilized for peaceful and useful purposes can instantly be turned into inimical ones. Thus, "the time interval between cyber-attack and detection is potentially zero." That is, there are no observable prior warning signs for cyberattacks, which not only obstructs the pre-determined ladders of escalation but also hampers the signaling in the cyber venue (Taipale, 2010, pp. 20-21).

Combining all together, what distinguishes the nuclear escalation strategy from the cyber escalation ladder is mainly the ambiguous nature of cyberspace as well as nonexistence of "ground rules" in the cyber domain. These facts greatly increase the risk of escalation by retaliation in the cyber sphere, thus making cyber deterrence more tenuous (Libicki, 2009, p. 69).

2.2.2 Technological, Legal, and Political/ Diplomatic Hurdles to Deterrence by Denial

David Elliott notes the distinction between cyber deterrence by denial and other deterrence strategies employed in the physical domain. He writes that defensive measures against a nuclear strike have, indeed, never been viewed as providing a substantial deterrent, regardless of how robust and effective the defenses are, because if a single nuclear weapon evaded those defenses the result would be devastating. Consequently, he suggests that the precepts of nuclear deterrence theory are not transferrable to the hindrance of cyberattack because "cyberattack represents the flip side. Defense is difficult, but possible" (Elliott, 2011, p. 36).

The difficulty of employing defensive measures to safeguard one's computer systems and networks against cyberattacks and cyberwarfare stems from numerous technical, political, and legal issues (Mudrinich, 2012, p. 182). For example, Geers emphasizes legal problems regarding deterrence by denial, stating that while deterrence by retaliation derives from "military doctrine," the baseline of deterrence by denial lies in the legal framework concerning criminology (Geers, 2010, p. 301). With that in mind, the issues impeding the efficacy of cyber deterrence by denial will be elaborated below.

2.2.2.1 Technological Impediments to Deterrence by Denial

Various pundits argue that the cyber application of deterrence by denial to cyberspace appears to be ill-suited partly because of the immense technological differentiation in the two domains. First, offensive cyber technology significantly varies from that of nuclear weapons. This fact makes anti-proliferation of cyber offense tools difficult to achieve, which lessens denial capability (Geers, 2010, pp. 299-301). Second, the protection of cyber systems is very challenging owing to the omnipresence of cyber systems and networks (Jensen, 2012, p. 808).

Geers points out that due to its "dynamic and fast evolving nature," cyber technology used to execute cyberattacks is very distinct from the technology utilized to develop nuclear weapons (Geers, 2010, p. 300). The 1968 Non-Proliferation Treaty (NPT) was meant to preclude proliferation of nuclear weapons and technology, as well as to effectuate the eventual disarmament of nuclear weapon-holders (Ruzicka & Wheeler, 2010, p. 74). Such a treaty was viable because states and non-state actors' access to menacing weapons in the Cold War era could be constrainable. The efforts to prevent the spread of nuclear weapons also contributed to a significant decrease in the number of potential aggressors that had to be deterred, thus facilitating attribution (Taipale, 2012, p. 19). Additionally, the International Atomic Energy Agency served as an inspection mechanism to ensure that nuclear materials were utilized for peaceful purposes. So, in the nuclear epoch, the logic of deterrence by denial mainly manifested itself in a norm-based framework simply because of the impracticality of defensive measures against a nuclear blast (Geers, 2010, p. 299).

However, scholars suggest that in cyberspace, a different picture emerges due mainly to the fact that it is relatively easy to attack, that entering the cyber domain is cheap, and that cyber technology rapidly evolves (Murdinich, 2012, p. 170). Consequently, anti-proliferation of cyber weapons vis-à-vis their nuclear counterparts is harder to accomplish. The acquisition, concealment, and deployment of cyber weapons are easier, thus complicating cyber defense (Geers, 2010, p. 299). As Morgan aptly puts it, "*proliferation of relevant* [cyber] *capabilities is already widespread*" (Morgan, 2010, p. 72). Cyber capabilities for malicious purposes are easily obtainable at low costs (Mudrinich, 2012, p. 167); they range from simple weapons with minor effects that are used by “script kiddies” to sophisticated weapons requiring advanced skills for their development and successful deployment. Stuxnet is an illustration of a cyber weapon that could possibly cause physical damage or death (Denning, 2015, p. 12). More challenging to preventing the propagation of cyber weapons, Geers adds, relates to the difficulty of defining “malicious code,” due to the intrinsic feature of cyberspace that significantly allows deceptive methods. For example, a deceptive hacker can conduct cyberattacks through a recognized, or “legitimate,” network, thereby making it difficult for experts to discern malicious codes (Geers, 2010, p. 299). As earlier discussed, cyber disarmament is also virtually out of question, thereby not only hampering deterrence but also destabilizing security relationships between disputing parties in the cyber venue (Morgan, 2010, p. 73). Furthermore, unlike a difficult-to-hide trial of nuclear weapons to demonstrate capability, the preparation phase of cyber weapons or capabilities is clandestine and, thus, is difficult to detect through inspection. For example, the test of cyber capabilities can “live on the [I]nternet” (Geers, 2010, p. 299).

The omnipresence of the Internet, networks, or systems is also shown to be a major hurdle to the successful employment of cyber deterrence by denial. In the Cold War period, the U.S. conceived of the Strategic Defense Initiative (“SDI”) with the aim of protecting itself against ballistic missiles fired by adversaries. Some have suggested that a corresponding strategy can be viable to cyberspace since it could make attacks futile; however, Jensen raises concern about the viability of this “SDI-type analogy” and contends that developing such a defense mechanism would be extremely challenging for several reasons (Jensen, 2012, pp. 808-809).

Firstly, in the kinetic world, although diverse, potential targets were detectable soon after the initiation of nuclear attacks and were contained geographically. This is not the case with cyberattacks. Owing to constant changes in attack systems of would-be opponents, instantly detecting the origin of an attack and its ultimate target is virtually impossible (Jensen, 2012, pp. 808-809). In addition, as previously discussed, cyberattacks can originate from “anywhere in the world, at any time” (Geers, 2010, p. 300), thus differentiating them from their nuclear counterparts that could only be fired from sea or ground. Secondly, had an intercontinental ballistic missile been fired by the adversary, the target would have been aware of the attack and usually been able to predict its effects. However, cyberattacks on networks or systems are mostly indiscernible; hence, one should remember the general belief that “the most dangerous attack is often the one you don’t know is occurring” (Jensen, 2012, p. 809).

2.2.2.2 Legal Impediments to Deterrence by Denial

As previously articulated, unlike the existing international rules, norms, and practices governing conventional warfare, such legal frameworks to govern cyberwarfare, or cyberattacks, are either lacking or immature in that because cyber phenomenon are very nascent (Geers, 2010, p. 300; Roberts, 2014, p. 552). To fill the legal vacuums in relation to the cyber venue, some steps have been taken. There are two different vantage points. On the one hand, various pundits argue that existing international law, such as the law of war and the use of force, can be applicable to cyberspace, or cyberwarfare, through analogy (Hollis, 2007, p. 1023). As an illustration, the former U.S. Army Colonel David E. Graham states that so long as its response to a cyberattack falls within the boundaries of the customary international law notions of proportionality and necessity, a state can use force in self-defense (Graham, 2010, pp. 100-101). On the other hand, others highlight the inadequacy of the existing rules and practices regarding non-state actors that play, and will continue to play, a significant role in the cyber sphere and in cyberwar. They contend that cyber-specific rules and practices are needed to fill these legal grey areas left by the existing international laws in addressing cyberwarfare. Otherwise, it is argued that these legal vacuums can lead to a higher chance of escalation and great uncertainty in cyberspace (Hollis, 2007, p. 1023).

2.2.2.2.1 The application of existing international law to cyberspace and legal gray areas at national and international level that hamper cyber deterrence by denial

The importance of establishing acceptable international cyber rules, norms, and practices by drawing analogies from existing international law, specifically from the Charter of the United Nations, is emphasized in the literature. This view is widely held mainly because the effectiveness of the existing established regimes to deter states from acting aggressively was proven in the kinetic world. In this light, many scholars and experts concur upon the relevancy of the Law of Armed Conflict (LOAC) to aggression of states in cyberspace. As mentioned earlier, the Tallinn Manual proposes rules for the application of LOAC to the cyber venue. In addition, Denning writes that Department of Defense (DoD), in a report concerning its cyberspace policy in 2011, expressed the applicability of relevant rules and norm at both the domestic and international levels, including the rules of LOAC, to its actions in the cyber area (Denning, 2015, p. 13). In this line, issuing guidelines for policy-makers and non-governmental organizations in combating threats of cybercrime and cyberwarfare, “The Soul Conference on Cyberspace” in 2013 is, according to S. Jasper, a step forward governing state’s’ behavior in cyberspace in accordance with the existing international law (Jasper, 2015, p. 72).

However, attempts to secure computer networks and systems do not always fall within the boundaries of the existing legal frameworks applied to cyberspace, thus raising legal concerns. For example, one way of securing cyber systems is the concealment of those systems by presenting them as something else. To this end, states may opt to make their military systems look like civilian ones in order to conceal them from potential cyberattacks, yet Jensen points out that such actions would be against the international law disallowing fighting parties to involve non-combatants in their military goals. He also cautions that governments' efforts to mask computer-oriented systems in such a manner may be a violation of the fundamental LOAC rule of "distinction" that mandates belligerents possess a distinguishable sign that is "fixed" and identifiable at a distance. By the same token, Jensen notes that honeypots might also raise legal concerns (Jensen, 2012, pp. 818-819). Honeypots, also known as honeynets, are used to protect systems from and detect attacks by emulating systems and vulnerabilities, and can aid defenders in acquiring information about attackers and their driving factors, threats, and tactics (Joshi & Sardana, 2011, pp. 64-65). Due to their deceptive nature, governments' use of honeypots to safeguard their military systems might lead would-be aggressors to attack other non-military targets, thus bringing up legal issues (Jensen, 2012, pp. 819-820).

Owing to legal gray areas, similar problems also exist in deterrence by resilience at the national and international level. Significant impediments to employing the deterrence by resilience strategy are caused by the legal difficulty of governments aligning domestic law and regulations with the deterrence strategy, as well as the implications of such a deterrence method for international law (Jensen, 2012, pp. 815-816). These two points will be discussed below.

First, many parliaments, such as the European Parliament, play little role in framing comprehensive cyber defense strategies due to a lack of expertise needed for creating such strategies, which impedes parliament, the public-private sector, and government from cooperating and exchanging relevant information (Bendiek, 2012, p. 24). In discussing domestic law and regulation issues, Jensen writes that because of the existing domestic legal framework in effect, the U.S. government can face legal challenges to providing substitute cyber systems following potentially crippling cyberattacks. He states that if the U.S. government needed to pass a bill to utilize private sector' "bandwidth" in the event of debilitating cyberattacks on the government's networks and systems, this action might be construed as an infringement upon individual rights. By extension, he also points to the fact that the U.S. government has to deal with "fiscal regulation" in purchasing substitute systems and computers in large quantities, which is another challenging issue (Jensen, 2012, pp. 815-816).

Secondly, as was stated earlier, in accordance with the international law, a retaliation to an attack must be proportional, and yet resilient systems may make cyberattacks fruitless. In that case, Jensen raises a legitimate question of how one can respond to an ineffectual cyberattack proportionately. He concludes that resilient systems may have self-restraining impacts upon the victim responding to attacks. Consequently, this dis-incentivizes nation-states from employing the deterrence by resilient strategy (Jensen, 2012, pp. 816-817).

2.2.2.2.2 Barriers to the initiatives toward establishing cyber-specific rules to deter

Numerous scholars point to the limits of the existing international rules and norms addressing cyber phenomenan. For example, there is still a heated debate about whether LOAC principles can be applicable to cyberattacks launched by non-state actors and whether the victim state has right of self-defense under Article 51 of the UN Charter. For that reason, the necessity of establishing new treaties governing cyberattacks and cyberwarfare is widely underscored in the relevant literature (Gervais, 2012, p. 541-542), but the literature simultaneously underlines the legal challenges to the establishment of cyber-specific rules and norms. These difficulties revolve around drafting new international cyber treaties; the harmonization of nations'' domestic laws with international law regarding cyber issues; sensitive technology transfer and trust issues in cooperation and collaboration among governments and allies for collective cyber defense posture (e.g. extended deterrence); unclear lines of legal liability in the event of cyberattacks and cyberwarfare between governments, or militaries, and private sectors; and finally the responsibility issue concerning the deterrence strategy of making cyber systems interdependent. Each of these elements will individually be addressed below.

Firstly, it is argued that given the insufficiency of the current established regimes, it is essential to draft new treaties that will promote cyber disarmament and offer “alternatives” to the use of military force in the regulation of the cyber venue (O’Connell, 2012, p. 206). Such treaties controlling and limiting cyber armament would, some suggest, not only pave the way for the restriction of cyber offensive weapons developed by states, but it would also communicate cyber commands of nations to each other. This is believed to increase “transparency norms,” which would, in turn, boost cyber deterrence (International Institute for Strategic Studies, 2016, p. v). Although promising, such international treaties prohibiting or limiting the development and use of cyber weapons for offensive purposes would, Scott Jasper notes, be challenging to implement. This is because there is still no universally agreed definition of cyber weapons, which hampers endeavors to verify whether states comply. Additionally, the bulk of the constituent component of cyber technology needed for the proper operation of cyberspace essentially falls in the category of “dual-use” technology. For these reasons, keeping the development of cyber weapons in check, limiting their proliferation, and ultimately preventing their use is, according to Jasper, “practically impossible” (Jasper, 2015, p. 71).

Secondly, in order to generate international cyber specific rules, it is important that nations harmonize their domestic laws with international laws regarding cyber issues and set standard procedures for cross-border investigation. By extension, he suggests that states enforce a set of practices that allow for the delegitimization and deterrence of cyberattacks. This approach is, Taipale notes, called the deterrent strategy of *counter-productivity* (Taipale, 2012, p. 42). To this end, the Council of Europe Convention on Cybercrime was adopted by the Council of Europe in 2001. It is the first international treaty aiming at the harmonization of nations' domestic laws on cyber-related issues, particularly on crimes committed online, such as child pornography and infringements of copyrights, to enhance international cooperation by enabling states to conduct transnational investigations of cybercrimes (Keyser, 2003, p. 297; Vatis, 2010, p. 207). However, Geers urges that states may raise opposing voices to this strategy owing to the potential breaches of their national sovereignty by law enforcement organs of foreign nations. Based on that, he highlights the difficulty of having states sign and enforce such treaties as the European Convention of Cyber Crime (Geers, 2010, p. 300).

Thirdly, securing computers and computer networks will have significant impacts upon a nation's communication and interaction with other nations. This situation necessitates establishing "collective defense" mechanisms with global partners and allies given that cyberspace does not lie within the bounds of a single nation's border but, rather, exists on the global scale. According to Major Erik M. Mudrinich, the importance of U.S. collaboration and partnership with allies in safeguarding cyberspace is emphasized in the DoD's cyber strategy released in 2011 because such approaches will not only increase information sharing but also raise "operational situational awareness" (Mudrinich, 2012, p. 185). However, Jensen writes that this does not come easy. He states that because such cooperation will require, for example, the U.S. to share and transfer technology with its allies, it may be subject to different "export regimes" and, hence, face domestic legal challenges, complicating deterrence by denial (Jensen, 2012, pp. 811-812).

One way of enhancing cooperation between allies manifests itself in the incorporation of extended deterrence into the strategy of deterrence by denial. During the bilateral standoff between the U.S. and the USSR, extended deterrence was believed to preclude proliferation of mass destruction weapons by the virtue of alliances. Engaging in similar cooperative interplays with allies can help states cope with the issue of the propagation of cyber offensive tools. Morgan, in this regard, states that the U.S. and its allies have already begun the integration of their cyber systems in the military area (Morgan, 2010, p. 73). The U.S.''s stance on such a concept is evident in former President Obama's speech. He remarks, "the United States will respond to hostile acts in cyberspace as we would to any other threat to our country…We reserve the right to use all necessary means--diplomatic, informational, military, and economic--as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners" (Bendiek & Metzger, 2015, p. 565).

Related to the idea of extended deterrence, some authors suggest that NATO can be a viable means of implementing extended deterrence doctrine to assist its members with lesser cyber power so as to safeguard their cyber infrastructure, including military cyber systems, as a part of an integrated defense strategy (Kramer, Butler, & Lotrionte, 2016). However, other scholars cautiously approach this idea. For instance, Morgan notes that such cooperation entails technology transfers as well as the exchange of expertise among allies (Morgan, 2010, p. 73), which possibly means the demonstration of additional vulnerabilities upon granting access to allies, raising trust issues (Libicki, 2009). Furthermore, Morgan also urges that integrating its cyber systems with allies bears some risks for the U.S. (e.g. making the U.S. more vulnerable through the integrated systems) (Morgan, 2010, p. 73).

It should be underlined that although the ideas of enhanced cooperation with allies and collective defense under NATO's extended deterrence doctrine bear some risks for the U.S., as stressed above, the potential benefits of these initiatives seem to outweigh their potential perils upon the examination of the case of Stuxnet, which will follow this chapter. Stuxnet is believed to be the joint undertaking of the United States and its ally, Israel, and was successful at its mission (Nakashima & Warrick, 2012; Sanger, 2012), thus underscoring the significance and effectiveness of such initiatives. This point is important to note since it directly corroborates this study's argument with respect to how the U.S. should manage cyber power to head off its rival, China.

Back to the discussion of the legal challenges to the establishment of cyber-specific rules and norms, fourth concerns the private sector playing a profound role in cyberspace as opposed to its comparatively minor role in other war-fighting venues, as earlier emphasized (Mudrinich, 2012, p. 183). Every state relies upon private companies in the provision of the Internet (O'Connell, 2012, p. 207). It is, for example, believed that over ninety percent of the U.S. government Internet traffic occurs through privately owned civilian ICT infrastructure (Jensen, 2012, p. 810). As a corollary of this, Sean Doherty aptly observes that defending cyberspace eventually hinges upon the private sector in the United States (Doherty, 2015); but the problem is, James A. Lewis stresses, that the private sector lacks capabilities to safeguard its computer systems against sophisticated adversaries of the U.S. such as China. This necessitates the U.S. government's intervention in the defense of civilian-owned cyber systems and networks. Implementing any security measure by the government in this sense will remarkably affect private ICT companies and Internet providers (Lewis, 2010, p. 58), thus leading to the problem of appropriate jurisdictions at the national level (Stevens, 2012, p. 152).

