International Strategy for Cyberspace;

Kinetic Solutions to Virtual Challenges

By

Chikere Uchegbu

International Relations Master's Program

McCormack Graduate School of Policy and Global Studies

University of Massachusetts, Boston

May 2012

Abstract

In a May 2011 document, President Barack Obama outlined the new U.S posture on Cyberspace asserting that the U.S. reserves the right to retaliate to cyber attacks using 'conventional' means – a new epoch. This paper reviews the implications of this position on the U.S./Chinese relationship. While it remains a major U.S. trading partner, China is widely perceived in Washington as arguably the most ‘prolific’ antagonist in this game of *virtual espionage*. What is the propensity for the new U.S. posture to lead to a conventional war between the U.S. and China? Applying liberal theoretical perspectives to my analysis, I agree with experts such as Richard Clarke that the likelihood of war between the two countries is low. A viable explanation for adopting such a truculent posture is to serve as a deterrent against further cyber attacks. The effectiveness of such an untested strategy to achieve its desired objectives, however, seems futile at best.

"*China is the world's largest developing country, while the United States is the largest developed country. To build a new type of co-operative partnership between two countries like ours is a pioneering endeavor with great and far-reaching significance. There is no precedent for us to follow and no ready experience for us to refer to. We can only do what Mr Deng Xiaoping said, "Cross the river by feeling the stones." Or what Secretary Clinton once quoted: "When confronted by mountains, one finds a way through. When blocked by a river, one finds a way to bridge to the other side…May I ask where the path is? It is where you take your first step.*"

~ Xi Jinping; Chinese Vice President and Presidential Heir Apparent.

"I remain convinced that a successful China can make our country more prosperous, not less. As trade and investment bind us together, we have a stake in each other's success. On issues from global security to global economic growth, we share common challenges and responsibilities — and we have incentives to work together. That is why our administration has worked to put our relationship on a stable footing. I am convinced…that China's leadership agrees."

~ Joe Biden; U.S. Vice President.

Contents

Introduction	Page 5
Chapter One: International Strategy for Cyberspace	Page 8
- Cyberspace	Page 9
- Strategic Approach	Page 11
- Strategy Outline	Page 11
Chapter Two: Cyber Attacks	Page 16
Chapter Three: Malevolent Actors	Page 19
- Attribution of Cyber Attacks	Page 20
Chapter Four: The Sino-American Dyad	Page 24
Chapter Five: The Deterrent Factor	Page 28
- Classical Deterrence	Page 28
- Analogies to Nuclear Deterrence	Page 29
- Deterrence by Denial	Page 33
- Deterrence by Punishment	Page 33
Chapter Six: U.S.-China War	Page 35
- Levels of Analysis	Page 35
- Theoretical Perspectives: Realism	Page 41
- Theoretical Perspectives: Liberalism	Page 45
Chapter Seven: Conclusion	Page 48
Appendix	Page 52
Glossary	Page 56
Works Cited	Page 57

Introduction

Advancements in science, particularly with regards to the computer, have occurred at breakneck speed. Today, computer network systems connect people across the world, exponentially increasing the speed at which we communicate. The contemporary era of globalization has been made possible, and sustainable, by advancements in technology making global communication and cooperation possible.

While the benefits of a networked world are innumerable it is important to note that the systems upon which the process rests bears significant vulnerabilities. As the technologies have advanced, the norms and international laws guiding the use and activity within the space have sadly lagged behind. To this effect, malevolent actors are able to take advantage of the vulnerabilities inherent in the system by perpetrating attacks on susceptible networks. Each day, an estimated 55,000 new pieces of malware are discovered while another 200,000 computers are turned into “zombies” (Lieberthal & Singer 2012). While there are three major categories of malevolent actors including individuals, criminal organizations and state sponsored groups, we will focus on those groups purported to have the sponsorship and backing of nation states.

In recognition of the immense value of cyberspace to the realization of our interests as a nation, it is now viewed as a medium of national interest. The continued activities of malevolent actors subject our interests in cyberspace to threats against which we have to defend. To this end, President Barack Obama has offered his vision for developing an international norm guiding the use of cyberspace, and a policy of deterrence for would-be aggressors that includes the threat of the use of conventional force in retaliation. There are implications to such a policy including the possibility of a

conventional war between the U.S. and states that attack American cyberspace. Using the U.S.-China relationship as a case study, this paper will analyze the propensity for the U.S. strategy to lead to a conventional war between the United States and China.

In Chapter One, we will review the proposed International Strategy for Cyberspace to understand President Obama's vision in greater detail. While previous U.S. governments have attempted to protect U.S. cyberspace and deter foreign aggressors, those attempts have not been as ambitious and aggressive as President Obama's strategy. In Chapter Two, we look at cyber attacks to show how and why they are a threat to U.S. cyberspace. While some attacks focus on infiltrating a networked system in search of data that can be exfiltrated for economic profit or leverage in negotiations, others seek to wreak damage or expropriate control abating command and control systems of the victim. The categories of malevolent actors are assessed in Chapter Three to show the distinction demonstrated among other things, by the nature of information or access they seek. Individual and criminal organizations are most likely to seek highly confidential but fungible information that can be traded on black market exchanges around the world. For state actors however, their interest and quest for information can best be described in terms of espionage where the compromised information is used in international negotiations, or to seek an advantage over other states. In seeking responsibility for attacks on U.S. cyberspace, forensic analysis of discovered computer virus attacks point to mainland China as their main source of origin. Even as attribution techniques leave much to be desired, policy analysts have come to view China as a malevolent state actor in cyberspace. To understand the complexity of the U.S.-China relationship, we examine this dyad in Chapter Four. International trade and cooperation in international

organizations are but two of the areas where the U.S. and China depend on each other. It is important to understand how this dynamic affects our considerations of the proposed strategy. In Chapter Five, we will apply the theory of deterrence – both in its classical and contemporary forms – to our analysis for potential similarities to the Obama Strategy. What we find is that cyberspace as a medium varies greatly from other mediums (Sea, Air and Lad) and as such requires a unique approach suitable to its peculiar form. While a war between the U.S. and China is inconceivable, we analyze this prospect in Chapter Six. Putatively recognized as the most antagonistic aggressor towards the U.S. in cyberspace, it infers that the Obama strategy is aimed directly at China. If the U.S. strategy for defending American cyberspace in the future calls for the use of any and all methods including the use of conventional methods in retaliation, what is the likelihood that the U.S. will levy attacks on China and its interests in the real world in retaliation for intrusions and or attacks on American cyberspace? To help answer these questions, two methods of investigation including the application of theoretical approaches and the levels of analysis method made popular by Kenneth Waltz are applied to the study. Finally, a conclusion is offered generally asserting that war between the U.S. and China, as a result of this new strategy, is very unlikely.