This problem emerges due to the lack of such lines that ought to be drawn to demark liability between the private sector and the government (Mudrinich, 2012, p. 184). Jasper remarks that private companies in the U.S. are mindful of the importance of sharing data about cyber threats among each other, but the problem is that due to the lack of cybersecurity legislation, private enterprises are concerned about the risk of potential infringement on civilians' freedom and their privacy rights, as well as liability (Jasper, 2015, p. 70). Thus far, stringent security measures dictated for the private sector have not existed. In this respect, former president Barack Obama made it clear that his administration would not impose security measures on privately owned enterprises (Etzioni, 2014).

Jensen accentuates that efforts to impose security standards on private companies in the U.S. face significant legal challenges. First, he states that security measures would mandate government officials monitor civilian networks, which has hitherto always been a contentious legal issue and, thus, would certainly be subject to objections. Second, he alludes to the "kill switch" discussion in the U.S. congress (Jensen, 2012, p. 811). In 2010, some Congress members proposed a bill that would grant the President the power to "flip a switch," essentially shutting down the Internet, in the event of cyberattacks against the economic and other cyber infrastructure in the U.S. However, this bill was strongly opposed due to its being unconstitutional. For example, some argued that such security measures granting the executive branch the authority to quell the communication of millions of people would infringe on such individual rights as freedom of speech. Thus, the bill was not enacted (Swartz, 2011). By extension, delegating such authority to the president would affect the private sector to a great extent. It would also lead to the abuse of the "constitutional authority" of the President. Lastly, legal issues also arise when governments attempt to safeguard systems and networks against "insider" threats (Jensen, 2012, pp. 811-812).

An insider is defined as an individual working inside an organization and using his "privileged" knowledge about and authorized access to the cyber systems within that organization with malicious intention. An employee or contractor can be an insider. One recent example of an insider is Edward Snowden, the whistleblower of classified NSA (National Security Agency) information (Gelles, 2016, pp. 1-3). Jensen points out that while Washington is mindful of a possible insider threat for espionage purposes, the protection of systems and networks against such threats would necessitate taking measures, such as monitoring personnel within and outside of the office, which raise serious "constitutional" concerns (Jensen, 2012, p. 812).

Fifth, Jasper stresses that "international norms, confidence-building measures, capacity-building assistance" are suitable means to deter through entanglement (Jasper, 2015, p. 72). As mentioned above, if the cyber relations of nations are more interlaced in cyberspace, especially in economic terms, they will refrain from acting aggressively in the cyber terrain by the virtue of the high level of "interdependency" (Denning, 2015, pp. 13-14)

However, legal concerns also exist when it comes to increasing global interdependency on computers and computer systems. To have a global sustainable cyber interdependence, technology transfers from nations with sophisticated cyber technology to nations with less cyber power may face legal challenges. For example, Jensen writes that despite the U.S. permitting "sensitive" technology transfer, it stipulates that the recipient states not allow for the transfer of the technology to another nation. This may necessitate the establishment of new inspection regimes to verify that further transfer of such does not occur, which is another challenge. Also, legal issues regarding making cyber systems interdependent relates to responsibility. The problem of who is going to be responsible for "losses" and "damage" arises, partly because of potential cascading effects of cyberattacks on interdependent computer-networked systems if cyber systems and networks are intertwined. In this light, Jensen urges that legal, diplomatic, and technological barriers will pose significant challenges to the establishment of ground rules to determine legal responsibility for damage on and losses of interdependent cyber systems (Jensen, 2012, p. 823).

2.1.2.3 Political/Diplomatic Issues Complicating Cyber Deterrence by Denial

Political issues revolve around conflicts of interest among major players, which hamper efforts to establish international rules and an acceptable code of conduct governing cyberattack and cyberwarfare, as well as the increased distrust among nations that further muddles the deterrence method of dependency.

First, the importance of norm-based approaches in deterring cyberattack and cyberwarfare has become clearer to the international community. Stevens, for example, points to the increased significance of norm-based deterrent effects in U.S. initiatives concerning cyberspace since 2008, stating that developing international norms and obligations that promote multilateral understandings of what constitutes admissible conduct in the cyber venue has gradually become the focal point of the U.S. The same also holds true for other major powers, such as China and Russia (Stevens, 2012). To illustrate, recently, the U.S. and China initiated bilateral talks about what will be the appropriate "code of conduct" regulating the control mechanism for cyber weapons (International Institute for Strategic Studies, 2016, p. v).

However, these bilateral talks have taken place sporadically and been rife with problems (International Institute for Strategic Studies, 2016, p. v). Stevens draws attention to the conspicuous disagreements among the major players which have resulted in difficulties establishing internationally agreed-upon regulative norms to govern cyberattack and cyberwarfare. He notes that this normative approach is still in its early stages not only because the U.S. does not have a coherent strategic stance on cyber deterrence but also because there exist considerable conflicts of interest between other norm entrepreneurs, such as Russia and China, who have their own political agendas and attitudes about the development of these regulative norms (Stevens, 2012). Jasper, too, makes similar point and highlights the existence of a “clash of self-interests” between major players that hampers cooperation. To exemplify, he points to the China’s suspension of a Sino-American cyber working group after the U.S. charged five Chinese military officers with hacking in 2014 (Jasper, 2015, p. 72). The clash of self-interests is also evident between the U.S. and Russia. Whereas Russia takes a more “regulatory” and “interventionist” approach, the U.S. fosters private companies owning and operating ICT infrastructure to undertake the liability for securing cyberspace. This notable interest differentiation between major actors makes the development of legal frameworks to govern the cyber area difficult, thereby subverting deterrence (Stevens, 2012).

The second issue concerns a lack of trust among nations that can impede the deterrence strategy of interdependency. Making cyber systems interdependent requires that nations, to a great extent, rely upon the same cyber systems, which, in turn, necessitates technology transfers among nations, as earlier addressed. This fact may be leveraged by some technologically advanced nations for espionage purposes, which alerts nations importing cyber technology to take protective measures, specifically against important components of “supply chain.” Consequently, this reduces dependency, which, in turn, hampers deterrence (Bendiek & Metzger, 2015, p. 561). The supply chain is defined as the “outsourced” dissemination of significant IT components, such as software (Boyson, 2014). Bendiek and Metzger, for example, point to China’s decision to decrease its dependence upon U.S.-based enterprise Microsoft’s Windows 8 in the aftermath of the Snowden’ disclosures. In the same vein, they hint at German Chancellor Merkel‘s call for greatly reducing reliance on U.S. cyber technology. This risk management strategy of diminishing the level of strategic interdependency is on the rise across nations, thereby making it difficult to implement the deterrence strategy of interdependency (Bendiek & Metzger, 2015, p. 561).

It is important to note that the aforementioned clash of interests between major powers, particularly the U.S. and China, results mainly from the lack of political convergence on issues regarding Internet economies and the governance of cyberspace. This study argues that the U.S. enhancing economic partnerships and creating all-inclusive economic associations in the cyber terrain can substantially contribute to the reconciliation of these divergent interests that exist between them.

2.2. Conclusion

The research on cyber deterrence represent two sides of a coin. On the one side, it is argued that the classical deterrence theory can successfully inform cyber deterrence in countering the threat of cyberattack and cyberwarfare. On the other side, the bulk of the relevant studies suggest otherwise, arguing that the tenets of classical nuclear and military deterrence don’t work properly when applied to cyberspace due to the technical, legal, and political problems inherent in cyberspace that lessen the effectiveness of communication, credibility, and capability, all necessary conditions for the success of deterrence.

At the very least, there are four major challenges hampering the efficacy of cyber deterrence against cyberattacks and cyberwar. Firstly, anonymity and attribution go hand-in-hand to thwart communication, capability, and credibility. Secondly, the projection of cyber capability by powerful nation-states is impaired due to the existing asymmetry in cyberspace. Thirdly, credibility is subverted by the fact that most of the attacks are left non-responded to due partly to the fear of cascading effects and escalation, as well as the problem of attribution. Lastly, the limits of existing international law and the immaturity of cyber-specific legal frameworks at the national and international level also undermine communication and credibility, thus contributing to cyber deterrence failure.

Considering the distinctive characteristics of cyberspace mentioned above that significantly restrain the successful cyber application of conventional and nuclear deterrence concepts, several scholars offer distinct propositions to enhance the efficacy of cyber deterrence against deleterious cyber operations. Some pundits suggest the cyber application of expanded deterrence, serial deterrence, and tailored deterrence, which are an extension of traditional deterrence concepts (Libicki, 2009; Kugler, 2009; Morgan, 2010; Lupovici, 2016). Active cyber defense, deterring cyberattacks by resorting to kinetic means, and cyber deterrence against specific types of cyber weapons amenable to dissuasion are also under consideration (Graham, 2010; Mudrinich, 2012; Denning, 2015; Keen, 2015). Even, re-configuring the underlying architecture of the Internet is on the table as a remedy to enhance cybersecurity (Mudrinich, 2012). Others search for solutions outside the technical domain of cyberspace. They propose norm-based approaches under the strategy of deterrence by denial, with a focus on human factors in generating identities and ideas in the cyber terrain and, therefore, on the social construction of the perceived cyber threats (Stevens, 2012; Lupovici, 2016). The 2009 Tallinn Manual, a manual on international law that governs cyberwarfare, is an example of the efforts to create norms-based cyber deterrence (Schmitt, 2013, p. 1). However, numerous scholars and experts still believe that cyber deterrence is “doomed to fail.” This consensus is specifically prevalent in the International Relations (IR) school (Lupovici, 2016, p. 322).

There are common components to the studies addressing cyber deterrence. One can observe that the same components are also manifest in the scholarly works investigating the link between cyberwarfare and deterrence. First, the research on cyber deterrence is heavily influenced by the classical deterrence strategies extensively developed during the nuclear standoff between the superpowers. Second, American scholars seem to dominate the relevant studies, specifically concerning viable cyber strategies that the U.S. can implement to successfully deal with cyber threats and leverage cyberwar for deterrence purposes (Lupovici, 2011, p. 49).

Third, the vast volume of the relevant work is policy-driven with few exceptions. Some scholars point to the "policy analysis community" domination of research on global cyber security issues as the underlying reason for a pervasive "theoretical vacuum" in the study of cyber deterrence. This theory-policy gap has inspired some to call for IR scholars to further develop theories to explain phenomenon in the cyber venue. Consequently, some tendencies toward such a goal have become noticeable recently. For example, along with the realist theory of deterrence, the constructivist approach, one of the IR theories, has begun to carry more weight in addressing cyber deterrence (Lupovici, 2016, p. 323; Stevens, 2012). More importantly, this theoretical vacuum is also ascribed to the inadequacy of historical cyber incidents and appropriate methodological frameworks (Kosenkov, 2016, p. 2), which makes it difficult to develop a theory that can allow us to better inform cyber deterrence and examine its efficacy in thwarting cyberwar, particularly between the U.S. and China.

This problem, or theory-policy gap, is more evident in the analysis of the efficacy of cyber deterrence versus potential cyberwar between the U.S. and China. Despite the existence of some insights into, or analyses of, a possible U.S-China cyberwar, especially over Taiwan (Libicki, 2009; Kugler, 2009; Clarke & Knake, 2010), these insights are mostly speculations and "threat-inflation" (Lindsay, 2013, p. 368), constrained by the cyber application of classical deterrence, and notably lacking a robust theoretical perspective, with few exceptions (Domingo, 2016; Thomas, 2016). This study applies Power Transition Theory to cyberspace. It aims to examine the efficacy of cyber deterrence between the U.S. and China within a theoretical framework and bridge the theory-policy gap. This analysis necessitates searching for a solution outside of the limits of classical deterrence and technical vulnerabilities in cyber systems and networks. PTT can provide such an analysis by focusing on the political and strategic calculus of the nation-states.

Chapter Three: Conceptual Landscape and Stuxnet

3.0 Introduction to Chapter

This chapter provides the conceptual landscape of the study. With that purpose, it defines cyberspace, characterizes it as hierarchical, and identifies the position and role of both the United States and China. Equally important is that the chapter describes the term "cyberwar," distinguishes the concept from other types of cyber operations, and lays out its strategic value as well as why nation-states, specifically China, may resort to it. In this sense, the case of Stuxnet is examined in order to understand the nature of cyberwar, justify the conceptualization of cyberwar in this study, and finally demonstrate its strategic utility and what can be accomplished with it.

3.1 Defining Cyberspace and Cyberwarfare

3.2 Cyberspace

In the early 1990s, commentators began to increasingly talk about "cyberspace" (Rattray, 2009, p. 254); and yet no consensus on the definition of cyberspace exists in the relevant literature. Franklin D. Kramer writes that there are twenty-eight varying definition of the term, according to one study done recently (Kramer, 2009, p. 4). Given this definitional chaos, dividing cyberspace into layers is one approach adopted by various scholars to get a better grasp of the term (Libicki, 2009; Clarks, 2010; Choucri, 2012). In this respect, David Clark provides a four-layered model, which is adopted by this study. The first layer is the physical layer; this layer consists of the physical components of cyberspace, such as computers and telecommunication companies, as well as all kind of networks. This physical layer is deemed “the foundation” of the domain (Clark, 2010, pp. 2-3).

The second layer is the logical layer built upon the first layer; cyberspace at this level is “a series of *platforms*, on each of which new capabilities are constructed, which in turn become a platform for the next innovation… [e.g.] platforms upon platforms upon platforms” (Clark, 2010, pp. 2-3). Services are enabled in this platform (Choucri, 2012, p. 8). Libicki offers examples of the logical layer, including “device recognition, packet framing, addressing, routing, document formatting, [and] data manipulation.” He adds that hacking usually occurs at this level (Libicki, 2009, p. 12).

The third layer is the information layer where information in various forms, such as video and music, is created, captured, stored, and processed (Clark, 2010, pp. 3-4). Nye notes that cyberattacks can be executed from this level against the physical realm (Nye, 2011, p. 123).

The fourth layer is the top layer where the people and organizations in pursuit of differing objectives and playing distinct roles engage in cyberspace (Choucri, 2012, p. 8). Subject to conventional attack is the physical layer, whereas the other three layers are conducive to “intrusion, exploitation and control” (Mudrinich, 2012, p. 177).

Laying out the characteristics of cyberspace, in this study, *cyberspace* is defined as a global, political (Choucri, 2012), and “operational domain” (Nye, 2011, p. 122) “*framed by use of electronics and the electromagnetic spectrum”* in order for the creation, storage, modification, exchange, and exploitation of information “*via interdependent and interconnected networks* [and computer-based systems] *using information-communication technologies*” (Kuebl, 2009, pp. 26-28). Governing cyberspace is software and hardware; shifts in software and hardware technology mean changes in cyberspace. For that reason, cyberspace is “malleable” (Kramer, 2009, p. 5; Rattray, 2009, p. 256). The evolving nature of cyberspace can be exemplified by the emergence of the Internet and the propagation of personal computers (Starr, 2009, p. 82). However, the malleability of cyberspace is limited by “physical laws, logical properties of code, and the capacities of organizations and people.” In addition, as mentioned earlier, one unique characteristic of cyberspace is that it is an offense-dominant terrain. Due to this and other distinctive features of cyberspace, such as its ever-evolving nature, it significantly differs from other domains (e.g. sea and land) (Rattray, 2009, pp. 256-272).

Franklin D. Kramer lists what he calls “cyber influence activities”, such as watching television and browsing the Internet (Kramer, 2009, p. 4). Danial T. Kuebl views cyberspace as an “*operational”* domain in which both individuals and entities utilize the required technologies in order to influence others not only in the cyber venue but also across different venues and “elements of power.” He also believes that cyberspace can be a principal means of conducting “strategic influence” in operational terms (Kuebl, 2009, p. 29). This view is consistent with the U.S.’s explicit emphasis on the concept of cyberspace as an operational domain in military terms (Lynn , 2011). Militarily speaking, not only is cyberspace an operational domain itself, but it also plays an enabler role in operations within and across other domains: sea, land, air, and space. As a result, cyberspace is regarded as a “warfighting domain.” The recognition of cyberspace as a warfighting domain was officially expressed by the U.S. Department of Defense in 2010. As a fifth warfighting venue, cyberspace inherently poses some risks and opportunities. David M. Hollis, for example, notes the innate potentiality of cyberspace that can render components in each of the four layers fruitless and can inflict harm on, or “destroy,” critical national infrastructure, such as those of government, military, education, and health, through cyberattacks and cyberwar (Hollis, 2010, p.49; Zeadally & Flowers, 2014; Cai & Dati, 2015, p. 549).

It should be noted that in this study, the Internet is mainly used in reference to cyberspace because a number of entities, ranging from government and military networks to cable and cellular networks, across the globe have begun using the Internet, and, thus, becoming increasingly Internet technology-dependent (Zimet & Skoudis, 2009, p. 91). Examples include financial transactions, television, and telephone service; all are increasingly becoming reliant upon the Internet. This makes Internet-enabled systems "the fastest growing elements" of the cyber domain (Skoudis, 2009, p. 171). As a result, the future of cyberspace is believed to rely, if not exclusively, upon the future of the Internet, which makes the Internet a central constituent of cyberspace (Blumenthal & Clark, 2009, pp. 207-209). Combining all together, in this study, the focus will be on Internet technology, specifically networks that utilize the Internet protocol (IP). Such a reductionist approach is manifest in Libicki's analysis in his book titled *Cyberdeterrence and Cyberwar* (Libicki, 2009, p. 6).

Offering a new landscape and opportunities for conflict, contention, and competition, Choucri comments that cyberspace as a new fifth domain displays all the principal components of politics, power, and influence. As a consequence, she states that cyberspace has a political salience and should be treated as a political venue. Choucri determines that there are three main types of cyber conflicts and contentions in cyberspace. She suggests that contentions may arise "over the architecture and management of cyberspace;" or cyber conflicts can occur for "political advantage and profit;" and that, ultimately, cyber conflicts can pose threats to national security (e.g. the militarization of cyberspace and cyberwar) (Choucri, 2012, pp. 126-131). The above-taxonomy is well-suited for the analysis in this study because it is in line with the probable causes of a cyber conflict or cyberwar that may occur between the U.S. and China.

3.2.1 Status Quo in Cyberspace

A cyber application of Power Transition Theory argues that the international system in the cyber sphere is characterized by a hierarchical structure. The diffusion of power in cyberspace virtually reflects the distribution of power in the real world with few exceptions. In the light of Power Transition Theory, this study asserts that an identical hierarchical structure in the kinetic world also exists in cyberspace, with the leader, the U.S.as the main rule-maker, at the top, followed by great powers, such as China. Various scholars make comments analogous to the above characterization of the cyber system. For example, Choucri states that the fundamentals of the current international relations in the kinetic world stay "salient" in cyberspace, too (Choucri, 2012, p. 42). A similar point is made by Francis C. Domingo, who notes that the great powers will remain "dominant" in the cyber sphere (Domingo, 2016, p. 164). In addition, Nye points out that powerful states, such as Russia, France, the U.S., and China, are reputed to possess greater cyber capability; hence, the great powers will be more influential in cyberspace, albeit not as much as they are in the other domains, such as sea and air (Nye, 2011, pp. 150-151).

3.2.1.1 The U.S. as a dominant power in the cyber venue

The determination of each nation's place within the hierarchy in cyberspace is, in a broad sense, based on their cyber power, defined by Nye as "the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyberdomain" (Nye, 2011, p.123). In this light, at the top of the pyramid in the cyber venue sits the U.S.; it is the dominant power in cyberspace just as is it in the physical realm. Thus, by the virtue of its leading role in the formation and development of the Internet, the United States reaps the most benefits from the prevailing status quo in cyberspace. It is considered to be the most effective rule-maker and, as a result, usually governs the most significant constituent components of cyberspace, such as the Internet. In other words, it is primarily the United States that sets the terms for the governance of the Internet and has the largest influence upon the critical organizations managing the cyber domain (Choucri, 2012, p. 128; Powers and Jablonski, 2015). By extension, the U.S. is reputed to possess the most potent cyber offensive capabilities (Singer & Friedman, 2014; Thomas, 2016), which will be discussed in the following chapter. The above points indicate that the U.S. is the dominant power in cyberspace.

Various scholars recognize the U.S.'s dominance over the economy of the Internet. They acknowledge that the U.S. accrues the most benefits from the global Internet economy; for example, it is stated that the U.S. provides thirty-eight percent of the manufacture necessary to create the elements of cyberspace, such as hardware and content associated with the Internet, followed by China as the third largest producer by ten percent. The U.S. also receives thirty-five percent word-wide Internet connectivity, or telecommunications, income as well as over forty percent of net revenue created online. According to Shawn M. Powers and Michael Jablonski, one ranking service suggests that in 2012 forty-three percent of the world’s million most favored Web sites were within the territory of the U.S., followed by Germany with 8 percent. China was ranked as the third competitor with only 5 percent, far behind the U.S. Furthermore, Powers and Jablonski present a table that presents the annual revenue of Tier 1 Internet Providers in 2013 in billions of dollars. The revenues of U.S. companies’ stand out when seen alongside that of their foreign competitors. For example, it appears that the sum of only two U.S. companies’ revenue, namely

AT&T and Verizon Communications, amounted to USD 249.4 billion in 2013, which is more than the sum of the revenues of their five foreign competitors. Based on that, the U.S. indisputably remains the greatest economic beneficiary of the Internet and dominates "the global [I]nternet industry" (Powers & Jablonski, 2015, pp. 109-124).

The pillar organizations of the global governance of cyberspace guiding the Internet are also dominated by the U.S. For example, some of the significant constituents of cyberspace are run by private enterprises located in the U.S., such as the Internet Corporation for Assigned Names and Numbers (ICANN) (Kramer, 2009, p. 10). Internet governance broadly means the management of fundamental components of the Internet, such as "protocol for data transmission" (e.g. IP address and HTTP), root servers, "corresponding domain names," and IP addresses. As an illustration, domain names enable services or web sites to be visible and accessible. To remove a domain name renders all associated services and websites "unreachable." Then, in order to be able to exercise power in the governance of the virtual world, one must have sway over the above-mentioned components that are core to the Internet. The U.S. seems to assume this role. For example, Domain Name System (DNS) is "highly centralized and controlled top-down by ICANN", a corporation under the influence of the U.S. government (Powers & Jablonski, 2015, pp. 131-132). As a corporation physically located in California, ICANN is responsible for the management of the internet (e.g. the assignment of address blocks to geographical Internet registries) (Powers & Jablonski, 2015, pp. 139-140). It is also tasked with the operation of the Internet Assigned Numbers Authority (IANA), which is also crucial to the governance of the Internet (Kwalwasser, 2009, p. 493).

Discussing the significance of ICANN, Milton Mueller comments that the formation of ICANN by the U.S Department of Commerce in 1998 was a landmark in the governance of the

Internet. Mueller also makes a critical observation, noting that, “ICANN arose from a unilateral construction of a global regime by the United States” (Mueller, 2010, p. 10). More to the point is that critical organizations in Internet governance, such as ICANN, IETF (Internet Engineering Task Force), and ISOC (The Internet Society) were designed in such a way that legitimized the perpetual U.S. dominance of cyberspace (Powers & Jablonski, 2015, p. 153). In the light of the U.S. dominance of the global Internet industry and the governance of the Internet, coupled with its arguable cyber offensive superiority to its potential competitors, some scholars conclude that the U.S. is in possession of sufficient power to determine who will survive and perish in cyberspace, and, thus, is sufficiently capable of dominating the cyber domain (Lindsay, Cheung, & Reveron, 2015, p. 3).

3.2.1.2 China as a rising challenger in cyberspace

As highlighted prior, Power Transition Theory characterizes China as a rising challenger to the U.S. preponderance in the kinetic world. In the same vein, in a reference to PTT’s description of China, this study conceptualizes China as the most dangerous rising cyber challenger to the U.S. preponderance in cyberspace. The corroboration of this argument is pervasive in the relevant literature. For example, in the eyes of U.S. decision-makers, while Russia represented the first dangerous cyber threat to the U.S. due to its cyber operations against Estonia and Georgia in 2007 and 2008 respectively, China has lately been portrayed in this role as a result of the cyber operations it conducted on U.S. soil (Cai & Dati, 2015, p. 542). Likewise, Singer and Friedman write that the U.S. Congress in its reports has characterized China as “the most active and persistent” cyber culprit intruding in U.S. networks and systems. P.W. Singer and Allan Friedman further add that in its *Strategy for Operating in Cyberspace*, released in 2011 to provide a blueprint for the U.S. military's Cyber Command, Washington, although not directly, defined China as one of the most dangerous cyber perpetrators (Singer & Friedman, 2015, pp. 133-138).

Akin to that, Jon R. Lindsay describes China as a rising cyber power by referring to its rapid growth in Internet economies and its increasing cyber operations (Lindsay, 2014). Others make corresponding arguments (Maness & Valeriano, 2016, p. 303). China increasingly displays a high Internet presence in parallel to its increasing leverage in cyberspace. As an illustration, based on the number of Chinese Internet users (485 million in 2011), Choucri observes that the world's largest Internet population will be in China. This means that China will far exceed the U.S. in Internet population (Choucri, 2012, p. 57). With respect to China's mounting cyber operations, Lindsay writes that Chinese cyber operations have significantly soared lately. He notes that those cyber operations have, however, been limited to CNE, such as industrial espionage, for the purposes of collecting intelligence and stealing commercial data from the U.S. business sector, rather than cyberattacks (CNA) that can be destructive in nature (Lindsay, 2014, pp. 7-28). Additionally, in 2013, a National Intelligence Estimate referred to China as the most aggressive country trying to infiltrate the computer systems and networks of the United States government and American enterprises in order to obtain data for "economic gains." More importantly, in recent years, as a rising cyber power, China has started to carry more weight in discussions of the global governance of the Internet (Lindsay, Cheung, & Reveron, 2015, p. 2).

3.3 Cyberwar

3.3.1 Distinguishing "Cyberwar" from Other Types of Cyber Operations

The "Information Era" is said to have a transformative impact upon the way societies function. In the aftermath of the 1991 Gulf War, military analysts came to understand that the way war is fought has also been transformed in parallel to developments in information technology, which led to the idea of the information-based technological Revolution in Military Affairs (RMA). It is this idea of the RMA that, David J, Betz notes, gave rise to Network-Centric Warfare (NCW) and Information Warfare (IW) (Betz, 2006, p. 505). The notion of "cyberwar" is, in this sense, regarded as the latest stage in the continuing progress of the RMA. Taking a glance at the growing literature on cyberwar, it appears that scholars, strategists, and experts seek to warn about the hazards of cyberwar. They understand the extent of damage that can be inflicted through cyberwar and whether or not it may have altered "the nature of political conflict" (Gartzke, 2013, pp. 41-44). Although the vast volume of the literature on cyberwar seems to prefer to use the term "cyberwar" or "cyberwarfare," this use is notably contested by various commentators, thereby leading to not only a vagueness as to the definition of the concept but also disagreements on certain facets unique to cyberwar (Eun & Abmann, 2016, p. 346).

Given the lack of consensus on criteria for the description and in order to avoid any possible confusion, there is utility in drawing a clear line between such terms as NCW and IW that have usually, and perhaps inaccurately, been used interchangeably. In a broad sense, Betz defines NCW as the exploitation of information so as to increase the efficacy of conventional weapons, whereas he, as earlier stated, refers to IW as "a potential weapon in its own right." Betz also adds that further sub-classification of IW is handy since this categorization may offer a description of the "conceptual landscape" (Betz, 2006, p. 508). Pertaining to that, John Arquilla and David Ronfeldt divide IW into two forms. First is "netwar." Netwar is a conflict of information occurring at a "societal-ideational" level, fought by networked systems, and waged at a strategic level, with the purpose of modifying or disrupting a society's knowledge about phenomenon. Second is "cyberwar," which is waged at the military level and is more linked to tactical-operational ICTs-related conflicts, with the aim of altering knowledge and information dominance in favor of the initiator. While categorizing netwar as "low-intensity" conflict, they classify cyberwar as being viable as both "low- and high-intensity conflicts" (Arguilla & Ronfeldt, 1993, pp. 27-31). Re-conceptualizing "netwar" and "cyberwar," Harknett, however, stresses attacks or defenses on *the societal and military connectivity* in defining the two terms respectively (Harknett, 1996, p. 94).

A further and broader categorization can also be made in order to depict a well-established contextual landscape and mark a clear distinction between cyberwar and other cyber operations. Colonel Jayson M. Spade points out that the United States Army classifies any exercise of cyber capability whose means are not kinetic as Computer Network Operations (CNO). CNO is further split into Computer Network Defense (CND), Computer Network Exploitation (CNE), and Computer Network Attack (CNA) (Spade, 2011, pp. 7-8; Liff, 2012, p. 404). CNE is, by nature, "intrusive" and is mostly non-destructive; it entails "unauthorized" extraction of information from a target's computerized systems. Cyber espionage is an example of CNE. However, CNA can be "destructive" and connotes the alteration, disruption, denying, deception, degradation, or destruction of an opponent's computerized-networks or systems, or "programs" and "information" that reside in and transit the cyber systems and networks. This study focuses on CNA since it accounts for offensive cyber operations that can potentially cause psychical damage (Spade, 2011, pp. 8-9; Lobel, 2012, pp. 622-623). In addition, Spade states that there are two chief objectives of CNA. Whereas the primary goal of CNA lies in denying the adversary "the ability to use their computer systems, stored information, and networks as designed or intended," the secondary goal focuses on affecting "all those people, systems, and organizations" dependent upon those ICTs, and "interfering with or denying them the ability to do their job" (Spade, 2011, pp. 8-9).

3.3.2 What does "Cyberwar" mean?

With the distinction made above, attempts to define "cyberwar" may prompt more ambiguity and confusion since cyber security experts and scholars have not been able to offer an agreed-upon clarification of the concept. By extension, as earlier stated, it is still disputable whether "cyberattack" can fall under the rubric of aggression in traditional terms or is merely a "nuisance" that does not merit attention due to its "unharmful" character (Eun & Abmann, 2016, pp. 346-347). Some ascribe this definitional chaos to "the multidisciplinary character" of research on cyberwar that spans such domains as International Law and International Relationships, and Computer Science. Consequently, pundits and experts with varying backgrounds interpret the meaning of cyberwar in accordance with their perspective on the issue, thus complicating the meaning of the term (Cai & Dati, 2015, pp. 545).

The debate is not only constrained by the pervasive conceptual divergence among scholars, experts, governments, and military strategists; some commentators have even gone so far as to call narratives of cyberwar "hype" or "myth" and cyberwar scenarios mere speculations (Gartzke, 2013; Rid, 2013). To the contrary, numerous other scholars, experts, and government officials have already come to believe that cyberwar may pose the "next existential threat" to nation-states (Gartzke, 2013, p. 50). For example, the 2011 European Parliament policy paper, according to some scholars, highlighted the increasing importance of cyberwar for states in the European Union, noting that future interstate war will have a cyber-dimension (Eun & Abmann, 2016, pp. 343-345). In particular the U.S government`s officials believe that the future war will occur in cyberspace (Hughes, 2010, p. 523). Lynn contends that cyberwar is imminent and poses a major threat (Lynn, 2010). Pointing to the danger cyberattacks can pose to U.S. national security, former President Barack Obama, Adam P. Liff writes, declared in 2009 that the U.S. cyber infrastructure will be regarded as a "strategic national asset" (Liff, 2012, p. 402). Leon E. Panetta, former Defense Secretary of the U.S., was particularly vocal on this issue and highlighted the magnitude and seriousness of the threat cyberwar poses. He urged that due to the increasing vulnerability of the U.S. to potential cyber perpetrators abroad, the United States faces the prospect of a "cyber-Pearl Harbor" that would "cause physical destruction and the loss of life, an attack that would paralyze and shock the nation and create a profound new sense of vulnerability" (Bumiller & Shanker, 2012).

Clarke and Knake offer more vivid depictions of a calamitous Pearl Harbor scenario with a digital component attached to it. They assert that through cyberattacks, trains could be derailed; financial information systems could collapse, resulting in the loss of immense amounts of data; air traffic control systems could be shut down; and nuclear power plants could possibly be damaged, giving rise to a nuclear catastrophe. Moreover, it is speculated that China could place logic-bombs, defined as pre-installed programs that cause networks or systems to shut down, in the power grids of major U.S. cities, leading to widespread blackouts (Clarke & Knake, 2010). Wesley Clark and Peter Levin, too, believe that cyberwar seems to be ineluctable and will affect a large section of populations by disrupting critical national infrastructure, such as power grids and financial networked-systems (Clark & Levin, 2009). A similar assessment is made by Gary McGraw, who asserts that cyberwar looms on the horizon and is inevitable unless vulnerabilities in critical infrastructure systems are closed by enhancing cyber defenses (McGraw, 2013). Some accounts go so far as to claim that the threat cyberwar poses is perceived as more worrisome than the risk of nuclear war or conventional assaults (Kaiser, 2014, p. 11).

To a broader extent, many commentators and cybersecurity experts argue that cyberattacks could disable or destroy both military and civilian critical cyber infrastructure and networks. Related to potential physical damage from cyberattacks, the Stuxnet worm, to be addressed below, was the first of its kind and was a cogent justification of such scenarios as cyber Peral Harbor or 9/11. Perhaps, that is why Stuxnet was seen as “the Hiroshima of cyber-war” (Gross, 2011).

With the cyberwar literature briefly addressed, Nye’s definition of cyberwarfare can be useful as a point of departure for further discussion. He defines cyberwar as “hostile actions in cyberspace that have effects that amplify or are equivalent to major kinetic violence” (Nye, 2011, p. 21). Corresponding thoughts in terms of the level of destructiveness of cyberwar are prevalent in others’ comments. For instance, the former FBI Director Robert Muller remarked that today’s cyberattacks can produce effects equivalent to a “well-placed bomb” (Eun & Abmann, 2016, p. 347). From the standpoint of Richard A. Clarke and Robert K. Knake, cyberwar refers to “actions by a nation-state to penetrate another nation’s computers or networks for the purposes of causing damage or disruption.” This definition is important because of its emphasis on nation-states. Cyberwar is, first and foremost, hostile actions among nation-states (Clarke & Knake, 2010, p. 6).

To achieve a precise picture of the distinctive characteristics of cyberwar, one must be able to unambiguously illustrate what types of cyberattacks qualify as cyberwar. Adam P. Liff suggests that cyberwarfare is defined as encompassing only the use of CNA against military and civilian cyber infrastructure, and it excludes “psychological warfare” in the cyber domain. Another stipulation for what constitutes cyberwar is its “non-kinetic” property (Liff, 2012, pp. 404-408). Cyberwar must also, as in conventional war practices, be politically driven and waged with an aim to coerce adversaries. Additionally, cyberwar has to be violent in character, causing or attempting to cause physical harm and destruction, perhaps, but not necessarily, including injury or death (Liff, 2012, p. 408; Singer & Friedman, 2014, p. 121). Treating cyberspace as a political venue means that the use of cyber tools must be seen as efforts to accomplish political ends just as are tools used in other domains (e.g. on land and at sea). In this vein, it is essential to recognize cyberwar as a “strategic challenge” rather than as a technological matter (Limnéll, 2016, p. 3).

Combining Liff’s definition of cyberwar with those of others, this study refers to cyberwar as *a nation-state’s cyberattacks (CNA) against its adversary nation’s military or civilian computers, computer-based systems, and networks with an aim of coercing adversaries and extracting political concessions by inflicting physical damage on these computers, computer systems, and networks, such damage possibly, but not necessarily, including injury and death, or total destruction.* Libicki views cyberwar waged with coercive intent as a feasible option and an effective means to “assert status in international relationships and to teach lessons to other countries” (Libicki, 2009, p. 121). Kugler makes a corresponding point, stating that cyberattacks can be instrumental in coercing and persuading others in pursuit of political and other agendas across different domains (Kugler, 2009, p. 314). The purpose of cyberwar is, then, to assert status by bending the opponent to offender’s “will” (Libicki, 2009, p. 118). This study considers a potential cyberwar initiated by China against the United States in this sense. For example, if China is disenchanted with the status quo in cyberspace, it will be likely to launch cyberwarfare against the U.S. in order to alter the prevailing cyber order in such a way that it can extract political, economic, and strategic concessions and accrue more benefits from it.