Chapter One: International Strategy for Cyberspace

President Barack Obama's 'International Strategy for Cyberspace', released in May 2011, highlights both the importance of the medium popularly referred to as *Cyberspace*, and the malevolent actions that threaten to limit our collective ability to realize the promises of modern technology. Obama's strategy offers his vision for altering the present course from one that calls the integrity of operations within cyberspace into question, to one where the safety of users and the integrity of their data is assured. The strategy also envisions a process for holding malevolent actors to account offering a series of recommendations and actions that will 'dissuade' and 'deter' nefarious behavior within cyberspace.

So who are these malevolent actors active in cyberspace today? For many reasons as we'll address in this paper, China has risen to the top of the list as the number one aggressor state within cyberspace. The prevalence of attacks on U.S. computer systems originating from China concerns policymakers and U.S. national security experts alike. President Obama's strategy calls for the U.S. to employ any and all means, including conventional military strikes, in retaliation for cyber attacks as a tactic for deterring cyber attacks against U.S. critical infrastructures. The question then arises, 'what is the propensity for this new U.S. strategy to lead to a conventional war between the United States and China'? This paper reviews this strategy document against available research on the subject of U.S.-China relations applying empirical evidence as we answer this question. Compared to other traditional mediums, cyberspace is very much new and most actors –state and non-state- are still in the process of understanding their roles and uses for it. This is a critical yet evolving media as this paper will demonstrate.

Cyberspace

Technological advancements have brought with them opportunities for people across the world to communicate, cooperate and achieve prosperity at levels previously unknown. Thanks to computer systems and networks, production of goods and services can now be spread out across multiple locations thereby bringing development and economic prosperity to millions who hitherto lived in poverty. Through the use of technology, China has integrated its workforce into the global economy achieving economic growth which has lifted "several hundred million people out of poverty" (Stiglitz 2006). In this digital world, it becomes imperative for individuals, corporations and governments to connect to this network in order to participate in this global epoch. Computers, along with the networks that connect them, have formed the backbone of innovation increasing productivity and welfare across the globe by enabling the sharing of information and the global flow of goods and services. Economies such as India's, which has placed itself as the recipient of high skill jobs which relocated from the advanced West, demonstrate how technology can be applied in creating knowledge economies which provide employment and a means of livelihood for millions of peoples. Taken together, the computer networks which have been developed to manage this digital explosion and the devices and systems which they control constitute what we refer to as *Cyberspace* (Clarke & Knake 2010). But in addition to this growing interdependency is an emerging and active malevolence that threatens to limit this progress. Presenting this as a 21st century challenge, President Barack Obama describes a scenario where nations and peoples, in harnessing the networks all around us, can either "work together to realize their potential for greater prosperity and security" through cyberspace stability, or

"succumb to narrow interests and undue fears" that serve no good (Obama 2011; Lord & Sharp 2011). In a demonstration of the significance of cyberspace and the threat posed therein, Leon Panetta, the director of the Central Intelligence Agency at the time, told a congressional committee that cyberspace "represents the battleground for the future. The potential for the next Pearl Harbor", he concluded, "could very well be a cyberattack" (Menn 2011). In an apparent recognition of both the "potential" and "vulnerabilities" of this new medium, the U.S. Air Force created the 24th Air Force wing whose sole priority is to wage war in this new and important medium (Libicki 2009).

In a 25 page document titled *'International Strategy for Cyberspace; Prosperity, Security, and Openness in a Networked World'*, President Obama describes the ever increasing importance of cyberspace as "indispensable to our daily lives"; and the need for maintaining the interoperability and integrity of the space by actively "confronting those who would destabilize or undermine" (Obama 2011) this increasingly networked world that is emerging. According to Obama, the priority accorded the realization of cyber security –to ensure that the benefits that networked technology promises are realized – aren't uniquely American. President Obama offers that assuring the unfettered flow of information, the protection and confidentiality of data and the continued reliability of these interconnected networks remain essential to the realization of "American and global economic prosperity, security and the promotion of universal rights" (Obama 2011).

Strategic Approach

With the International Strategy for Cyberspace, President Obama is attempting to fill a void that exists in the international system as to the arrangement and maintenance of order in the use of cyberspace. As Clarke puts it, "the lack of geopolitical boundaries…allows cyberspace operations to occur nearly anywhere, …cyberspace reaches across geopolitical boundaries…and is tightly integrated into the operations of critical infrastructure and the conduct of commerce" (Clarke & Knake 2010).