Possible objections to the definition of the term “cyberwar” offered in this study are worth noting. Some may argue that using the term “cyberwar” is inaccurate in that such a thing has never existed. Of those skeptical of such a term, Thomas Rid is perhaps the most vocal. His main argument is that cyberwar has never occurred in the past, nor will it transpire; thus, using the notion “cyberwar” is problematic at best on the grounds that cyberattacks have not yet met Carl von Clausewitz’s three required components of war. First, war must entail elements of violence in terms of lethality, be instrumental in terms of means and ends, and be political in terms of motive (Rid, 2012, pp. 7-8).

However, Rid’s view is contestable. It is true that no human casualty due to cyberattacks has, as has been earlier stated, been reported so far; yet as John Stone suggests, lethality and violence have no inexorable link to one another. Violence inflicted on objects, but not to individuals, can also be considered acts of war. Thus, the insistence that only aggressions with a “lethal dimension of violence” qualify to be called acts of war is misleading and inaccurate. Cyberattacks that cause physical damage to objects, as did Stuxnet, can fall under the rubric of war. In addition, even assuming that Rid’s point that in history, there has been no war that has remained unattributed is true, Stone aptly and accurately observes that Clausewitz’s description of war as an act of force does not stipulate that it be attributable. More importantly, just because the historical record suggests that there has been no unattributed war does not necessarily mean that future war could not entail “unattributed acts of force” (Stone, 2013, p. 105).

Corresponding arguments to that of Stone are to be found in the cyberwar literature. For example, Alex Calvo argues that cyberwar can and will be equal to an act of war. Once an alternative reading of Clausewitz’s definition of what war is made, cyberwarfare will be entitled to be labeled among acts of war in Clausewitzian terms because cyberattacks can lead to physical damage. To reinforce his argument, he contends that once most of the physical systems, ranging from industrial complexes to weapon systems to household appliances, become internet-reliant on a permanent basis, the borderline between the real and virtual world may become more blurred. As a result, the distinction between denying access to a harbor by incapacitating its cyber systems and besieging the harbor by placing mines around it may fade away (Calvo, 2014). The cogency of this observation can be justified by the U.S. government's declaration in 2011 that a cyberattack will be considered akin to an act of war; therefore, responding with kinetic means is among the options available to the U.S. government (Department of Defense, 2011).

Important to note is that in the context of potential cyberwar between the U.S. and China, political attribution will not be an unsurmountable problem whatsoever because the would-be-attacker, China, would be willing to reveal its identity. The validity of this argument can be corroborated by various scholars. In comparison to Russia's stealthy cyber pursuits, Matthew D. Crosston finds China's openness about its cyber activities surprising (Crosston, 2011, p. 106). Broadly speaking, Libicki writes that cyber perpetrators may, in some cases, "make it fairly clear who is attacking and why," depending on their motivations (Libicki, 2009, p. 90). With regards to that, Charles L. Glaser notes that if a state seeks to compel the U.S. to "make political concessions" in times of crisis by initiating cyberattacks on the U.S.'s cyber systems and its society, which is called the "countervalue" attack strategy, this state has a political motivation. Thus, for the threatening state to succeed in compelling the U.S., its demands and menacing message must explicitly be conveyed or "spelled out." This makes political attribution clear and, to some degree, ensures the U.S. that if it satisfies the attacker's demands, attacks will cease (Glaser, 2011, p. 3). Additionally, Kugler sees it as unlikely that any major cyberattacks or threats on the U.S. will be in a “political vacuum;” instead, they will, he comments, be carried out “with an explicit political and strategic goal” (Kugler, 2009, pp. 317-318).

3.3.3 Cyberwar as a Strategic Means

There are divergent views as to whether cyberwar can be leveraged as means of “brute force,” defined as “measures…in which the damage done by the attack serves as an end in itself,” or “political coercion,” referred as the extraction of “concessions” from the victim (Liff, 2012, p. 403). Scholars also argue whether cyberwar can be used as a potent “force multiplier” at the tactical and operational level (Sharma, 2010, p. 63). While Libicki defines strategic cyberwarfare as “launched by one entity against a state and its society, primarily but not exclusively for the purpose of affecting the target state’s behavior,” he refers to operational cyberwar as “wartime cyberattacks against military targets and military-related civilian targets” (Libicki, 2009, pp. 117-139).

Gartzke argues that cyberwar cannot be used as a means of political coercion due to the very nature of cyberwarfare, such as the difficulty of attribution and inability to cause unacceptable damage, which undermines the credibility of the coercing actor. He suggests that in order for cyberwar to accomplish long-term political objectives that may alter the balance of power, it has to be employed in conjunction with conventional war practices as a force-amplifier. Otherwise, Internet-mediated attacks, he contends, create only a “soft kill,” the effects of which are only temporary (Gartzke, 2013, pp. 57-58). A useful illustration of cyberwar as a force enhancer is provided by Libicki. He speculates that China may initiate a war to invade Taiwan by first executing cyberattacks on the United States’ military networks so that the U.S. cannot step in until China has accomplished its objective (Libicki, 2009, pp. 82-83). Taking all together, Garzke is skeptical about cyberwarfare being a political instrument at a strategic level and serving as an end in itself in pursuit of foreign policy (Gartzke, 2013).

While there is a notable diversity of views among pundits and military leaders about the strategic utility of cyberwar, numerous scholars acknowledge the strategic aspect of cyberwarfare. John Arquilla and David Ronfeldt, for instance, claim that cyberwar can be waged, both for offensive and defensive purposes, not only at a tactical level but also at a strategic level (Arquilla & Ronfeldt, 1993, p. 43). While admitting the low possibility of massive casualties resulting from cyberattacks, Adam P. Liff, accentuates the efficacy of cyberwar as a means of brute force and political coercion. He further adds that as a means of "coercive counter-value weapon," cyberwar can "disable or destroy critical physical infrastructure (e.g., power generators; air traffic control systems)" for strategic purposes (Liff, 2012, pp. 403-404). Moreover, confirming the strategic facet of cyberwarfare, Amit Sharma notes that strategic cyberwar can serve to accomplish "the desired ends" through the imposition of "strategic paralysis" on the adversary's cyber-systems and networks with almost no employment of kinetic instruments. He further adds that cyberwar can also serve as a principal means of accomplishing "grand strategic objectives" in the twenty-first century (Sharma, 2010, pp. 63-72).

Having alluded to the cyberwar literature and defined the term, it is important to consolidate the conceptual landscape pertaining to cyberwar with a case study. To this end, the case of Stuxnet will be discussed in the next section.

3.4. Stuxnet

Exploring the case of Stuxnet is important for three reasons. First, it provides a cogent, definitional justification of cyberwarfare. Second, due to its sophistication and its being the first cyberattack causing physical damage, Stuxnet is believed to be the precursor of a new form of war: Cyberwar (Clayton, 2011). Third, not only did Stuxnet set an example of how destructive a cyber weapon could be, but also it was a vindication of political, strategic, and coercive facets of cyberwarfare (Farwell & Rohozinski, 2011, p. 24; Lewis, 2012, p. 83). Therefore, a brief analysis of the case of Stuxnet will give better insights in understanding the nature of cyberwar as well as what can be feasible with it.

Dubbed as a “mysterious piece of malicious software (malware)” by cyber experts, the worm “Stuxnet” was discovered in 2010 and presented “the most sophisticated” cyber weapon designed for targeting the Iranian nuclear infrastructure located at Natanz (Lindsay, 2013, pp. 365-366). Representing a brand new “fire-and-forget” malicious software that can be leveled against specific targets in the cyber domain, Stuxnet did not require the common Internet connection in order to penetrate the targeted computer-oriented systems. Instead, it infiltrated these systems in the nuclear facility via other instruments (e.g. USB sticks). Leveraging four “zero-day vulnerabilities,” defined as vulnerabilities in software yet to be discovered, the worm is believed to “alternate the frequency of electrical current” powering the enrichment centrifuges (Farwell & Rohozinski, 2011, pp. 24-25). As a consequence, Stuxnet inflicted physical damage on more than a thousand centrifuges in the facility. According to an account, the level of destructiveness of the cyber weapon may have delayed Iran’s aspiration of being a nuclear power to 2015 (Lindsay, 2013, p. 366).

For Stuxnet was the first of its kind capable of causing physical damage, some experts described it as “military-grade cyber missile” fired at the nuclear infrastructure in Iran (Farwell & Rohozinski, 2011, p. 23). In the same vein, some media accounts, according to Lindsay, depicted the worm as “‘the cyber equivalent of the dropping atomic bomb’ and ‘a new era of warfare.’”

This line of thought is manifest in other comments that regard Stuxnet as “the leading edge of cybersecurity in the Revolution in Military Affairs” (Lindsay, 2013, p. 366). So, the bottom line is that the discovery of Stuxnet and its technical performance has proven that cyber weapons are effective means capable of causing physical destruction. Therein lies its strategic importance in terms of its transformative effect on the conduct of foreign affairs and war (Cohen, Freilich, & Siboni, 2016, p. 308). Pertaining to this point, James P. Farwell and Rafal Rohozinski note that the strategic significance of Stuxnet “lies in the insight it offers into the evolution of computer warfare that is occurring far away from Washington’s beltway” (Farwell & Rohozinski, 2011, pp. 25-26).

Along with its destructive capability and strategic characteristics, Stuxnet was also an explicit manifestation of a politically driven cyberattack. Attacks that are political in motive propose to gain advantages (e.g. economic and diplomatic) over an opponent. Attacks of this sort include endeavors to incapacitate critical cyber infrastructure, such as those of government and civilian, to coerce the target for the purposes of extracting political concessions (Cohen, Freilich, & Siboni, 2016, p. 309). In the words of Lukas Milevski, Stuxnet “serves a pioneering purpose and holds the door open for the serious consideration of cyberattack as an instrument of strategy and policy” (Milevski, 2011, p. 65).

The creation of Stuxnet is said to have begun during George W. Bush’s term under the name of Olympic Games program, with an aim to forestall a potential Israeli kinetic attack on Iran’s nuclear power plant. Thus, Stuxnet is, as formerly mentioned, believed to be engineered as a joint effort of Israel and the United States to delay the Iranian nuclear program (Sanger, 2012). This fact indicates that Stuxnet had a political agenda, which was to maintain the balance of power in the Middle East by preventing Iran from acquiring nuclear weapons. It was designed to coerce Iran to cease its nuclear program, with a specific goal of inflicting lasting damage on the enrichment facility so as to extract political concessions. In this respect, one may point to the U.S.-Iran nuclear deal made during Obama's term in 2015 (Said-Moorhouse, 2016) as the fruitful product of Stuxnet's coercive power that persuaded Iran to sign such a deal that ended its nuclear program. After all, it does not appear as fortuitous that Stuxnet could, as previously stated, have delayed Iran's nuclear program to 2015 and that the nuclear deal was reached in the same year.

As a concluding remark, all these accounts of Stuxnet serve as a cogent justification of the offered definitional landscape of cyberwarfare, its aspects, and its strategic and political salience in this study. With that being pointed out, the next section of this work provides useful theory-based accounts and an analysis guided by Power Transition Theory of whether cyber deterrence could be effective in preventing cyberwar between the U.S. and China, and whether cyberwar between the two major powers is imminent under the guidance of Power Transition Theory.

Chapter Four: U.S.- China Cyber Offensive Capabilities and the Level of China's Satisfaction with the Status Quo in Cyberspace

4.0 Objective of the Study: The Main Question and the Fundamental Argument

This study has explored the efficacy of cyber deterrence within the confines of classical deterrence and technical vulnerabilities in cyber systems and networks, and now this analysis will be applied in the context of cyberwar between the U.S. and China. The main question to be answered is: How can Power Transition Theory allow us to better understand the efficacy of cyber deterrence in preventing cyberwarfare between the United States and China? The fundamental argument made in this study is that cyber deterrence is largely an ineffective approach to understanding how best to prevent cyberwar between China and the United States. Applying PTT indicates that China is likely to initiate cyberwar to alter the prevailing status quo in cyberspace in its favor, particularly if it approaches offensive cyberwarfare capability parity with the U.S. while simultaneously remaining dissatisfied with the cyber order.

Based on the thesis statement, there are two variables critical to determining under what conditions cyber deterrence will be ineffective in hindering cyberwar. First, this study analyzes the offensive cyberwar capability of both China and the U.S. to ascertain whether China, as a rising challenger, has reached a parity of cyber offensive warfare capability with the United States. Secondly, this study investigates the level of China's satisfaction with the current status quo in cyberspace.

4.1 Cyber-Offense Power of China and the United States

Offensive cyber capabilities encompass Computer Network Attacks (CNA) and Computer Network Exploitation (CNE). However, as previously emphasized, this study concentrates upon CNA because they can be destructive in nature (Spade, 2011, p. 7). It should be noted that gauging states' cyber-offense power is difficult because states do not overtly make their offensive cyber capabilities a subject matter of discussion for several reasons. Firstly, the demonstration of cyber-offense capabilities, as stated prior, renders them ineffective since adversaries will work on countering them and develop so-called "anti-codes," or fix existing vulnerabilities that might be exploited by the cyber weapons. Secondly, it is usually detrimental to a state's reputation to make it public that it disrupts another state's computer networks and systems or that it spies upon other states. Nonetheless, states do not refrain from investigating and discussing other states' cyber warfare capabilities and what options they have at their disposal, which provides some insights in understanding their offensive cyber warfare power (Hjortdal, 2011, p. 4).

4.1.1 Offensive Cyber Capability of China

Although joining the Internet "relatively late" as opposed to the U.S., China is believed to have swiftly compensated for the time lost. The dramatic increase in the number of Chinese Internet users from two million following the mid-1990s, when the public had, for the first time, access to the Internet, to 538 million in the second half of 2012, is illustrative of China's tremendous leap forward in cyberspace. In parallel to that, Chinese strategists and military analysts equally and rapidly grasped the broader strategic ramifications of ICTs (Inkster, 2013, p. 57). This awakening occurred particularly in the aftermath of Operation Desert Storm in the first half of

1990s, when Chinese decision-makers witnessed the U.S.-led collation's ability to readily "dismantle" the army of Saddam Hussein by the virtue of integrating military cyber systems and computer-oriented networking technology. They came to the realization of "how far behind the state-of-the-art their conventional capabilities had become." From then on, scholars state, an exhaustive modernization effort in the Chinese People's Liberation Army (PLA) ensued. This thrust for modernization in the PLA has also spawned the creation of "an advanced cyberwarfare capability" (Manson, 2011, pp. 121-122).

According to G. P. Manson III, there are several ways to ascertain China's offensive cyber capabilities. One way is the examination of China's effort to place "logic bombs," defined, in the broadest sense, as "malicious code," in other nations' networks. For example, it is speculated that China placed logic bombs in U.S. computer-oriented systems, such as those of power grids and financial systems, in order to activate them when circumstances are right (e.g. during the course of a conflict). This speculation was, Manson notes, acknowledged by Robert Lawless, the former Deputy Undersecretary of Defense, who stressed China's intention to subvert the critical systems of the U.S. through sophisticated cyber instruments (Manson, 2011, p. 123). Similarly, some argue that Chinese's infiltration of computers in over 103 countries to conduct surveillance against the "exiled" Tibetans struggling for an independent Tibet is also a manifestation of China's sophisticated cyber-offense capabilities (Verton, 2008).

Another way to understand China's cyber-offense power is to look at its recruitment of civilian hacker groups. Manson III writes that it was estimated by the 2010 U.S.-China Economic and Security Review Commission that the Chinese Communist Party has around 250 state-backed hacker groups capable of conducting a variety of cyberattacks, ranging from unsophisticated denial-of-service attacks to perplexing cyber espionage. These "patriotic hackers" were purportedly behind the cyberattacks directed at the website of the American Embassy in Beijing in response to the United States' inadvertent bombardment of China's Embassy in Belgrade in 1999 (Manson, 2011, p. 123; Denning, 2001).

A third way to gain insight into China's cyber offensive capabilities is to examine "its role as a major source of manufactured IT hardware to distribute compromised routers and servers abroad." China is known for selling "compromised" cyber technology to some countries in the West. A report by the Federal Bureau of Investigation (FBI) in 2007, according to Manson, sets forth that China wanted to disseminate its compromised ICTs products, such as hardware, abroad by leveraging "its role as a major player in the global IT supply chain" (Manson, 2011, pp. 121-123).

A fourth way to gauge China's cyber offensive warfare capabilities is to scrutinize the formation and training of cyber-units in its military (Manson, 2011, p. 122). In an effort to develop cyberwarfare capability, China has initiated an undertaking in mid-1995 that would make a strategic use of cyberspace: The formation of an Information Warfare (IW) plan. By 2000, IW units were established, and it was said that Beijing was aiming to confront its adversaries in the cyber area by utilizing computer networks for the manipulation of adversaries' information systems (Ball, 2011, p. 81). In 2003, China moved one step further and declared the formation of cyberwarfare units. Clarke and Knake write that around the same time as China's announcement of the new unit, up to 20 terabytes of data from the non-confidential computer networks of the Pentagon were extracted, implying that China was the perpetrator of this cyber espionage, known as "Titan Rain" (Clarke & Knake, 2010, pp. 57-58). Above all, in July 2010, the PLA announced the establishment of an "Information Protection Base." China's decision to create such a base was made soon after the U.S. formed its own Cyber Command (Ball, 2011, p. 81; Branigan, 2010).

The management of the various types of military cyber units created to conduct Computer Network Operations (CNO), based on available information, is handled by “the Third and Fourth departments of the General Staff Department” in the PLA (Domingo, 2016, pp. 158-159). Singer and Friedman remark that the Third Department was established in the 1980s and situated in Beijing; it is akin to the U.S.’ National Security Agency (NSA) and is tasked with “signals intelligence and code-breaking.” They further add that this department is reported to possess around 130,000 personnel (Singer & Friedman, 2014, p. 141). According to Francis E. Domingo, the department’s responsibility also entails computer network exploitation (CNE) and computer network defense (CND) (Domingo, 2016, p. 159).

Moreover, the PLA’s General Department 418th Research Institute is also deemed a key component of China’s cyber units; some even believe that what this unit is to China is what Cyber Command is to the U.S. The unit is said to have subsections. Of those, one unit, called “informationized Blue Team,” draws special attention because it is believed to be formed for the purposes of selecting potential targets for the Chinese cyber units as well as simulating how the United States’ military and its allies utilize the cyber venue. Singer and Friedman also emphasize the significance of the Second Bureau of the Third Army, dubbed the “‘Comment Crew’ or ‘Shanghai Group,’” on the grounds that this unit is responsible for collecting intel on the U.S. with regard to military, economic, and political issues through the utilization of cyber mediums. For example, this unit is known for being caught while trying to infiltrate the computer networks of the *New York Times* in 2013 (Singer & Friedman, 2014, p. 141). As for the PLA’s Fourth Department, it was established in the early 1990s and plays the main role in managing computer network attacks (CNA). The department is also considered the PLA’s “electronic countermeasures” unit. However, the paucity of available information on the main task and future trajectory of these cyber military units and departments should be highlighted (Domingo, 2016, p. 159).

Important to note is that it is widely expressed in the relevant literature that China's build-up of its cyberwarfare capabilities is informed by the PLA's doctrine of asymmetric warfare contained in *Unrestricted Warfare*, produced by two of the PLA's colonels in the late 1990s. According to this warfare strategy, China is and will continue to be incapable of taking on the military might of the United States in a conventional war scenario and, therefore, should, instead, be in pursuit of information dominance that will provide China a substantial asymmetric advantage. In this sense, the PLA's doctrine asserts that the U.S. can be defeated by conventionally inferior China by exploiting its weaknesses or vulnerabilities through cyberattacks (Adams, 2001, pp. 102-103).

Following the examination of China's cyber-offense power, various scholars and experts appear to conclude that China falls far behind the U.S. when it comes to cyberwarfare capabilities. For example, Desmond Ball tracks down the evolution of China's cyber offensive capabilities. Judging by the involvement of China's military and intelligence organizations in cyberattacks and cyber defense practices on computer networks and systems abroad since 1995, Ball concludes that China demonstrated "fairly rudimentary" offensive cyber warfare capabilities, adding that the demonstrated offensive cyberwar power of China proved "little proficiency with more sophisticated hacking techniques" such as the ability to cripple the air defense system of a nation (Ball, 2011). Similarly, some suggest that China's cyber capability is limited because the country still needs to import advanced cyber technology from ICTs companies in the U.S., such as Intel, and, in a broader sense, is dependent on "foreign intellectual property" (Singer & Friedman, 2014, p. 94; Lindsay, Cheung, & Reveron, 2015, p. 3). Others suggest that, in spite of the PLA's swift improvement in cyber offensive power, the U.S. is “second-to-none” when it comes to offensive cyber capabilities (Libicki, 2009, p. 32; Clarke and Knake, 2010, p. 147; Morgan, 2010).

4.1.2 Offensive Cyber Capability of the United States

It is discussed that the U.S. is so superior at cyber offense that some U.S. military officials and experts recently urged that the U.S. ought to concentrate less on offense and more on defense in the cyber venue (Singer & Friedman, 2014, p. 137). While the belief that the U.S. has an incomparable cyber -offense dominance is pervasive and is backed up by some evidence, as is the case with the level of sophistication of Stuxnet, it is still not known to what extent this holds true or how capable the U.S. is in conducting CNA. This ambiguity is due mostly to the classified nature of the cyber offense capabilities of the U.S. Despite Edward Snowden’s 2013 revelations highlighting the level of sophistication of the U.S.’s capability to conduct surveillance on the Internet, very few details are known about the U.S.’s CNA capability, except from the case of Stuxnet (Lindsay, 2014, p. 7). Morgan offers several possible reasons for the secrecy of cyber offensive capability. First, he points out that the U.S. may be reluctant to utilize its cyber offensive instruments so as not to diminish their future efficacy. Second, the U.S. may opt to refrain from using offensive cyber power because of the fear that offensive tools could inform adversaries of how to duplicate these capabilities. As a result, the U.S. may, Morgan comments, seek to leverage “its reputation rather than to show what it can do” (Morgan, 2010, p. 63).

Nevertheless, there are some organizational developments in the accounts of numerous commentators, experts, and government officials that offer considerable insights that can help us understand U.S. offensive cyber power. In a bid for the militarization of cyberspace, the Department of Defense (DoD) sought the simultaneous employment of the U.S. military cyber capabilities, both defensively and offensively, in 2003. Afterwards, the Bush administration decided to task the National Security Agency (NSA), under the auspices of the U.S. Strategic Command, with undertaking offensive cyber operations and, then, transferred this task “to the newly created Joint Functional Component Command-Network Warfare (JFCC-NW) in 2004 under the same command” (Domingo, 2016, pp. 161-162). Of those organizational changes, the creation of the U.S. Cyber Command (USCYBERCOM) has a great significance in terms of demonstrating U.S cyber-offense power. The Pentagon formed the U.S. military’s Cyber Command as a subdivision of Strategic Command in 2010. The U.S. Cyber Command has been mandated to fulfill a wide range of responsibilities. In a broader sense, USCYBERCOM’s mission includes, but is not limited to, the defense of the cyber systems and networks of DoD and carrying out full-fledged military-enabled computer network operations (CNO) so as to allow or facilitate operations in the other realms (O’Connell, 2012, p. 196).

Combining all fragments of the U.S military dealing with cyber matters, ranging from the “Fleet Cyber Command of the Navy to the Army’s Ninth Signal Command”, USCYBERCOM has approximately 60,0000 personnel or, perhaps more correctly, cyber warriors. According to Singer and Friedman, not only has the size of Cyber Command been expanding swiftly, but its perceived significance in the eyes of the U.S. military has also been increasing given the notable rise in the 2014 Pentagon`s spending on Cyber Command. The growth in the perceived importance of USCYBERCOM within the U.S. military possibly warrants Singer and Friedman’s observation that Cyber Command is “a revolutionary new military organization” (Singer & Friedman, 2014, pp. 133-135). In addition to Cyber Command, Lynn notes that prior to 2011, the Defense Advanced Research Projects Agency (DARPA), an agency having made a great contribution to the invention of the Internet, developed the National Cyber Range program to assist the U.S. military in its efforts to “test” cyber offensive instruments, with the aim of maintaining U.S. offensive dominance in the cyber sphere (Lynn, 2010, p. 105).

As earlier stated, while succeeding in conducting unsophisticated cyberattacks, such as defacing web sites and distributed denial-of-service attacks, China is believed to be incapable of orchestrating highly sophisticated cyberattacks such as Stuxnet. On the contrary, the U.S.’s superiority in terms of cyber-offense power is highlighted by various scholars. Of those, Clarke and Knake stand out. They argue that the U.S. is by far ahead of China when it comes to utilizing the most advanced and sophisticated offensive cyber capabilities. They go so far as to speculate that the U.S. is likely to defeat China in a cyberwar scenario. Most important to the analysis in this paper is that Clarke and Knake provide a chart wherein five differing nations are compared based on their cyberwar capabilities.

Table 1 OVERALL CYBER WAR STRENGTH

Nation	Cyber Offense	Cyber Dependence	Cyber Defense	Total
United States	8	2	1	11
Russia	7	5	4	16
China	5	4	6	15
Iran	4	5	3	12
North Korea	2	9	7	18

Note. Adapted from “Cyber War: The Next Threat to National Security and What to do about it,” by R. A. Clarke & R. K. Knake, 2010, New York, NY: HarperCollins, p. 148. Copyright 2010 by Richard A. Clarke and Robert K. Knake.

In this study, the information in Table 1 is considered the basis for the analysis of offensive cyber capabilities of both the U.S. and China. In other words, this study will use Table 1, which scores the cyberwar strength of five states, in the assessment of whether China has approached parity of offensive cyberwarfare capabilities with the U.S.

Having underlined that, the chart measures the cyberwar strength of the five states according to three factors: offense, defense, and dependence. While Clarke and Knake define "Defense" as "a nation's ability to take actions that under attack, actions which will block or mitigate the attack," they measure "Dependence" based on the degree of dependency of a nation on cyber infrastructure--that is, how much a nation is dependent on cyber systems and networks that could have vulnerabilities to exploitation in times of cyber conflict. Each country in the chart receives scores in accordance with Clarke's own evaluation of their defensive capability, offensive capability, and how much they are dependent upon computer systems and networks. Necessary to note here is that if a country's dependency on cyber infrastructure is low, it gets a higher score since being a connected-nation in the cyber realm is deemed a disadvantage in the event of cyberwarfare due to the increased number of potential vulnerabilities in computerized-systems and networks to exploitation (Clarke & Knake, 2010, pp. 147-148).

Upon the analysis of the chart above, it appears that the U.S. receives a higher score for offensive cyber power while China performs relatively poorly in the realm of offensive cyber capabilities. Although China's overall cyberwarfare strength score (15) seems to be greater than that of the U.S. (11), it does not necessarily mean that China has overtaken the U.S. in cyberspace. Because China is far behind the U.S. in relation to cyber offensive power, it is likely to be incapable of executing sophisticated cyberattacks that could wreak more, or equal in scale and scope, havoc on the dominant power than could the U.S. on China. This point is going to made clearer below.

In the light of the analysis above, this study concludes that China as a rising challenger has not yet reached cyber offensive power parity with the U.S. Consequently, China is tenuously deterred and, thus, is unlikely to initiate cyberwarfare unless it reaches a parity of cyber-offense power with its U.S. antagonist. Crucial to the analysis above is that the efficacy of cyber deterrence is tenuous, depending on China's relative cyber-offense capability. The underlying logic of this analysis is, as Power Transition Theory would suggest, that the potential challenger (China) will gauge the odds of winning and losing a cyberwar, and if the possibility of losing cyberwarfare outweighs the chance of winning, owing to the China's weaker offensive cyber power relative to that of the U.S., it, then, follows that cyberwarfare between the dominant power and the rising challenger is unlikely to occur since the initiator of cyberwar will be the challenger, China, which is tenuously deterred.

At this point, one may argue that the U.S. may seek to initiate a preemptive cyberwar against China while it still enjoys cyber-offense power preponderance. Applying Power Transition Theory, this study contends that such preemptive war would disrupt the established cyber system and, thus, would lead to uncertainty among the satisfied system adherents. Once the existing web of cyber relations favorable to the satisfied nations is disrupted, these satisfied nations' support for the status quo would dramatically decline. When the legitimacy of the status quo diminishes, so does the power preponderance of the United States in the cyberspace. Consequently, the U.S. as the dominant power will be unwilling to wage an early cyberwar against China in order not to disrupt the established cyber order by creating uncertainty and causing confusion among its allies. It is in this context that Power Transition Theory refers to the dominant power as risk-averse and unlikely to start a war.

Another possible objection to the analysis above may be that China may seek to launch cyberwar against the U.S. before it catches up to the offensive cyber power level of its adversary given its superiority in cyber defense and the U.S. being the most “plugged in” of all countries, thereby rendering it a more vulnerable target (Valeriano & Maness, 2014, p. 356). The U.S., based on the chart above, suffers from a high degree of dependence on computer networks and systems, and significantly performs poorly concerning cyber defense strength (Clarke & Knake, 2010, p. 147). In other words, the U.S.’s reliance on cyber systems is in sharp contrast to the insufficiency of its defensive power (Mudrinich, 2012, p. 179). From another perspective, China’s cyber systems are mostly owned by the state, thus making it easier for the Chine government to implement a protective and controlling Internet-regime. The level of Chinese government control over the country’s cyber infrastructure is said to give the Chinese Communist Party a considerable advantage because the Party has the capacity to unplug the country’s entire network from the global Internet in the event of cyberattacks or cyberwar, thereby enabling China to possess a daunting cyber defensive capability (Yang, 2009). However, as articulated prior, this is not the case with the dominant power whose cyber infrastructure and systems are, in a great measure, operated by the private sector, thereby limiting its ability to isolate the mainland from global networks if necessary. In consequence, it may be argued that this situation presents the U.S. as an alluring target for the rising challenger, regardless of its superior offensive cyber capabilities, since China supposedly enjoys less dependency on cyber systems and, thus, is less vulnerable to cyberattacks (Manson, 2011).

It may be true that China is less wired and, therefore, less reliant on cyber systems. This means that China may have fewer vulnerabilities to be exploited by potential cyber weapons, defined as computer codes that are “used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living things" (Rid & McBurney, 2012, pp. 6-7). However, it should be recalled that one of the intrinsic characteristics of cyberspace is that offense, as Lynn III aptly puts it, has "the upper hand" (Lynn, 2010, p. 99). For that reason, in order to be able to come out of a cyberwar as a victor, China has to possess, at least, the same cyber-offense power with the U.S., which is not the case currently as the analysis above indicates. More importantly, Power Transition Theory argues that the potential challenger is unlikely to launch a war prior to power parity, as stressed earlier.

Additionally, it may also be true that China has more control over its cyber systems than does the U.S., thus allegedly improving its ability to defend its networks and systems in the case of cyberwarfare. However, it should be noted that there exists no "absolute defense" in the cyber realm due to the fast-evolving nature of cyber technology. Above all, unplugging from the global networks entirely for the purposes of defending cyber systems against cyber threats is an "unrealistic" notion given the nations' pervasive reliance on cyberspace, from financial transactions to communication and the transmission of information on a global scale (Mudrinich, 2012, p. 180).

Following the assessment of whether China has approached a parity of cyber-offense capabilities with the U.S., the second critical variable to be examined so as to understand whether cyber deterrence can be successful, which determines whether cyberwar looms on horizon, is China's level of satisfaction (relative assessment of the status quo) with the existing system in cyberspace.

4.2 China's Degree of Satisfaction with the Prevailing Status Quo in Cyberspace

As underscored in Chapter Two, from Power Transition Theory's perspective, states dissatisfied with the prevailing international system are more likely to engage in non-cooperative interactions with their opponents and the leader nation. While satisfied states are prone to be more cooperative in their relations with each other in a bid for maximizing their "absolute gains," the relations between content and discontented nations are characterized by efforts to maximize their "relative gains" through non-cooperative actions. Therefore, the relationship between a satisfied and dissatisfied nation, or dyad, are, to a great extent, predisposed to be conflictual since their interests reside in conflict (Tammen et al., 2000, pp. 110-111).

Building on the PTT perspective above, this study has investigated the quality of cyber-relations between the U.S. and China in order to determine what characterizes both countries' bilateral relations in cyberspace, whether they are conflictual or cooperative. If China's engagement with the U.S. in the cyber venue is conflictual, it, then, follows that China is dissatisfied with the existing status quo in cyberspace, as Power Transition Theory would suggest. In that case, it will be concluded that the efficacy of cyber deterrence between the U.S. and China will be tenuous because the rising challenger will pursue a revisionist path in the hope of bringing about changes in the cyber order in its favor, rendering cyber deterrence ineffective, which markedly increases the odds of cyberwar.

It is essential at this point to consider the question of how China's level of satisfaction can be measured. Some examine the cyber military build-up of and level of mistrust between China and the U.S. in their bilateral relations in order to understand China's intentions (Manson, 2011; Thomas, 2016; Domingo, 2016). Drawing on research by Brandon Valeriano and Ryan C. Maness featuring cyber conflict among rival states from 2001-2011 (including the updated version of 2015), this study attempts to discern the level of satisfaction of China with the existing status quo in cyberspace by examining the rivalry dyad of the dominant power and the rising challenger to determine whether the latter has been conflictual in its relations with the former.

Table 2 ***Summary of Cyber Disputes among Rival States (2001–2011)***

Rival A (number initiated)	Rival B (number initiated)	Cyber Incidents	Cyber Disputes	Most Severe Dispute	Highest Method Type	Highest Objective	Highest Target Type
China (20)	US (3)	23	5	3	6	2	7
Pakistan (7)	India (6)	13	3	3	4	2	3
North Korea (10)	South Korea (1)	11	3	2	6	1	6
Israel (7)	Iran (4)	11	2	3	6	3	5
China (7)	Japan (0)	7	7	3	4	2	3
South Korea (4)	Japan (3)	7	5	2	3	2	4
US (6)	Iran (1)	7	2	3	6	3	5
China (5)	Taiwan (0)	5	2	2	3	2	2
China (4)	India (0)	4	1	3	6	2	6
Russia (3)	Georgia (1)	4	1	1	5	3	4
Russia (4)	Estonia (0)	4	1	2	2	1	2
Russia (3)	US (0)	3	3	3	4	1	3
North Korea (3)	US (0)	3	1	1	5	1	2
China (2)	Vietnam (0)	2	2	2	4	2	2
Lebanon (1)	Israel (1)	2	2	1	4	1	2
North Korea (1)	Japan (0)	1	1	1	2	1	2
India (1)	Bangladesh (0)	1	1	1	3	3	2
Syria (1)	US (0)	1	1	1	1	1	2
Kuwait (1)	Iraq (0)	1	1	2	4	1	2
China (1)	Philippines (0)	1	1	2	3	2	2

Note. Adapted from “The Dynamic of Cyber Conflict between Rival Antagonists,” by B. G. Valeriano & R. C. Maness, 2015, In *Cyber Hype Versus Cyber Realities: Cyber Conflict in the International System* [eBook] (pp. 78-108). New York, NY: Oxford University Press, p. 89. Copyright 2015 by Oxford University Press.

Prior to discussing the analysis of Table 2, it is necessary to provide information on the methodology of this research to demonstrate its reliability. Valeriano and Maness obtained the data to create the above table from cyber security reports by internet security corporations, such as Symantec and Kaspersky, and sources from media outlets or news, books, and testimonies regarding cyber incidents. A cyber dispute may include a single or a number of cyber incidents .and the initiator of cyberattacks in the analysis is either a government or an entity associated with a government. In addition, non-state actors may be among targets so long as they are deemed crucial to a country’s national security interests (Valeriano & Maness, 2014, pp. 351-356; Valeriano & Maness, 2015, pp. 81-85).