President Obama's International Strategy for Cyberspace – Outline

Strategic Approach
- Build on the Successes of Cyberspace
- Recognize the Challenges
- Ground Potential Solutions in Principle

Cyberspace's Future
- An Open and Interoperable Cyberspace that Empowers
- A Secure and Reliable Cyberspace That Endures
- Achievement of Stability Through Norms
    - Diplomacy: Strengthening Partnerships
    - Defense: Dissuading and Deterring Would-be Aggressors
    - Development: Building Prosperity and Security

Priorities
- Promoting International Standards and Innovative, Open Markets
- Enhancing Security, Reliability, and Resiliency
- Extending Collaboration and the Rule of Law
- Preparing for 21st Century Security Challenges
- Promoting Effective and Inclusive Structures for Internet Governance
- Building Capacity, Security, and Prosperity
- Supporting Fundamental Freedoms and Privacy

The U.S. strategy is based on a collection of principles that seek an open and interoperable cyberspace which rewards innovation and empowers individuals and

nations; a secure and reliable medium that will ensure the endurance of the medium as a veritable source of exchange; and the assurance of stability through the reinforcement of existing norms, as well as the furtherance of emerging norms that are essential to the viability of this space. According to the President, the U.S. seeks to work with "like-minded states to establish an environment of expectations, or norms of behavior" (Obama 2011) which will anchor foreign and defense policies creating stability. Lamenting the absence of norms to guide the use of cyberspace, Obama points to an imbalance in the rise of the rates of societies' reliance on networked information systems against a dearth in the development of norms that guide its use and activity within the space. This strategy will seek to restore this balance by pursuing two major goals: (1) to promote an *open, interoperable, secure and reliable* information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation, and (2) build and sustain an environment in which *norms of responsible behavior* guide states' actions, sustain partnerships, and support the rule of law in cyberspace. The United States' international cyberspace policy is built on the foundational belief that networked technologies possess tremendous possibilities for the U.S. and the rest of the world. With more than "four billion" (Obama 2011) digital devices connected wirelessly in the world today and more than a third of the world's population with access to the internet, there is a sudden realization as to the pervasiveness of this medium in our world. Critical life-sustaining infrastructures that deliver electricity and water, control air traffic, and support our financial system are all dependent on networked information systems (Clarke & Knake 2010; Obama 2011).

As these technologies have evolved transforming our economic and daily lives, we have also witnessed the migration of offline challenges such as exploitation and aggression into cyberspace. According to President Obama, for these systems to remain an empowering force that inspires individuals, improves societies, and advances research and development – which are essential to building modern economies- they must retain the "openness and interoperability that have characterized their explosive growth" (Obama 2011). Networked technologies possess a global reach and President Obama foresees a time when fundamental digital infrastructure will become a *national asset* for all nations.

This challenge is made more acute by the presence of *malevolent actors* whose sole desire is to disrupt and exploit cyberspace activities. With regards to these threats, individuals, criminal organizations, non-state groups as well as nation-states –and their proxies – can pose a threat to systems of networked technologies. The time has come for the systems to adapt to meet these challenges. The current U.S. posture, outlined in the May 2011 document, describes a series of measures aimed at '*dissuading and deterring'* groups from mounting cyber attacks. But who exactly is the U.S. trying to dissuade and deter? This monograph will focus on the cyber attacks attributable to nation-states and the potential levels of response from the United States as outlined in the Obama document.

In building a cyberspace policy, President Obama stresses the need to secure the future of an "open, interoperable, secure and reliable cyberspace" by developing internationally acceptable norms of behavior while confronting "those who would destabilize" our collective interests in a networked world (Obama 2011). To achieve this,

Obama hopes to build on the success of cyberspace by working to expand the reach of cyberspace while also improving its operation in the U.S. and internationally. The principles guiding this policy for cyberspace reflects the core commitments of the United States to *fundamental freedoms*, *privacy*, and the *free flow of information.* The policy seeks to propagate a future where cyberspace connects communities seamlessly strengthening communities and driving innovation. The integrity of the system has to be maintained to guarantee the continued confidence of users. This is the only way to ensure that cyberspace endures. Finally, Obama offers that international stability in cyberspace can only be achieved through working with like-minded states to "establish an environment of expectations, or norms of behavior" (Obama 2011) including the interoperability of cyberspace – the free flow of information in cyberspace– and worldwide connectivity to the web giving individuals the world over access to knowledge, ideas and one another. The free flow of information is a principle affirmed by more than 170 countries in the Tunis Commitment of the World Summit on the Information Society. The role of norms includes the maintenance of stability along with the provision of a foundation for international action when corrective actions are needed. When states adhere to these norms, it confers a measure of predictability to state behavior which prevents miscalculations which could lead to conflict.

To achieve these ends, the United States will combine diplomacy, defense, and development in seeking the enhancement of the benefits of a networked world. The U.S. will also seek to strengthen partnerships through bilateral and multilateral partnerships, international and multi-stakeholder organizations and through private sector collaboration. Defensively, the U.S. proposes a strategy for dissuading and deterring malevolent actors

from perpetrating attacks in cyberspace. Protecting networks, domestically and abroad, will go a long way to dissuade attacks. To deter against attacks, the policy states that the U.S. reserves “the right to use all necessary means” (Obama 2011), including conventional military operations –or ‘Kinetic’ operations as the military prefers to call it– in the defense of the state and its interests. The final step of development aims to expand the reach and access to cyberspace as a way to extend prosperity and security to all peoples of the world.

Chapter Two: Cyber Attacks

As outlined by President Obama, there are risks associated with such high levels of exposure to, and dependency on, computer networks which are accessible from any *node* anywhere in the world. In addition to arbitrary operational risks of malfunctioning, there are security flaws inherent in the design of the internet and the networks it integrates. There are malevolent actors as well who seek to exploit these weaknesses for financial gains and other malicious reasons. The computer networks of a company can be infiltrated in search of intellectual property and other patented trade secrets which can be traded or used in the manufacture of competing and counterfeit products. Unscrupulous individuals may seek to gain access to information with which to gain economic advantages or to exploit victims in other ways. Nation-states can hack into other nations' database systems to gain access to information that can offer a competitive edge in negotiations and other interactions in the global arena. Others may simply wish to access and disable the communications and defense systems of victims making them vulnerable to more conventional methods of attacks. While there are numerous motivations for various groups and individuals to seek such unauthorized access to secure networks, this paper will continue to focus only on cyber attacks perpetrated by sovereign nation-states. Such exploitative actions "by a nation-state to penetrate another nation's computer networks for the purpose of causing damage or disruption" (Clarke & Knake 2010) is collectively known as cyber war.

According to Clarke and Knake, cyber attacks are possible largely due to three factors which include: "(1) flaws in the design of the internet; (2) flaws in hardware and software; and (3) the move to put more and more critical systems online" (Clarke &

Knake 2010). Even at its creation, the internet, or ARPANET as it was called then, was designed with greater emphasis on decentralization than to security. With funding from the Defense Department's Advanced Research Project Agency (DARPA), scientists at MIT, Stanford and Berkeley created what was known as the Advanced Research Project Agency's Network (ARPANET). It was originally intended as a means for the Defense Department to communicate. ARPANET, which initially connected four computers –at UCLA, Stanford, UC Santa Barbara and the University of Utah (Clarke & Knake 2010)- was intended for use within this small network of specialists who all shared the same norms and integrity, making security an after thought. As it is today, cyberspace is an unsecured and largely unregulated medium where actors play according to their own rules. The global presence and reach of computer networks makes it difficult for any one nation's laws to regulate cyberspace activities. Barring the existence of a global authority, it is left to each participant to secure itself and its connections to the network. But this has also meant that those who perpetrate attacks in cyberspace are usually not held accountable for their actions. Cyber attacks have increased in intensity over time. In 2009, "a new type or variant of malware was entering cyberspace every 2.2 seconds" on average (Clarke & Knake 2010).

Imagine a scenario where critical infrastructure systems of a state are compromised and infiltrated by foreign actors who gain unauthorized access to such networks. By strategically inserting programming language known as 'logic bombs' – virtual explosives that are placed in critical computer systems during peacetime, and activated in conflict to disrupt an adversary's computer networks- in the system, the infiltrators are able to command the network to perform certain operations at their will. A

compromised air traffic control system can be shut down remotely causing planes to fly blindly across the skies. Cooling systems at power plants can be disabled causing a ‘melt down’ leading to huge disruptions and massive blackouts within a vast region of a country. Dams and flood-gates can be remotely triggered open flooding cities. Cyber attacks such as these are increasingly possible especially in a country such as the United States where critical systems have been brought online. The next chapter presents a review of the categories of actors who perpetrate attacks in cyberspace and the methods for identifying them.

Chapter Three: Malevolent Actors

The attribution of cyber attacks to responsible entities or groups is somewhat "difficult" and discouraging (Clarke & Knake 2010; Watkins 2011). The sophisticated and complex nature of the attacks, which are intended to shroud the source and identity of the perpetrators in mystery, lends to this difficulty. Often times, non-state criminal operators and state-sponsored professional intelligence or military actors typically operate in the same environment and sometimes against similar classes of targets. This overlap poses "attribution challenges for information security professionals, policymakers, business leaders, and members of the law enforcement and intelligence communities all of whom have uniquely different responses to these two categories of actors" (Krekel, Adams & Bakos 2012).

To further demonstrate this complexity, we will review a typical cyber attack known as DDOS, a Distributed Denial of Service attack. The attack uses a "preprogrammed flood of internet traffic designed to crash or jam networks (Clarke & Knake 2010). It is 'distributed' in that thousands, perhaps even hundreds of thousands, of computers are utilized in sending the electronic requests to a handful of targeted locations on the internet. The computers conscripted into doing the attacking are called a 'botnet', a robotic network of computers that are remotely controlled. The attacking computers are following commands loaded onto them without their owners' knowledge. The malicious activity usually occurs in the background and invisible to the user. Prior to the botnet attacking, often weeks or months before, malicious software is secretly downloaded while surfing the internet, turning a users computer into a 'zombie'. These zombie computers often sit idle awaiting further commands from the remote hacker. Other times,

they are programmed to automatically seek out other computers to infect, and they in turn do the same, expanding the botnet. This creates the phenomenon known as a "worm" (Clarke & Knake 2010). But when activated to attack networks, botnets do leave a discovery trail which cyber security experts have tried to use in finding the origins of the attacks. Using *trace-back* techniques, security experts can follow the attacking pings to specific zombie computers and then monitor them to see when the infected computers will communicate back to their masters. The messages are traced back to controlling machines and devices which are then identified as the sources of the attacks.

As you can imagine, this is hardly a fool-proof process and still leaves an avenue for doubt. What further constrains the process of attribution is the seeming unwillingness of victims to publicly acknowledge the attacks on their systems. Companies are embarrassed at their inability to adequately protect theirs and their clients' confidential information. Governments have an incentive to avoid a panic by the public which can ensue in the aftermath of admitting to an intrusion of critical infrastructure systems by unknown elements with intent to harm the nation and the defenseless public. For these reasons, the incidence of cyber attacks which compromise confidential data has been under reported inhibiting the public understanding of the significance of this threat to national security. On their part, McAfee states that their goal in publishing a comprehensive analysis revealing the profile of victims of cyber attacks over a five year period was to raise the "level of public awareness" (McAfee 2011).

Using the imperfect process described above, cyber security experts have discovered and attributed certain major cyber attacks to specific countries considered the most capable and adept at initiating cyber attacks. The DDOS attacks on Estonia in 2007

were sophisticated both in magnitude and scope. A large amount (millions) of computers was involved in the attacks and their targets included networks that were previously unknown to the public. Addresses of "servers running parts of the telephone network, the credit-card verification system, and the internet directory" (Clarke & Knake 2010) were all attacked. McAfee describes its discovery of a 'Command and Control' server used in the perpetration of what it called the most audacious cyber attack which went unnoticed for over six years. Operation Shady RAT (which stands for Remote Access Tool), as McAfee labeled it, began in mid-2006 targeting more than 70 global companies, governments and non-profit organizations (McAfee 2011). The levels of sophistication witnessed in these attacks are beyond those to which individuals and criminal organizations are capable. These levels of coordination and sophistication usually suggest the involvement – and responsibility – of a state actor (McAfee 2011) although this is the entirety of the proof informing this suggestion. Ultimately, Estonia claimed that the attacks originated in Russia where the controlling machines were located; though the Russians "indignantly" denied the accusation (Clarke & Knake 2010, Keating 2012).