Table 2 contains cyber events between rival countries from 2001 to 2015. It provides a significant insight in understanding the state of China’s satisfaction with the current status quo in cyberspace. Assessing the data, the table indicates that there were 23 cyber incidents between the U.S. and China, with 20 initiated by the latter and only 3 launched by the former. Based on this picture, it appears that China seeks to follow a conflictual path in its relations to the U.S. in cyberspace. Therefore, this study construes China’s conflictual attitude in its cyber engagements with the U.S. as the manifestation of its discontent with the existing status quo in the cyber realm. This conclusion is made based on PTT’s argument that if the challenger is dissatisfied, its engagement with the dominant power is characterized as conflictual because their interests reside in conflict. However, that is not to say that the bilateral relations between the two countries should be seen as entirely non-cooperative and conflictual in the cyber domain. As Nir Kshetr notes, both countries have, nonetheless, engaged in some cooperative actions, albeit seldomly. With the combined efforts of the FBI and Chinese officials, the two states, for instance, accomplished to dissolve and close an illicit child pornography website (Kshetri, 2014, p. 11).

A detailed, or a careful, analysis of Table 2 also provides convincing justification that the U.S. will not be the initiator of cyberwar against China while still enjoying cyber-offense power preponderance in order not to disrupt the cyber order. This assertion is supported by the relatively small number of U.S.-executed cyberattacks directed at China. Ryan C. Maness and Brandan Valeriano aptly make such an observation, noting that in the wake of China's use of cyber conflict in managing its cyber relations with the U.S., the responses from the U.S. seem to be conciliatory, aiming to settle disputes through the means of diplomacy to enhance bilateral relations with the rising challenger (Maness & Valeriano, 2016, p. 303).

Additionally, to fortify the argument that China's relative assessment of the current status quo in cyberspace is negative, it is instructive to look at the debate about where government sovereignty sits in the cyber venue. Also, it will be useful to consider the current Chinese leader's speech addressing the country's state of dissatisfaction with the existing order in cyberspace.

Power Transition Theory contends that both the challenger and the dominant power have conflicting interests, distinct preferences, and varying objectives in pursuits of their external agendas (Tammen et al., 2000). Taking this as a point of departure, the extent to which there exist conflicting preferences over the governance of cyberspace between the U.S. and China is an indication of China's degree of satisfaction with the prevailing status quo in the cyber sphere. So, relevant to this point is the discussion about the fate of governments' sovereignty in cyberspace. The debate about governments' sovereignty in cyberspace revolves around two camps. One camp advocates *the multilateral model* suggesting that governments should wield more control over the Internet, or cyberspace, as a part of sovereignty. The primary advocates of this pole include, but are not limited to, China and Russia (Goldsmith & Wu, 2006). China's main concern is potential cyber threats that could be posed by foreign entities to the country's national security and its very integrity (Lindsay, 2014, pp. 12-14). That is why the proposed Internet governance reforms by Chinese's ruling Communist Party seeks more control over the content of information transmitted through cyber systems by creating an effective mechanism to monitor the Internet. This would bolster the government's authority over the governance of the Internet (Yang, 2009; Wang & Mark, 2015; Lindsay, 2014).

The other camp, however, advocates the *multi-stakeholder model* (Goldsmith & Wu, 2006). The advocates of this model are mainly the U.S. and its Western allies. The multi-stakeholder model is premised on the idea that the Internet is a global "commons." In this model, the involvement of multiple actors, such as private sector entities, academics, and international organizations in Internet governance is fostered to a great extent. More importantly, global Internet management currently relies upon the multi-stakeholder model (Hill, 2014, pp. 16-29), which is believed to be "closely aligned with the U.S. vision of 'an open, interoperable, secure, and reliable' internet" that promotes U.S. interests (Thomas, 2016). For this reason, China strongly opposes the multi-stakeholder model backed by the U.S.; instead, China advocates the multilateral model that conforms to its national preferences in Internet governance. So, core to the argument here is that the existence of conflicting preferences over Internet governance between China and the U.S. and, as a result, the former's aspiration to alter the model on which Internet is currently running can be interpreted as evidence indicating a negative assessment of the existing status quo in the cyber domain on the part of China.

China’s discontent with the status quo in cyberspace can also be illustrated by current Chinese president Xi Jinping’s remarks at the second World Internet Conference held in China in 2015. Addressing the issue of cyber governance, Xi underscored “the primacy of sovereignty” and “gave the current system [in cyberspace] poor marks,” adding that the existing cyber order “does not reflect the desire and interests of the majority of countries,” specifically the desire and interests of China (Tiezzi, 2015).

In conclusion, this analysis has examined the efficacy of cyber deterrence in preventing cyberwar between the U.S. and China, and the prospect for cyberwarfare between them through the lens of Power Transition Theory. The fundamental argument made in this study is that cyber deterrence is mostly an ineffective approach when and if China reaches a parity of cyber offensive capabilities with the U.S. while, concurrently, remaining discontented with the prevailing status quo in cyberspace. This study argues that China will not be deterred in such a case; it will be a risk-taker rather than risk-averse. This situation will increase the odds of cyberwar between the two countries because China will be more willing to wage cyberwar against the U.S. when and if it believes there is a high chance of altering the cyber system in its favor.

Two critical variables were analyzed to better understand the effectiveness of cyber deterrence and the imminence of cyberwar between the two major powers. The first variable under scrutiny was China’s relative cyber-offense power (parity of offensive cyber capability) to that of the U.S. This study concludes that China has not approached parity of cyber offensive warfare capabilities with the U.S. and, thus, is tenuously deterred, diminishing the prospect of cyberwar. The second variable examined was China’s relative assessment of the existing status quo in cyberspace (level of satisfaction). This study concludes that China is dissatisfied with the current status quo. This conclusion indicates that U.S. cyber deterrence is likely to be ineffective in deterring China, thereby increasing the possibility of cyberwar.

It should be noted that China’s degree of dissatisfaction with the order in cyberspace itself alone does not meet the necessary preconditions under which cyberwarfare between the two major players might occur, nor does China reaching parity of offensive cyberwarfare capability with its rival necessarily result in cyberwar. Potential cyberwar is the most likely, or imminent, upon the simultaneous presence of the two variables, namely China’s dissatisfaction and its cyber offense power parity with the United States. This study deduces that the potential outbreak of cyberwarfare between the U.S. and China is currently a remote possibility because the simultaneous presence of both critical conditions is not currently the situation; thus, the U.S. tenuously deters China. In other words, cyber deterrence is tenuously effective in preventing cyberwar between the U.S. and China.

4.3 Conclusion

During the past three decades, the Internet has become ubiquitous, leading to an outstanding increase in global connectivity. This rapid development, coupled with countries’ increasing reliance on ICTs, are said to have transformative impacts upon not only the way societies, governments, and militaries function and interact, and commerce and business are conducted the worldwide, but also upon the way inter-state warfare is fought. This paradigm shift toward interconnectedness on a global scale through the integration of a broad array of areas, ranging from finance to governmental and military affairs, with the Internet indisputably offers numerous advantages and betters the conditions under which nations live in the 21th century. While the expansion of cyberspace poses great opportunities in the Information era, it inevitably poses numerous challenges and dangers to nation-states at the same time by creating considerable security vulnerabilities for possible exploitation by a multitude of actors, both states and non-state. Of those challenges and threats, the danger posed by cyberwar has recently been the focal point of governments and militaries across the globe, specifically in the aftermath of the case of Stuxnet. The U.S., for instance, announced in 2011 that it viewed cyberattack as an act of aggression and accelerated the development of cyber offense and defense capabilities to protect its cyber systems against cyberattacks and cyberwar. China, Russia, and some countries in Europe followed suit.

In attempts to repel the threat posed through cyberspace or cyberwarfare, the cybersecurity community, scholars, and policy-circles in various nations, specifically in the United States, began to search for effective ways of safeguarding cyber systems. Out of these efforts came cyber deterrence theory. Treating the cyber sphere as a warfighting or operational domain, various pundits applied the concepts of classical deterrence to cyberspace in order to inform cyber deterrence theory.

However, not long after the employment of the fundamental principles of Cold War deterrence theories to cyberspace, the abundance of comments skeptical that conventional nuclear and military deterrence theories were applicable to cyberwarfare made numerous scholars doubt the efficacy of cyber deterrence. In parallel to this increased skepticism, many came to the realization that the complexity of cyberspace and, for that matter, cyberwar, did not allow a successful application of Cold War deterrence theories, particularly deterrence-by-punishment and deterrence-by-denial, to the cyber realm. This is because when it comes to cyberwarfare, the very fundamental and necessary elements of classical deterrence, namely credibility, capability, and communication of menacing massages to the would-be challenger, are not present due to the distinctive characteristics of cyberspace. Of those intrinsic characteristics, the most articulated ones are the ambiguity of the source of attacks, the anonymity of the potential cyber offender, high technological volatility, the ubiquity of computer networks and systems, the asymmetric and complex nature of cyberspace, and finally the immaturity of international laws, rules, and norms. For example, the credibility of deterrence by punishment is undermined due to the difficulty of attributing the source of the attack, the anonymity of the potential attacker, and the asymmetry between the defending party and the challenger. Similarly, the inadequacy of international rules and norms that define an appropriate code of conduct in cyberspace, the lack of cross-borders cooperation for the investigation of cybercrimes, and the absence of international configurations for inspection purposes render credibility and communication of cyber deterrence ineffective. Therefore, there is a common perception in the pertinent literature that cyberspace ought to be approached on its own merit; it has distinctive characteristics that render the Cold War deterrence theories ill-suited for cyberspace.

In the wake of this skepticism, different strategies and policy constructs have been deliberately considered to increase the efficacy of cyber deterrence. On the one hand, some have suggested the application of serial deterrence, expanded deterrence, tailored deterrence, active defense, and deterring specific cyber weapons in addition to deterrence by kinetic means. Even, re-configuring the very architecture of the Internet has been suggested. On the other hand, others take a constructivist approach and focus more on human factors and, for that matter, the social construction of cyber threat perception rather than on technical difficulties of the cyber domain.

However, the problem with the existing literature is that the vast volume of the studies usually analyzed the efficacy of cyber deterrence within the theoretical framework of classical deterrence and technical vulnerabilities in cyber systems. The bulk of these studies lacked a rigorous theoretical perspective because they were from policy-circles and because historical cyber incidents are insufficient to develop an independent cyber-based theory. This theory-policy vacuum is more evident in regards with doomsday scenarios, specifically in the context of cyberwar between the U.S. and China. Although some scholars have provided useful insights into potential cyberwarfare scenarios between China and the U.S., particularly over the issue of Taiwan, these insights suffered significantly from a lack of a robust theoretical approach. Thus, the purpose of this study has been to address the issue outside the limits of classical deterrence and vulnerabilities in networks and systems, and to bridge this theory-policy gap by examining the effectiveness of cyber deterrence between the U.S. and China through the lens of Power Transition Theory.

Power Transition Theory is relevant to the discussion on cyberwarfare and cyber deterrence for two main reasons. First, because PTT is a probabilistic theory that explains under what conditions power transition from the dominant power to the rising challenger is likely to lead to a system-wide war in the real world, it can be a useful theoretical framework for the examination of the success or failure of cyber deterrence in preventing cyberwar between China and the United States. Second, the relevancy of PTT lies in the fact that Cold War classical deterrence is the very basis for cyber deterrence theory while PTT has been critical of some tenets of classical deterrence. So, this makes PTT relevant to the analysis here.

PTT contends that the classical deterrence concept of MAD did not make war prohibitive; but, instead, nuclear war did not occur because the USSR never approached national power parity with the U.S. before its dissolution. In PTT, power parity between the preeminent nation and the challenger is one of the required conditions that ought to be present prior to the outbreak of power transition warfare. In fact, according to PTT, there are several critical variables that dictate the success of deterrence. The challenger's level of satisfaction with the status quo and whether it has reached power parity with the dominant power, however, have the utmost importance and pertinence to this study.

Applying PTT to cyberspace, the theory would suggest that cyber deterrence in the context of cyberwar between China and the U.S. will be tenuous under the simultaneous presence of the two conditions. Once China achieves parity in cyber offensive warfare capabilities with the U.S. while, at the same time, remaining discontented with the existing status quo in cyberspace, China will not be deterred and, rather, will become a risk-taker trying to alter the order in cyberspace in its favor. This would cause cyber deterrence to fail, making cyberwar very likely. After analysis of China's satisfaction level with the prevailing status quo in the cyber sphere and its relative cyber-offense power to that of the U.S., this study concludes that while China notably exhibits a certain level of dissatisfaction with the international *cyber* system, it seems not to have approached a parity of offensive cyber capabilities with the United States. China falls far behind the U.S. in terms of cyber offensive warfare power. Hence, China is tenuously deterred. As a corollary of this, this study contends that an outbreak of cyberwar between the U.S. and China is a remote possibility in the foreseeable future.

Despite being currently non-conducive to cyberwar, the international cyber system might see cyberwar once China as a rising contender reaches a parity of offensive cyber capabilities with the dominant power while still remaining dissatisfied with the existing status quo in the cyber system. One possible, and perhaps a utilitarian, way to prevent future cyberwar between the U.S. and China is, as Power Transition Theory would suggest, to make the current status quo in cyberspace favorable to the rising contender to enhance its satisfaction. China is rising rapidly, both in the kinetic and virtual world. Essentially, it will demand a greater share of benefits from the cyber domain commensurate with its growing cyber power and influence. As the main cyber rule maker, the U.S. can play a facilitator role in turning China's negative assessment of the existing cyber order into a positive view. In this sense, the U.S. government might consider revising its 2015 DoD Cyber Strategy, in which classical deterrence notions are the points of departure in creating the nation's cyber policy (Department of Defense, 2015). Instead, Washington should provide positive incentives to China to be more cooperative on the cyber issues. The dominant power ought to take into account China's preferences for the governance of cyberspace and Internet economies because the increased cooperation between the two states can make the status quo in the cyber realm more favorable to the challenger. This would marginalize areas where there are dramatic disagreements between the two. More to the point is that the U.S. should try to find ways to cooperate with China to specifically set rules and norms to govern cyberspace for the purposes of dispersing more satisfaction in the cyber system.

Cooperating with China to establish rules and norms governing the cyber sphere requires political convergence. The United State can accomplish this through manipulating economic incentives, as suggested by PTT and discussed in Chapter One. Economic associations with China that govern the internet economy can foster such political convergence by creating economic benefits that catalyze economic growth, thus enhancing China's satisfaction. More specifically, in managing China's satisfaction with the cyber order, the U.S. may leverage globalization as a means to help China grow private ICTs enterprises. A growing Chinese private sector that manufactures ICT-related products would influence China's calculus of national security interests. Therefore, a Chinese ICT business sector integrated with the global economy would be a disincentive for Chinese government and military to act aggressively in the cyber venue. For a strong ICT private sector to grow in China, the United States can utilize information technologies to penetrate Chinese borders and generate information constituencies, perhaps facilitating the decentralization and democratization of Chinese government, as well as free enterprise. This would, in turn, spread satisfaction.

The United States can ensure China’s satisfaction through China’s integration into an alliance or offering opportunities that may help China socialize into the prevailing cyber system. China would, then, be more willing to abide by the existing rules and norms governing cyber space. In this sense, China may be integrated into NATO’s extended cyber deterrence doctrine (Kramer, Butler, & Lotrionte, 2016), which would enhance China’s satisfaction level.

In terms of managing cyber offensive power capability, the dominant power can resort to expanding its Western alliance block, which will put more resources at its disposal in order to maintain its cyber-offense power preponderance over China in cyberspace. Combining its cyber power with that of European countries and allies around the world can help the U.S. remain ahead of China. Again, NATO’s collective cyber defense policy under the extended deterrence doctrine can be a viable tool in forging such an alliance. Integrating Russia and India into this alliance could dramatically increase the pool of resourses available to the United States to maintain its cyber power preponderance. This could, as PTT would suggest, also contribute to Russia and India staying satisfied nations, which would likely prevent China from establishing a coalition with these countries against the United States in cyberspace. In addition, acting with allies can dramatically contribute to the U.S.’s offensive cyberwar capability. The case of Stuxnet is informative in this respect. Stuxnet is, as stated formerly, the most advanced cyber weapon—the first to cause physical destruction-- and this effective worm was designed by the joint effort of the U.S. and its ally Israel, thus indicating the significance and effectiveness of combining resources with allies to manage cyber offensive power and combat against any common threat.

Despite the major role the U.S. can play in the prevention of cyberwar, the global community should also bear some responsibility for ensuring a peaceful *cyber* power transition between the U.S. and China if the transition is inevitable. This can be achievable through taking a conciliatory stance toward cyber disputes between the U.S. and China, specifically over the governance of the Internet and embracing China as a member of the international community, not as an adversary of the West and the values it holds. A peaceful cyber power transition can also be accomplished by promoting more cooperative and corroborative discourse, as well as undertakings with China on cyber-related issues, such as cyber terrorism and cyber espionage, and cooperatively combatting mutually recognized crimes committed online (e.g. child pornography), which may increase transparency and utilitarian interactions. This will increase China's level of satisfaction. Ultimately and, more importantly, the international community can achieve such a goal through working in tandem with the U.S. in order to remove the barriers to a fair diffusion of power in cyberspace.

The international community should act because potential cyberwar between the U.S. and China can jeopardize the global order, security, and peace. In the economic realm, ICTs already play a critical role in the proper functioning of the global economy. In global trade, e-commerce has been growing exponentially; a significant volume of global financial transactions is made through the Internet and other communication and information networking (Choucri, 2000, pp. 246-252; Choucri, 2012). The U.S. and China are considered the backbone of the global economy. Specifically, the U.S. is the hub of global economic activities. Potentially crippling cyberattacks on U.S. financial networks and systems in the context of cyberwar against China may have far-reaching consequences for the global web of economic relations. A disrupted, unstable global economy may be followed by political disorder across nations, thus immensely destabilizing the existing order both in the kinetic and virtual world. Perhaps, this would be the worst-case scenario in which it would be apt to say that, "welcome to the era of *power transition cyberwarfare."*

The implications of this study can potentially bring the different strands of International Relations (IR) theories, such as Liberalism and Constructivism, together in order to explain the practicality of the policy implications and how they can be actualized. For example, Liberalism can provide a useful explanation of how NATO as an international organization can absorb China under extended deterrence doctrine or how economic interdependency in cyberspace can lead to political convergence. In the same vein, Constructivism can explain how both countries domestically construct cyberspace through their own subjective understanding. Because the paucity of space in this study does not allow such a breadth of analysis, future research will concentrate on blending these distinct IR schools in a practical and pragmatic way to address the issues.