Operational differences existent between non-state criminal organizations and their state-sponsored counterparts allow for a systemic analysis of intrusion and incident reports which assists in the classification of attacks leading to proper attribution to responsible entities –state or non-state actors. As opposed to criminal network cyber attacks, state-sponsored attacks possess a scale, focus and complexity revealing a degree of financial and analytic resource that exceed what the most organized cyber criminal organizations can manage. Their objectives are seen as the continued support for espionage operations, conducting reconnaissance and layering of critical network

infrastructure with sensors or logic bombs for later use in the event of a conflict, to obtain commercially competitive information or intellectual property and in rare cases, to demonstrate capabilities to deter rivals. Most commonly, activities attributed to state actors "often appear to target data that is not easily monetized in the underground criminal online auctions or markets" (Krekel, Adams & Bakos 2012).

Due largely in part to the trace-back technique, responsibility for many other attacks has been attributed to entities –including individuals, criminal organizations and nation-states. With a focus on those attacks initiated by nation-states, Joshua Keating has identified those that are considered the most significant of their time (see table 1), and the alleged states behind them. It is clear that many states have developed the capacity to execute cyber attacks with as many as twenty to thirty militaries possessing respectable cyber war capability including those of Taiwan, Iran, Australia, South Korea, India, Pakistan and several NATO states (Clarke & Knake 2010). But distinguished by its intensity of attacks and focus on the United States and its global interests, China stands out as the most antagonistic aggressor. In a January 2012 'Worldwide Threat Assessment' report to the Senate select committee on intelligence, the Director of National Intelligence, James Clapper, made it clear that China, among state actors, is of "particular concern" to the United States (Clapper 2012). There is little doubt in the minds of U.S. policymakers that the Chinese government is responsible for a majority of cyber attacks on American networks making China the intended target for U.S. deterrent action. In the 2011 Executive report of the U.S. office of National Counterintelligence, China was named specifically as the "most active and persistent perpetrator of cyber intrusions into the United States" (Lieberthal & Singer 2012). According to Clarke &

Knake, China, for inexplicable reasons, continues to leave cyber crumbs that allow investigators to successfully trace cyber attacks on the U.S. back to the Chinese mainland. While this could be an inadvertent display of hacker immaturity, Clarke & Knake theorize that this could well be a conscious act on the part of the Chinese to demonstrate their ability to access American critical systems serving as a warning to American leaders. The putative acuity in Washington policy circles is that China is the most persistent perpetrator of cyber attacks against the United States (Clarke & Knake 2010; Lieberthal & Singer 2012). The question then arises as to the effect of the new U.S. posture on cyber attacks on U.S.-Chinese relations. What is the potential for this new posture to encourage aggression? And more importantly, what is the propensity for this new strategy to lead to a conventional war between the U.S. and China?

Chapter Four: The Sino-American Dyad

While the U.S. remains China's largest trading partner (USCBC 2010), the relationship has been wrought with challenges for both nations. In 2010, trade between the U.S. and China was valued at over $457 billion making China America's second largest goods trading partner. In its 2011 annual report to congress, the United States Trade Representative (USTR) credits what it called the "impressive" growth in U.S.-China trade with having provided "numerous substantial opportunities for U.S. businesses, farmers and service suppliers" as well as a "wealth of affordable goods for American consumers" (USTR 2011). To underscore the importance of the trade relationship between both nations, consider that China was America's number one supplier of goods import in 2010 and America's 3rd largest goods export market for the same year (USTR 2011). Both nations have gained from this relationship although America's widening trade deficits have led some to question the current arrangement. But that is a topic for different study.

Underlying this economic boon is the tension attributable to competing aspirations and designs for economic and geopolitical dominance. In '*Understanding Conflict and War*', R. J. Rummel explains that the key to avoiding conflict, which he describes as a "balancing of vectors of power", is to maintain the status quo. When unpredictability arises in the equation leading to what Rummel describes as "random 'trigger events'", the status quo is upstaged necessitating the development of new structures of expectations to replace the former establishing a new balance of power. According to Rummel, the process of developing this new structure is conflict. Using this

process, the parties will test each other measuring their capabilities, interests and will to act leading ultimately to the development of “a new modus vivendi” (Rummel 1981).

Generally recognized as the lone super power after the demise of the Soviet Union, U.S. policymakers view a rising China as a potential threat to its exercise of global hegemony. Power transition theory tells us that the “potential for war is greatly increased” when a major challenger to the present distribution of global power attains capabilities equal to –or almost equal to- the dominant hegemonic leader who is the defender of the status quo (Cashman & Robinson 2007). As this theory goes, China, the rising power, is slowly approaching the era where it’s economic and military capabilities will rival those of the hitherto dominant United States. Recent steps taken by the Chinese to modernize the Peoples Liberation Army (PLA) including the development of Fifth generation Jet Fighters, an Aircraft carrier and acquiring sophisticated long-range missile systems all point to this looming epoch. The Chinese, on their part, have presented their rise as benign and focused more on ambitions of “peaceful” economic development rather than military dominance (Lieberthal & Jisi 2012; Information Office of The State Council 2011).

The rational actor model perceives a state to be a “unitary actor driven by its national interests” while also assuming the decisions made by the leaders to be based on rational choice (Jackson & Sorenson 2010). This perspective focuses on the strategic interaction between states which in the case of the U.S. and China does cover a lot of areas including “military-to-military” contacts (Kissinger 2012) which removes uncertainty –a major component of military miscalculation. As major trading partners who also possess permanent membership in the United Nations Security Council (UNSC),

the U.S. and China have a lot of reasons to work together to achieve each others desires for geopolitical stability and economic growth. According to Lieberthal and Jisi, extensive dialogues are held between the two countries at more than sixty regular government-to-government forums where the "highest level leaders meet" (Lieberthal & Jisi 2012). With major concerns to its stated national security interests in the Middle-East in particular, the U.S. values Chinese cooperation in international organizations to generate international support for its policies –be it sanctions and or military action against rogue regimes. In essence, China can play a major role in legitimizing –or de-legitimizing– U.S. foreign policy actions. On the flip-side, the Chinese recognize that their intentions for superiority in South East Asia can be thwarted by the United States and its support for other regional contenders such as Japan, Vietnam and the Philippines. The expected rational choice for the Chinese leadership would be to avoid a direct confrontation with the U.S. at all costs thereby maintaining the status quo with regards to regional power distribution.