References

Adams, J. (2001). Virtual defense. *Foreign Affairs*, *80*(3), 98-113.

Ambach, P., Bostedt, F., Dawson, G., & Kostas, S. (Eds.). (2015). *The protection of non-combatants during armed conflict and safeguarding the rights of victims in post-conflict society : Essays in honour of the life and work of Joakim Dungel* [e-Book]. Leiden, AN: Brill.

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming!. In J. Arquilla & D. Ronfeldt (Eds.), *In Athena's camp: Preparing for conflict in the information age* (pp. 22-60). Arlington, VA: RAND Corporation.

Babacan, N. (2017, May 18). Turkey to form 'cyber army' against possible cyberattacks: Minister. *Hurriet Daily News.* Retrieved from http://www.hurriyetdailynews.com/turkey-to-form-cyber-army-against-possible-cyberattacks-minister-.aspx?pageID=238&nID=113252&NewsCatID=374

Ball, D. (2011). China's cyber warfare capabilities. *Security Challenges*, *7*(2), 81-103.

Bartos, C. A. (2016, June). Cyber weapons are not created equal. *Proceeding*s, *142*(6), 30-33. Retrieved from https://www.usni.org/magazines/proceedings/2016-06/cyber-weapons-are-not-created-equal

Beidleman, S. W. (2009). *Defining and deterring cyber war*. Carlisle Barracks, PA: U.S. Army War College. Retrieved from http://indianstrategicknowledgeonline.com/web/DEFINING%20AND%20DETERRING%20cyber%20war.pdf

Bendiek, A. (2012). *European cyber security policy*. Berlin, DE: German Institute for International and Security Affairs. Retrieved from https://www.swp-berlin.org/fileadmin/contents/products/research_papers/2012_RP13_bdk.pdf

Bendiek, A., & Metzger, T. (2015). Deterrence theory in the cyber-century: Lessons from a state-of-the-art literature review. Berlin, DE: German Institute for International and Security Affairs. Retrieved from https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/Bendiek-Metzger_WP-Cyberdeterrence.pdf

Betz, D. J. (2006). The more you know, the less you understand: The problem with information warfare. *Journal of Strategic Studies*, *29*(3), 505-533. doi:10.1080/01402390600765900

Blank, S. (2001). Can information warfare be deterred?. *Defense Analysis, 17(2)*, 121-138. doi:10.1080/07430170120064212

Blumenthal M. S., & Clark, D. D. (2009). The future of the internet and cyberpower. In F. D. Kramer, S. H. Starr, & L. K. Wentz (Eds.), *Cyberpower and national security* (pp. 206-240). Washington, DC: Potomac Books.

Blumenthal, M. S. (2012, Spring). Who should govern the internet? [Review of the book *Networks and states: The global politics of internet governance* by M. L. Mueller]. *Issues in Science And Technology*, *28*(3), 89-92.

Bologna, S., Fasani, A., & Martellini, M. (2013). From fortress to resilience. In M. Martllini (Ed.), *Cyber security: Deterrence and IT protection for critical infrastructures* [e-Book] (pp. 53-56). New York, NY: Springer.

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, *9*(2), 27-40. doi:10.3316/QRJ0902027

Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation*, 34(7), 342-353. https://doi.org/10.1016/j.technovation.2014.02.001

Branigan, T. (2010, July 22). Chinese army to target cyber wat threat: New department dedicated to protecting information security follows creation of US cyber command. *The Guardian*. Retrieved from https://www.theguardian.com/world/2010/jul/22/chinese-army-cyber-war-department

Bumiller, E., & Shanker, T. (2012, October 11). Panetta warns of dire threat of cyberattack on U.S. *The New York Times.* Retrieved from http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html

Bunn, M. E. (2007). Can deterrence be tailored?. *Strategic Forum*, *225*, 1-8. Retrived from http://cyberanalysis.pbworks.com/f/SF225.pdf

Cai, C., & Dati, D. (2015). Words mightier than hacks: Narratives of cyberwar in the United States and China. *Asian Perspective*, *39*(3), 541-553.

Calvo, A. (2014). Cyberwar is war: A critique of “Hacking can reduce real-world violence”. *Small Wars Journal*. Retrieved from smallwarsjournal.com/printpdf/15514

Caton, J. L. (2013). Exploring the prudent limits of automated cyber attack. In K. Podins, J. Stinissen, & M. Maybaum (Eds.), *Cyber conflict* (pp. 1-16). Tallinn, EE: NATO Publications.

Cebrowski, A. K. (2002). CNE and CNA in the network-centric battlespace: Challenges for operators and lawyers. In M. N. Schmitt & B. T. O’Donnell (Eds.), *Computer network attack and international law* (pp. 1-6). Newport, RI: Naval War College.

Chertoff, M. (2010, March 10). Cyber shockwave exposed missing links in U.S. security. *Government Computer News*. Retrieved from https://gcn.com/articles/2010/03/15/commentary-chertoff-cyber-shockwave.aspx

Cheswick, W. R., Bellovin, S. M., & Rubin, A. D. (2003). *Firewalls and internet security: Repelling the wily hacker* (2nd ed.). Boston, MA: Pearson.

Choucri, N. (2000). Introduction: CyberPolitics in international relations. *International Political Science Review*, *21*(3), 243-263.

Choucri, N. (2012). *Cyberpolitics in international relations*. Cambridge, MA: MIT press.

Cimbala, S. J. (2014). Nuclear deterrence and cyber: The quest for concept. *Air & Space Power Journal*, *28*(2), 87-107.

Clark, D. (2010). Characterizing cyberspace: Past, present and future. *MIT CSAIL*. Retrieved from http://docshare01.docshare.tips/files/9608/96080638.pdf

Clark, D. D., & Landau, S. (2011). Untangling attribution. In National Research Council, *Proceedings of a workshop on deterring cyberattacks: Informing strategies and developing options for U.S. policy*. Washington, DC: National Academies Press. https://doi.org/10.17226/12997

Clark, W. K., & Levin, P. L. (2009). Securing the information highway: How to enhance the United States' electronic defenses. *Foreign Affairs*, *88*(6), 2-6, 8-10.

Clarke, R. A. & Knake, R. K. (2010). *Cyber war: The next threat to national Security and what to do about it.* New York, NY: HarperCollins.

Clayton, M. (2011, March 7). The new cyber arms race. *The Christian Science Monitor*. Retrieved from https://www.csmonitor.com/USA/Military/2011/0307/The-new-cyber-arms-race

Cohen, M. S., Freilich, C. D., & Siboni, G. (2016). Israel and cyberspace: Unique threat and response. *International Studies Perspectives*, *17*(3), 307-321. doi:10.1093/isp/ekv023

Crosston, M. D. (2011). World gone cyber MAD: How “mutually assured debilitation” is the best hope for cyber deterrence. *Strategic Studies Quarterly*, *5*(1), 100-116.

Dal, S., & Ozyurt, K. (2014). NATO article statue 5 in terms of a cyber-war. In A. Liaropoulos & G. Tsihrintzis (Eds.*), Proceedings of the 13th European conference on cyber warfare and secuirty* (pp. 311-314). Reading, UK: Academic Conferences and Publishing International Limited. Retrieved from https://cryptome.org/2014/12/ECCWS2014.pdf

Davis, P. K. (2014). Deterrence, influence, cyber attack, and cyberwar. *New York University Journal of International Law and Politics*, *47*(2), 327-356.

Deibert, R. J., Rohozinski, R., & Crete-Nishihata, M. (2012). Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war. *Security Dialogue, 43*(1), 3-24. doi:10.1177/0967010611431079

Denning, D. E. (2001). Cyberwarriors: Activists and terrorists turn to cyberspace. *Harvard International Review*, *23*(2). 70-75.

Denning, D. E. (2015). Rethinking the cyber domain and deterrence. *Joint Force Quarterly, 77*(2), 8-15.

Department of Defense. (2011). Department of Defense strategy for operating in cyberspace. Retrieved from https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf

Department of Defense. (2015). The Department of Defense cyber strategy. Retrieved from https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy/

Department of Homeland Security. (2016). What is critical infrastructure?. Retreived from https://www.dhs.gov/what-critical-infrastructure

Doherty, S. (2015, March 31). Why cyber defense ultimately rests with the private sector. *FCW Magazine*. Retrieved from https://fcw.com/articles/2015/03/31/private-sector-cyber.aspx

Domingo, F. C. (2016). Conquering a new domain: Explaining great power competition in cyberspace. *Comparative Strategy*, *35*(2), 154-168. doi:10.1080/01495933.2016.1176467

Elliott, D. (2011). Deterring strategic cyberattack. *IEEE Security & Privacy, 9*(5), 36-40. doi:10.1109/MSP.2011.24

Eriksson, J., & Giacomello, G. (2006). The information revolution, security, and international relations: (IR) relevant theory?. *International Political Science Review*, *27*(3), 221-244. doi:10.1177/0192512106064462

Etzioni, A. (2014). The private sector: A reluctant partner in cybersecurity. *Institute for Communitarian Policy Studies*. Retrieved from https://icps.gwu.edu/private-sector-reluctant-partner-cybersecurity

Eun, Y. -S. & Abmann, J. S. (2016). Cyberwar: Taking Stock of Security and Warfare in the Digital Age. *International Studies Perspectives*, *17*(3), 343-360. doi:10.1111/insp.12073

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the tuture of cyber war. *Survival*, *53*(1), 23-40. doi:10.1080/00396338.2011.555586

Freedman, L. (2004). *Deterrence.* Cambridge, UK: Polity Press.

Fritz, J. (2008). How China will use cyber warfare to leapfrog in military competitiveness. *Culture Mandala: The Bulletin of the Centre for East-West Cultural and Economic Studies, 8*(1), 28-80.

Gartzke, E. (2013). The myth of cyberwar: Bringing war in cyberspace back down to Earth. *International Security, 38*(2), 41-73. doi:10.1162/ISEC_a_00136

Gartzke, E., & Lindsay, J. R. (2015). Weaving tangled webs: Offense, defense, and deception in cyberspace. *Security Studies, 24*(2), 316-348. doi:10.1080/09636412.2015.1038188

Geers, K. (2010). The challenge of cyber attack deterrence. *Computer Law & Security Review*, 26(3), 298-303. doi:10.1016/j.clsr.2010.03.003

Geiß, R., & Lahmann, H. (2012). Cyber warfare: Applying the principle of distinction in an interconnected space. *Israel Law Review, 45*(3), 381-399. https://doi.org/10.1017/S0021223712000179

Geist, E. (2015). Deterrence stability in the cyber age. *Strategic Studies Quarterly, 9*(4), 44-61.

Gelles, M. G. (Ed.). (2016). *Insider threat: Prevention, detection, mitigation, and deterrence*. Oxford, UK : Butterworth-Heinemann.

George, A. L., & Smoke, R. (1974). *Deterrence in American foreign policy: Theory and practice*. New York, NY: Columbia University Press.

Gervais, M. (2012). Cyber attacks and the laws of war. *Berkeley Journal of International Law, 30*(2), 525-579. https://doi.org/10.15779/Z38R66C

Glaser, C. L. (2011). Deterrence of cyber attacks and U.S. national security. *The George Washington University Cyber Security Policy and Research Institute*. Retrieved from http://www.offnews.info/downloads/2011-5CyberDeterrenceGlaser.pdf

Goldsmith, J., & Wu, T. (2006). *Who controls the internet*?*: Illusions of a borderless world* [eBook]. New York, NY: Oxford University Press.

Goldstein, G. -P. (2013). Cyber defense from "reduction in asymmetrical information" strategies. *Military and Strategic Affairs, 5*(3), 129-155.

Goodman, W. (2010). Cyber deterrence: Tougher in theory than in practice?. *Strategic Studies Quarterly, 4*(3), 102-135.

Graham, D. E. (2010). Cyber Threats and the Law of War. *Journal Of National Security Law & Policy*, *4*(1), 87-102.

Gross, M. J. (2011). A declaration of cyber-war. *Vanity Fair*. Retrieved from https://www.vanityfair.com/news/2011/03/stuxnet-201104

Hare, F. (2012). The significance of attribution to cyberspace coercion: A political perspective. In C. Czosseck, R. Ottis, & K. Ziolkowski (Eds.), *Cyber conflict* (pp. 125-139). Tallinn, EE: NATO Publications. Retrieved from https://ccdcoe.org/cycon/2012/proceedings/d2r1s2_hare.pdf

Harknett, R. J. (1996). Information warfare and deterrence. *Parameters*, *26*(3), 93–107.

Hill, R. (2014). The internet, its governance, and the multi-stakeholder model. *Info, 16*(2), 16-46. doi:10.1108/info-05-2013-0031

Hjortdal, M. (2011). China's use of cyber warfare: Espionage meets strategic deterrence. *Journal of Strategic Security*, *4*(2) 1-24. http://dx.doi.org/10.5038/1944-0472.4.2.1

Hollis, D. B. (2007). Why states need an international law for information operations. *Lewis & Clark Law Review, 11*(4), 1023-1061.

Hollis, D. B. (2011). An e-SOS for cyberspace. *Harvard International Law Journal, 52*(2), 373-432.

Hollis, D. M. (2010). USCYBERCOM: The need for a combatant command versus a subunified command. *U.S. Army*. Retrieved from https://www.army.mil/article/41585/uscybercom_the_need_for_a_combatant_command_versus_a_subunified_command

Hughes, R. (2010). A treaty for cyberspace. *International Affairs*, *86*(2), 523-541. doi:10.1111/j.1468-2346.2010.00894.x

Iasiello, E. (2014). Is cyber deterrence an illusory course of action?. *Journal of Strategic Security, 7*(1), 54-67. doi:10.5038/1944-0472.7.1.5

Inkster, N. (2013). Chinese intelligence in the cyber age. *Survival, 55*(1), 45-65. doi:10.1080/00396338.2013.767405

International Institute for Strategic Studies. (2016). Cyber conflict and deterrence. *Strategic Comments, 22*(7), iii-v. doi:10.1080/13567888.2016.1237761

Jackson, D. (2016, December 29). Obama sanctions Russian Officials over election hacking. *USA Today*. Retrieved from https://www.usatoday.com/story/news/politics/2016/12/29/barack-obama-russia-sanctions-vladimir-putin/95958472/

Jackson, V. (2014). Power, trust, and network complexity: Three logics of hedging in Asian security. *International Relations of the Asia-Pacific, 14*(3), 331-356. https://doi.org/10.1093/irap/lcu005

Jasper, S. (2015). Deterring malicious behavior in cyberspace. *Strategic Studies Quarterly*, *9*(1), 60-85.

Jensen, E. T. (2012). Cyber deterrence. *Emory International Law Review, 26*(2), 773-824.

Jensen, E. T. (2013). Cyber attacks: Proportionality and precautions in attack. *International Law Studies*, *89*, 198-217.

Johnson, J. B., & Reynolds, H. T. (2012). *Political science research methods* (7th ed.). Washinton, DC: CQ Press.

Joshi, R. C., & Sardana, A. (Eds.). (2011). *Honeypots: A new paradigm to information security* [eBook]. Enfield, NH: Science Publishers.

Kaiser, R. (2015). The birth of cyberwar. *Political Geography*, *46*, 11-20. doi:10.1016/j.polgeo.2014.10.001

Kang, K., & Kugler, J. (2015). Assessment of deterrence and missile defense in East Asia: A power transition perspective. *International Area Studies Review*, *18*(3), 280-296. doi:10.1177/2233865915595762

Keen, J. F. (2015). Conventional military force as a response to cyber capabilities: On sending packets and receiving missiles. *Air Force Law Review*, *73,* 111-150.

Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft. *International Security*, *38*(2), 7-40. doi:10.1162/ISEC_a_00138

Kesan, J. P., & Hayes, C. M. (2012). Mitigating counterstriking: Self-defense and deterrence in cyberspace. *Harvard Journal of Law and Technology*, *25*(2), 415-529.

Keyser, M. A. (2003). Convention on cybercrime. *Journal Of Transnational Law & Policy*, *12*(2), 287-326.

Kim, W. (2015). Rising China, pivotal middle power South Korea, and alliance transition theory. *International Area Studies Review*, *18*(3), 251-265. doi:10.1177/2233865915595531

Kim, W., & Gates, S. (2015). Power transition theory and the rise of China. *International Area Studies Review*, *18*(3), 219-226. doi:10.1177/2233865915598545

Klein, A. G. (2015). Vigilante media: Unveiling anonymous and the hacktivist persona in the global press. *Communication Monographs*, *82*(3), 379-401. doi:10.1080/03637751.2015.1030682

Kosenkov, A. (2016). Cyber conflict as a new global threat. *Future Internet*, *8*(3), 1-9. doi:10.3390/fi8030045

Kott, A. (2014). Towards fundamental science of cyber security. In R. E. Pino (Ed.), *Network science and cybersecurity* [eBook] (pp. 1-13). New York, NY: Springer.

Kramer, F. D., Butler, R. J., & Lotrionte, C. (2016). *Cyber, extended deterrence, and NATO*. Washington, DC: Atlantic Council. Retrieved from http://www.atlanticcouncil.org/images/publications/Cyber_Extended_Deterrence_and_NATO_web_0526.pdf

Kramer, F. D. (2009). Cyberpower and national secuirty: Policy recommendations for a strategic framework. In F. K. Kramer, S. H. Starr, & L. K. Wentz (Eds.), *Cyberpower and national security* (pp. 3-23). Washington, DC: Potomac Books.

Kshetri, N. (2014). Cybersecurity and international relations: The U.S. engagment with China and Russia. Retrieved from http://web.isanet.org/Web/Conferences/FLACSO-ISA%20BuenosAires%202014/Archive/6f9b6b91-0f33-4956-89fc-f9a9cde89caf.pdf

Kuebl, D. T. (2009). From cyberspace to cyberpower: Definin the problem. In F. K. Kramer, S. H. Starr, & L. K. Wentz (Eds.), *Cyberpower and national security* (pp. 24-42). Washington, DC: Potomac Books.