Considering the recently articulated U.S. "pivot" (Hille 2011) towards the Asia-Pacific, China is faced with a choice to either accept an attenuation of its growing influence within the region, or to directly confront the United States. Weary of confronting a more advanced military power such as the U.S. in conventional warfare –at the present, the Chinese continue to seek asymmetric ways of balancing the disproportionate distribution of power currently in U.S. favor. Cyber war provides such an opportunity since the Chinese can effect an inordinate amount of damage to U.S. critical public and private infrastructure at arguably negligible costs to the Peoples Republic of China. For this reason, the incentive to continue its alleged intrusion into U.S.

cyberspace –exfiltrating sensitive data and undermining the integrity of U.S. command and control systems- is very high, necessitating the need for immediate U.S. action to dissuade and or deter further acts of attack. By all indications, Chinese defense spending has continued to rise annually by an average of 11% and is projected to surpass the U.S. military budget by 2035 (See figure 3). Henry Kissinger describes the long-term strategic objectives of the Chinese as desirous of "displacing the United States as the preeminent power in the Western Pacific and consolidating Asia into an exclusionary bloc deferring to Chinese economic and foreign policy interests" (Kissinger 2012). This objective can only be achieved through an absolute dominance of the U.S. military by the PLA. And until this happens, Beijing will continue to seek ways to "negate traditional U.S. advantages" (Kissinger 2012) through the pursuit and projection of asymmetric balances.

Chapter Five: The Deterrent Factor

Classical deterrence is based largely on the understandings of classical criminology which posit that "decisions to violate the law are weighed against possible punishments (Paciotti 2005). It follows then, that to deter the commission of a crime the pain of punishment must outweigh the purported benefits of illegal gain. Along this rubric, the policy of deterrence was developed reaching its contemporary maturation during the Cold War. The theory makes certain assumptions as to the nature of mankind considering that individuals, possessing of free will, will make decisions in order to maximize the perceived utility of an action when weighed against the cost of said actions. An effective deterrent factor therefore, will boast of both "celerity" (swiftness of action) and "certainty" of reprisal (Paciotti 2005). Elevated to the state level, political realism or *realpolitik* is seen as the intellectual root of the theory which describes states as rational units driven by "their nature to maximize power, or by their environment to maximize security" (Zagare & Kilgour 2000). Consisting of two basic components, deterrence is based first on an expressed intent to defend a given interest; secondly, there has to be a "demonstrated capability…to achieve the defense of the interest in question" (Libicki 2009). In an anarchic system of international relations, states must rely on their own "strength and art for caution against others" (Zagare & Kilgour 2000). This strength, exhibited through state power, is understood along two perspectives; Latent power and Military power (Mearsheimer 2001). Extending this theory to military parlance, Zagare & Kilgour offer that prior to 1945, "The chief purpose of our military establishment [had] been to win wars." But in the post World War II era, its "chief purpose must be to avert them. It can have almost no other purpose" (Zagare & Kilgour 2000).

According to Joseph Nye, the current thinking about cyber security, in some ways, "is analogous to the thinking about nuclear security in the 1950s, when the weapons were new and the concepts underlying adversarial interactions were still being developed" (Nye 2011). But how effective is this Obama strategy as a deterrent factor? What qualities of a deterrent factor are most responsible for its success in deterring the unwanted behavior? A review of the nuclear deterrent will help with answering these questions.

Prior to the detonation of the atomic bomb in Hiroshima, the world lacked a true understanding of the devastatingly incredible power of the bomb. After the explosion of the bombs in Hiroshima and Nagasaki, the Japanese and much of the world were convinced of the power of this superior American weapon; and the willingness of the Americans to deploy it in conflict –having done so twice in quick succession. It convinced the Japanese to end the war shortly after the explosions to avoid further devastation and carnage (Rotter 2008). It sent a message to all adversaries that attacking the United States came with the risk of nuclear attack, one that was ferocious and whose effects were unimaginable. Decades after the end of World War II, the nuclear deterrent still retains its viability and no nation possessing a nuclear arsenal has been attacked or invaded by another state. One can only conclude that the efficacy of the nuclear weapon as a successful deterrent can only be attributed to the successful display of its might and ability in combat. Even in instances where two nations embroiled in conflict are possessing of nuclear weapons, they both still exercise tremendous restraint especially in the knowledge that an exchange of nuclear bombs will most assuredly lead to mutual destruction.

Cyber attacks differ greatly from conventional attacks –one using armies, tanks and bombs in invading another country- and therefore do not subscribe to the conventional rationality of deterrence. Unlike with nuclear weapons, "where an attacker may be deterred by the promise of retaliation …launching a cyber attack may run fewer risks" (Clarke & Knake 2010). Current methods of attribution are faulty at best and ruefully unreliable at worst. More often than not, we are unable to discover the true source of cyber attacks; and the mystery surrounding them accords a possible perpetrator the element of deniability. In a system where states seeks legitimation of their actions by other states, it becomes important that a method for identifying states responsible for acts of aggression –include cyber attacks- are beyond reproach to convince neutral observers that "retaliation is not aggression' (Libicki 2009). Lacking the ability to successfully attribute attacks to a nation-state makes it exceptionally difficult to unleash a lethal response to attacks. Deterrence is based largely on precedence and we, as an international community, have yet to demonstrate an eagerness to legitimize the use of conventional force in retaliation for virtual attacks. The difficulties of proper attribution may lead to the targeting of responses towards an innocent state creating newer enemies; or a delayed response requiring time for a proper vetting of the attack route to determine the aggressor. This removes the threat of celerity thereby reducing the intended threat to would-be aggressors which ultimately weakens the efficacy of deterrence.

American failure in developing an effective policy regarding the security and integrity of U.S. cyberspace is not due to a lack of effort. In a series of steps begun during the presidency of George H.W. Bush, Clarke describes attempts by the U.S. to dissuade other states from inflicting cyber attacks on the United States. In all, more than 30 cyber

security bills have been introduced in one form or another as Congress tries to legislate its way through the problem (Smith 2012). The Comprehensive National Cybersecurity Initiative (CNCI) and the 'National Security Presidential Decision 54' were both products of this attempt (Clarke & Knake 2010). Unfortunately, however, both remain classified. President Bush requested "$50 billion over five years" for the CNCI which called for steps to secure "government's networks" alone (Clarke & Knake 2010). While the initiative was supposed to develop an "information warfare deterrence strategy and declaratory doctrine" (Clarke & Knake), it was criticized for failing in that regard. In May 2008, the Senate Armed Services Committee questioned the initiative's secrecy in a public report commenting that "it is difficult to conceive how the United States can promulgate a meaningful deterrence doctrine if every aspect of our capabilities and operational concepts is classified" (Clarke & Knake 2010). The efforts at legislation are still on-going, as recent as April 27, 2012, the House of Representatives passed the *Cyber Intelligence Sharing and Protection Act* more popularly known as CISPA. The bill allows the government and private companies to by-pass privacy concerns in sharing information that could lead to the prevention of cyber attacks. With concerns relating to potential violations of privacy, the White House has threatened to veto the bill (Goldman 2012). Even as this monograph is written, the United States and Russia are nearing completion of an agreement that will among other things, establish a "secure communication channel" to ensure that attacks in cyberspace, where attribution is difficult, "do not escalate to full hostilities" (Nakashima 2012). The agreement currently under deliberation will adopt elements of the 'Nuclear Risk Reduction Center', a strategic

communication link established in 1988 so that Washington and Moscow could alert each other to ballistic tests which could be mistaken for acts of aggression.

Unlike conventional mediums such as Sea, Air and Land, where battles are fought, cyberspace possesses a unique attribute which is reflected in the difficulty experienced by Americans in securing and maintaining its integrity. The computer networks and critical infrastructures they connect are mostly privately owned by corporations while the risk associated with their failure or compromise affect the public interest. Consider a nuclear power generating plant, or a water & sewage treatment facilities which though privately owned, are widely relied upon by millions of people in the cities and regions that they support. An attack on any one of these critical infrastructures retains the capacity to destabilize entire cities or regions in the case of the power grid. In consideration of this dynamic, the question then becomes, whose duty is it to protect these critical infrastructures? Attempts by congress to create legislation that compels the owners of these private organizations to shore up their cyber defenses have been met with resistance by industry groups due to the cost the legislations and regulations levy on them. The failures, by Congress, to legislate its way through this issue can be attributable in part to this opposition from the businesses. Some, on the other hand, recommend that the U.S. declare these critical infrastructures a national security asset and assert our intention to 'defend' them as a means to deter would-be attackers. The problem with this approach is that it provides an incentive for the private owners of these businesses not to adopt cyber security measures to secure their networks, depending instead on the government to protect and defend their interests.

Previous attempts to create cyber norms ensuring the security of cyberspace have been ineffective due to the divergence of interests that exists in a large, unregulated vacuity that is cyberspace. President Obama attempts to avoid this same criticism by stating explicitly in his strategy document that the United States, like all other nations, reserves the "right to use all necessary means – diplomatic, informational, military and economic – as appropriate…to defend our Nation, our allies, our partners, and our interests." The United States he adds, "Will respond to hostile acts in cyberspace as we would to any other threat to our country" (Obama 2011). The intent is to provide a clear warning to potential adversaries that the risk of attacking the United States and its interests in cyberspace will transcend the virtual realm with potential U.S. response occurring in the *conventional* form. Though the question remains as to the efficacy of this warning, Obama takes steps in the prescribed direction incorporating the recommendation of select technocrats and cyber security experts in laying the foundations for an international strategy for cyberspace. But as Libicki tells us, deterrence that dissuades an attack usually is made up of two components; "deterrence by denial (the ability to frustrate the attacks) and deterrence by punishment" (Libicki 2009). So far, the U.S. approach to deterrence, including President Obama's stated strategy, dwells on the latter aspect to the detriment of the former and defense capabilities. Given the unique nature of the media, it seems apparent that the more effective course of deterrence would be the shoring up of defenses against savvy attackers who are capable of masking their footprints in cyberspace making deterrence by punishment largely irrelevant. As Deputy Secretary of Defense, William J. Lynn III, put it in his remarks on the Department of Defense (DoD) Cyber Strategy at the National Defense University in

July 2011, “If an attack will not have its intended effect, those who wish us harm will have less reason to target us through cyberspace in the first place” (Lynn III 2011). It is for this reason that deterrence should focus more on denial rather than punishment. For reasons yet unknown to us, U.S. policymakers have yet to explore deterrence by denial, which ‘plays a greater role’ in deterrence calculation (Libicki 2009), as a viable strategy for dissuading attacks choosing instead, to deleterious effect, to dwell on an escalation of the possible punishments for attacking U.S. cyberspace as deterrence.

Chapter Six: U.S. – China War

Having discredited the Obama strategy as a viable deterrent, we are left to tackle the prospect of a conventional war between the U.S. and China. To assist in this analysis, we employ a heuristic method for understanding the complex relationship between both countries known as the *levels of analysis* – a multi-dimensional approach to understanding the actions of states and influences that inform those choices. Additional examination using two theoretical perspectives including power politics (realism) and interdependence (liberal) theories allow for a thorough review of the potential for a conflict between the United States and China.

The levels of analysis method, developed by Kenneth Waltz in the 1950s, remains one of the more lasting methodologies for studying international relations theory (Genest 2004; Jackson & Sorenson 2010). The method analyzes states foreign policy activities at three distinct levels; (1) the system level, (2) the state level and (3) the individual level.