Kugler, J., & Lemke, D. (1996). *Parity and war: Evaluations and extensions of the war ledger*. Ann Arbor, MI: University of Michigan Press.

Kugler, R. L, (2009). Deterrence of cyber attacks. In F. K. Kramer, S. H. Starr, & L. K. Wentz (Eds.), *Cyberpower and national security* (pp. 309-340). Washington, DC: Potomac Books.

Kwalwasser, H. (2009). Internet governance. In F. K. Kramer, S. H. Starr, & L. K. Wentz (Eds.), *Cyberpower and national security* (pp. 491-524). Washington, DC: Potomac Books.

Lakhani, K. R., & Wolf, R. G. (2005). Why hackers do what they do: Understanding motivation and effort in free/open source software projects. In J. Feller, B. Fitzgerald, S. A. Hissam, & K. R. Lakhani (Eds.), *Perspectives on free and open source software* (pp. 3-21). Cambridge, MA: MIT Press.

Lan, T., & Xin, Z. (2010). Can cyber deterrence work? In T. Lan, Z. Xin, H. D. Raduege, Jr., D. I. Grigoriev, P. Duggal, & S. Schjølberg, *Global cyber deterrence: Views from China, the U.S., Russia, India, and Norway*. New York, NY: The EastWest Institute.

Lee, S. -H. (2015). Global and regional orders in the 21st century in terms of multi-layered power transition theory: The cases of US–China and China–Japan relations. *International Area Studies Review, 18*(3), 266-279.

Lewis, J. A. (2010). Sovereignty and the role of government in cyberspace. *Brown Journal of World Affairs, 16*(2), 55-65.

Lewis, J. A. (2012). In defense of Stuxnet. *Military and Strategic Affiars*, 4(3), 65-76.

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. Santa Monica, CA: RAND Corporation.

Liff, A. P. (2012). Cyberwar: A new ‘absolute weapon’? The proliferation of cyberwarfare capabilities and interstate war. *Journal of Strategic Studies*, *35*(3), 401-428. doi:10.1080/01402390.2012.663252

Lilienthal, G., & Ahmad, N. (2015). Cyber-attack as inevitable kinetic war. *Computer Law & Security Review*, *31*(3), 390-400. doi:10.1016/j.clsr.2015.03.002

Lim, Y. -H. (2015). How (dis)satisfied is China? A power transition theory perspective. *Journal of Contemporary China*, *24*(92), 280-297. doi:10.1080/10670564.2014.932160

Limnéll, J. (2016). *Developing a proportionate response to a cyber attack*. Aalto, FI: Aalto University. Retrieved from https://aaltodoc.aalto.fi/handle/123456789/19849

Lin, H. (2016). Attribution of malicious cyber incidents: From soup to nuts. *Journal of International Affairs*, *70*(1), 75-137.

Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies*, *22*(3), 365-404. doi:10.1080/09636412.2013.816122

Lindsay, J. R. (2014). The impact of China on cybersecurity: Fiction and friction. *International Security*, *39*(3), 7-47. doi:10.1162/ISEC_a_00189

Lindsay, J. R. (2015). Tipping the scales: The attribution problem and the feasibility of deterrence against cyberattack. *Journal of Cybersecurity*, *1*(1), 53-67. doi:10.1093/cybsec/tyv003

Lindsay, J. R., Cheung, T. M., & Reveron, D. S. (Eds.). (2015). *China and cybersecurity: Espionage, strategy, and politics in the digital domain.* New York, NY: Oxford University Press.

Lobel, H. (2012). Cyber war inc.: The law of war implications of the private sector's role in cyber conflict. *Texas International Law Journal*, *47*(3), 617-640.

Lupovici, A. (2011). Cyber warfare and deterrence: Trends and challenges in research. *Military and Strategic Affairs*, *3*(3), 49-62. Retrieved from https://i-hls.com/wp-content/uploads/2013/02/Cyber-Warfare-and-Deterrence.pdf

Lupovici, A. (2016). The "attribution problem" and the social construction of "violence": Taking cyber deterrence literature a step forward. *International Studies Perspectives*, *17*(3), 322-342. doi:10.1111/insp.12082

Lynn, W. J., III. (2010). Defending a new domain: The Pentagon's cyberstrategy. *Foreign Affairs*, *89*(5), 97-108.

Lynn, W. J., III. (2011). The Pentagon's cyberstrategy, one year later: Defending against the next cyberattack. *Foreign Affiars.* Retrieved from http://globalpublicsquare.blogs.cnn.com/2011/10/03/the-pentagons-cyberstrategy-one-year-later/

Maness, R. C., & Valeriano, B. (2016). The impact of cyber conflict on international interactions. *Armed Forces & Society*, *42*(2), 301-323. doi:10.1177/0095327X15572997

Manson, G. P., III. (2011). Cyberwar: The United States and China prepare for the next generation of conflict. *Comparative Strategy*, *30*(2), 121-133. http://dx.doi.org/10.1080/01495933.2011.561730

Markoff, J. (2009, July 16). Internet's anonymity makes cyberattack hard to trace. *The New York Times*. Retrieved from http://www.nytimes.com/2009/07/17/technology/17cyber.html

Martellini, M. (2013). *Cyber security: Deterrence and IT protection for critical infrastructures.* New York, NY: Springer.

McGraw, G. (2013). Cyber war is inevitable (unless we build secuirty in). *Journal of Strategic Studies*, *36*(1), 109-119. http://dx.doi.org/10.1080/01402390.2012.742013

McReynolds, P. (2015). How to think about cyber conflicts involving non-state actors. *Philosophy & Technology, 28*(3), 427-448. doi:10.1007/s13347-015-0187-x

Milevski, L. (2011). Stuxnet and strategy: A space operation in cyberspace. *Joint Force Quarterly*, *63*(4), 64-69.

Morgan, P. M. (1977). *Deterrence : A conceptual analysis*. Beverly Hills, CA: SAGE Publications.

Morgan, P. M. (2010). Applicability of traditional deterrence concepts and theory to the cyber realm. In *Proceedings of a workshop on deterring cyberattacks: Informing strategies and developing options for U.S. policy* (pp. 56-76). Washington, DC: The National Academies Press.

Mudrinich, E. M. (2012). Cyber 3.0: The Department of Defense strategy for operating incyberspace and the attribution problem. *Air Force Law Review*, 68, 167-206.

Mueller, M. L. (2010). *Networks and states: The global politics of internet governance* [eBook]. Cambridge, MA: MIT Press.

Nakashima E., & Warrick J. (2012, June 2). Stuxnet was work of U.S. and Israeli experts, officials say. *The Washington Post.* Retrieved from https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.9cbd760ab35b

Nishikaze, H., Ozawa, S., Kitazono, J., Ban, T., Nakazato, J., & Shimamura, J. (2015). Large-scale monitoring for cyber attacks by using cluster information on darknet traffic features. *Procedia Computer Science,* 53, 175-182. doi:10.1016/j.procs.2015.07.292

Norrlof, C., & Reich, S. (2015). American and Chinese leadership during the global financial crisis: Testing Kindleberger’s stabilization functions. *International Area Studies Review*, *18*(3), 227-250. doi:10.1177/2233865915573638

Nye, J. S., Jr. (2011a). Nuclear lessons for cyber security?. *Strategic Studies Quarterly*, *5*(4): 18-38.

Nye, J. S., Jr. (2011b). *The future of power*. New York, NY: PublicAffairs.

Obama, B. (2009). *Remarks by the president on securing our nation's cyber infrastructure* [Transcript]. Retrieved from https://obamawhitehouse.archives.gov/realitycheck/

O'Connell, M. E. (2012). Cyber security without cyber war. *Journal of Conflict & Security Law*, *17*(2), 187-209. https://doi.org/10.1093/jcsl/krs017

Organski, A. F. K. (1968). *World politics* (2nd ed.). New York, NY: Alfred A. Knopf.

Paul, T. V., Morgan, P. M., & Wirtz, J. J. (Eds.). (2009). *Complex deterrence: Strategy in the global age.* Chicago, IL: University of Chicago Press.

Payne, T. (2016). Teaching old law new tricks: Applying and adapting state responsibilty to cyber operations. *Lewis & Clark Law Review*, *20*(2), 683-715.

Philbin, M. J. (2013). *Cyber deterrence: An old concept in a new domain*. Carlisle, PA: U.S. Army War College. Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA589940

Powell, R. (1990). *Nuclear deterrence theory : The search for credibility*. New York, NY: Cambridge University Press.

Powers, S. M., & Jablonski, M. (2015). *The real cyber war: The political economy of internet freedom.* Chicago, IL: University of Illinois Press.

Rash, W. (2016, December 3). MAD concept of deterrence doesn't apply in world of cyber war. *eWeek*. Retrieved from http://www.eweek.com/security/mad-concept-of-deterrence-doesn-t-apply-in-world-of-cyber-war

Rattray, G. J. (2009). An environmental approach to understanding cyberpower. In F. K. Kramer, S. H. Starr, & L. K. Wentz (Eds.), *Cyberpower and national security* (pp. 253-274). Washington, DC: Potomac Books.

Rattray, G. J., & Healey, J. (2011). Non-state actors and cyber conflict. In K. M. Lord & T. Sharp (Eds.), *America's cyber future: Security and prosperity in the information age* (pp. 65-86). Washington, DC: Center for A New American Security. Retrieved from https://scadahacker.com/library/Documents/White_Papers/CNAS%20-%20Security%20and%20Prosperity%20in%20the%20Information%20Age%20-%20Vol%202.pdf

Rauch, C. (2016). Adjusting power transition theory - satisfaction with the status quo, international power constellations, and the case of the Weimar Republic. *Geopolitics, History, and International Relations*, *8*(2), 127-158.

Rice, M., Butts, J., & Shenoi, S. (2011). A signaling framework to deter aggression in cyberspace. *International Journal of Critical Infrastructure Protection*, *4*(2), 57-65. doi:10.1016/j.ijcip.2011.03.003

Rid, T. (2012). Cyber war will not take place. *The Journal of Strategic Studies*, *35*(1), 5-32. http://dx.doi.org/10.1080/01402390.2011.608939

Rid, T. (2013). Cyberwar and peace: Hacking can reduce real-world violence. *Foreign Affairs*, *92*(6), 77-87.

Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks. *Journal Of Strategic Studies*, 38(1/2), 4-37. doi:10.1080/01402390.2014.977382

Rid, T., & McBurney, P. (2012). Cyber weapons. *The RUSI Journal*, *157*(1), 6-13. doi:10.1080/03071847.2012.664354

Roberts, S. (2014). Cyber wars: Applying conventional laws of war to cyber warfare and non-state actors. *Northern Kentucky Law Review, 41*(3), 535-572.

Ruzicka, J., & Wheeler, N. J. (2010). The puzzle of trusting relationships in the nuclear non-proliferation treaty. *International Affairs, 86*(1), 69-85. doi:10.1111/j.1468-2346.2010.00869.x

Said-Moorhouse, L. (2016, December 6). US-Iran nuclear deal: Iran's president warns Trump not to ruin agreement. *CNN Politics*. Retrieved from http://www.cnn.com/2016/12/06/politics/iran-warns-donald-trump-nuclear-deal/

Sanger, D. E. (2012). *Confront and conceal: Obama's secret wars and surprising use of American powe*r. New York, NY: Crown Publishers.

Schearer, M. (2016). The short life and quick death of cyber deterrence (How I learned to stop worrying and love cyber). doi:10.2139/ssrn.2766017

Schelling, T. C. (1966). *Arms and influence*. New Haven, CT: Yale University Press.

Schelling, T. C. (1979). *A tribute to Bernard Brodie and (incidentally) to Rand*. Santa Monica, CA: Rand Corporation.

Schmitt, M. N. (2013). *Tallinn manual on the international law applicable to cyber warfare* [eBook]. Cambridge, MA: Cambridge University Press.

Schneider, F. B. (2012). Blueprint for a science of cybersecurity. *The Next Wave, 19*(2), 47-57.

Shamsi, J. A., Zeadally, S., Sheikh, F., & Flowers, A. (2016). Attribution in cyberspace: Techniques and legal implications. *Security and Communication Networks, 9*(15), 2886-2900. doi:10.1002/sec.1485

Sharma, A. (2010). Cyber wars: A paradigm shift from means to ends. *Strategic Analysis, 34*(1), 62-73. doi:10.1080/09700160903354450

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. New York, NY: Oxford University Press.

Skoudis, E. (2009). Information security issues in cyberspace. In F. K. Kramer, S. H. Starr, & L. K. Wentz (Eds.), *Cyberpower and national security* (pp. 171-206). Washington, DC: Potomac Books.

Solomon, J. (2011). Cyberdeterrence between nation-states: Plausible strategy or a pipe dream?. *Strategic Studies Quarterly*, *5*(1), 1-25.

Spade, J. M. (2011). China's cyber power and America's national security. *The U.S. Army War College*. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a552990.pdf

Starr, S. H. (2009). Toward a preliminary theory of cyberpower. In F. K. Kramer, S. H. Starr, & L. K. Wentz (Eds.), *Cyberpower and national security* (pp. 43-88). Washington, DC: Potomac Books.

Sterner, E. (2011). Retaliatory deterrence in cyberspace. *Strategic Studies Quarterly, 5*(1), 62-80.

Stevens, T. (2012). A cyberwar of ideas?: Deterrence and norms in cyberspace. *Contemporary Security Policy, 33*(1), 148-170. doi:10.1080/13523260.2012.659597

Stone, J. (2013). Cyber war will take place!. *Journal of Strategic Studies*, *36*(1), 101-108. http://dx.doi.org/10.1080/01402390.2012.730485

Swartz, J. (2011, February 15). 'Kill switch' internet bill alarms privacy experts. *USA Today*. Retrieved from https://usatoday30.usatoday.com/tech/news/internetprivacy/2011-02-15-kill-switch_N.htm

Taipale K. A. (2010). Cyber-deterrence. *Law, policy and technology: Cyberterrorism, information, warfare, digital and internet immobilization.* Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1336045

Tammen, R. L. (2008). The Organski legacy: A fifty-year research program. *International Interactions, 34*(4), 314-332. doi:10.1080/03050620802561769

Tammen, R. L., & Kugler, J. (2006). Power transition and China–US conflicts. *The Chinese Journal of International Politics, 1*(1), 35-55. https://doi.org/10.1093/cjip/pol003

Tammen, R. L., Kugler, J., Lemke, D., Stam, A. C., III, Abdollahian, M., ..., Organski, A. F. K. (2000). *Power transitions: Strategies for the 21st century*. New York, NY: Chatham House Publishers.

The MITRE Corporation. (2010). Science of cyber-security. *JASON Program Office*. Retrieved from https://fas.org/irp/agency/dod/jason/cyber.pdf

Thijssen, B. (2016). *The cyber triad: Towards effective deterrence in cyberspace*. Brussels, BE: Vrije Universiteit Brussel. Retrieved from https://www.researchgate.net/profile/Bart_Thijssen/publication/306013562_The_Cyber_Triad_Towards_effective_deterrence_in_cyberspace/links/57aa433e08ae42ba52ac2e92/The-Cyber-Triad-Towards-effective-deterrence-in-cyberspace.pdf

Thomas, E. (2016). US-China relations in cyberspace: The benefits and limits of a realist analysis. *E-International Relations Students*. Retrieved from http://www.e-ir.info/2016/08/28/us-china-relations-in-cyberspace-the-benefits-and-limits-of-a-realist-analysis/

Tiezzi, S. (2015, December 16). China vows no compromise on 'cyber sovereignty': Xi Jinping doubles down on the controversial concept at the 2nd world internet conference. *The Diplomat*. Retrieved from http://thediplomat.com/2015/12/china-vows-no-compromise-on-cyber-sovereignty/

Tran, H., Campos-Nanez, E., Fomin, P., & Wasek, J. (2016). Cyber resilience recovery model to combat zero-day malware attacks. *Computers & Security,* 61, 19-31. doi:10.1016/j.cose.2016.05.001

Trujillo, C. (2014). The limits of cyberspace deterrence. *JFQ: Joint Force Quarterly, 75*, 43-52.

Valeriano, B. G., & Maness, R. C. (2014). The dynamics of cyber conflict between rival antagonists, 2001-11. *Journal of Peace Research*, *51*(3), 347-360. doi:10.1177/0022343313518940

Valeriano, B. G., & Maness, R. C. (2015). The dynamic of cyber conflict between rival antagonists. In *Cyber hype versus cyber realities: Cyber conflict in the international system* [eBook] (pp. 78-108). New York, NY: Oxford University Press. doi:10.1093/acprof:oso/9780190204792.003.0004

Vatis, M. A. (2010). The council of Europe convention on cybercrime. In *Proceedings of a workshop on deterring cyberattacks: Informing strategies and developing options for U.S. policy* (pp. 207-223). Washington, DC: National Academies Press. Retrieved from http://sites.nationalacademies.org/cs/groups/cstbsite/documents/webpage/cstb_059441.pdf

Verton, D. (2008). The evolution of espionage: Beijing's red spider web. *China Brief, 8*(15). Retrieved from https://jamestown.org/program/the-evolution-of-espionage-beijings-red-spider-web/

Wang V. W. & Stamper, G. (2002). Asymmetric war?: Implications for China's information warfare strategies. *American Asian Review, 20*(4), 167-207.

Wang, D., & Mark, G. (2015). Internet censorship in China: Examining user awareness and attitudes. *ACM Transactions On Computer-Human Interaction, 22*(6), 31:1-31:22. doi:10.1145/2818997

Wedgwood, R. G. (2002). Proportionality, cyberwar, and the law of war. In M. N. Schmitt & B. T. O'Donnell, *Computer network attack and international law* (pp. 219-232). Newport, RI: Naval War College.

Yang, G. (2009). *The power of the internet in China: Citizen activism online*. New York, NY: Columbia University Press.

Zeadally, S., & Flowers, A. (2014). Cyberwar: The what, when, why, and how [commentary]. *IEEE Technology & Society Magazine, 33*(3), 14-21. doi:10.1109/MTS.2014.2345196

Zimet, E., & Skoudis, E. (2009). A graphical introduction to the structural elements of cyberspace. In F. K. Kramer, S. H. Starr, & L. K. Wentz (Eds.), *Cyberpower and national security* (pp. 91-112). Washington, DC: Potomac Books.