The System Level

The first of the levels of analysis is the system level where states are putatively understood as existing in an anarchic global system. Multiple theoretical perspectives are utilized in analyzing this system and how states relate to one another in the absence of a superior authority. Realists emphasize the value of national security offering the enhancement of military power and balancing that of other states as the best approach to achieving national security. A liberal approach emphasizes international institutions such as the United Nations (UN) or World Trade Organization (WTO) as possessing the means to reduce international conflict and promoting mutual understanding and interests. Theories at the systemic level explain foreign policy by describing conditions present in

the international system that constrain states towards certain actions (Genest 2004; Jackson & Sorenson 2010). As a state consumed by its increasing appetite for resources (Economist 2008) and aspirations for power (Nye 2012; Information Office of the State Council 2011), China is very intent on continuing its pursuit of growth objectives fuelled by its domestic production which will be gravely destabilized by war. Its main focus remains the securing of energy resources which will allow it to continue to grow its economy and ultimately leading to economic prosperity. According to Mearsheimer, this economic prosperity is what all great powers are built upon (Mearsheimer 2001). In recent time, China has shown its intent to secure the resources of the South China Sea as a means of ensuring its energy security against a backdrop of rising costs and competition for mineral energy across the world. And as the U.S. is pivoting towards the Asia-Pacific in projection of its power (Hille 2011), it is safe to say that the American effort will have to be balanced against a swelter of prior interests and priorities. These include the war on terror, U.S. energy security and domestic and international economic stability to name but a few. This geo-political canvass is hardly an ideal setting from which either state would wish to engage in a conflict with another world power – while retaining the capacity to adequately address all of its obligations and aspirations.

The State Level

The second level in the level of analysis for international relations theory is the state level. Here the methodology explores the system of ordering activity and authority within the state. At this level, political culture is more paramount than any other consideration (Genest 2004). The relationship between a country's state apparatus and the domestic society is examined for clues pertaining to the ease of the government to

mobilize and manage the country's power resources. "Foreign policy", the experts say, "is made not by the nation as a whole but by its government" and therefore what is of most significance is 'state power' and not national power (Jackson & Sorenson 2010). State power in this context, is defined as the portion of national power which the government can extract for its purposes and reflects the ease with which the central decision-makers can achieve their end (Jackson & Sorenson 2010). With both the United States and China in the midst of political transitions (Presidential elections in the U.S. and the National Peoples Congress & Politburo changes in China), economic issues, rather than foreign military aggression, have emerged as the major concern of these two states. The popular rhetoric of the major political parties in the U.S. is captured in the ubiquitous chant of 'jobs, jobs, jobs' and both parties are now offering competing agendas for returning the U.S. economy to its previous levels of dominance. The same can be witnessed in China –to some varying degree- where the Chinese Premier Wen Jiabao, in his penultimate opening address to the 2012 people's congress as Premier – and last as a member of the all powerful politburo; spoke of "new problems" (Economist 2012 (1); Wines 2012) calling for further developments within the internal economy of China as a means of averting popular revolt against the communist party led government. The growing disparity in wages and lack of adequate social welfare structures are all major internal issues confronting the Party. The current political discourse in both countries centers on a theme of economic prosperity and an acknowledgement that wars and military campaigns carry a cost that the people are unwilling to pay. Despite the obvious differences in the types of regimes in power in both countries –Liberal Democracy in the U.S. and Authoritarian Communism in China – both sets of leaders still

exercise a rationality that is motivated by self preservation. Where the liberal American system will constrain its leadership from waging aggression in its foreign policy, the Chinese ruling elite will recognize that a disruptive foreign military campaign has the capacity to diminish its domestic control and authority which is currently unstable –at best – due to economic and social volatilities. As the Economist puts it, the legitimacy of the Communist Party is highly dependent on its ability to deliver on the "promise of economic prosperity" (Economist (3) 2012)

The Individual Level

The third and final level of our levels of analysis theory for international relations is the individual level. Theorists at this level perceive the "foreign policy and interaction of states" as an end product of the "nature, characteristics and values of …individuals in leadership roles" (Genest 2004). Using the cognitive model, we can analyze the actions of the key decision-makers for an insight into what we can expect from their countries foreign policies. In this process, one of the more poignant indicators is the rhetoric of the individual leaders. This usually points to how they "create their own images of reality and simplify decision-making through the use of analogies" (Jackson & Sorenson 2010). For President Hu Jintao, images of the 'cultural revolution' that rocked China in the 1960s, and the Tiananmen square massacres that led to revolts in 1989, still affect his decision making process (Wines 2012). Calling for serious reforms to China's political setup, Wen Jiabao cautioned that China could slip back into the chaos that characterized much of the country in the days of the 'cultural revolution' when violence, masterminded by the 'gang of four' killed thousands of Chinese people. As the levels of analysis indicate, rhetoric such as this indicates the events that shape leaders cognition and how

they affect foreign relations calculus. This is especially critical given the on-going transition within the communist party in China. And if the congeniality of Mr. Hu's presumed successor, Xi Jinping, expressed through out his visit to the U.S. (Economist (2) 2012) is anything to go by, the Sino-American relationship will continue to grow stronger in the years to come. The strength of the current crop of Chinese leadership is to demonstrate to their people that they are able to navigate the treacherous waters of international relationships, dominated by the United States, as they continue to grow their economy and the power of a modern Chinese state with it.

President Obama on his part has demonstrated time and again that he is a rational actor given to intellect and strategic calculations. In both public speeches and in private decision making, President Obama has displayed a poise and calm indicative of a steely reserve and a thoughtful approach towards foreign policy. Adopting the choice of 'carrot' or 'stick' as necessitated by the situation, Obama has shown a flair for presenting his foreign policy priorities in language that is most avuncular in nature and far from inflammatory. In a previous paper, I argued that even as a candidate for the presidency, Obama took a "conciliatory approach" in prescribing his vision for American foreign policy offering at the time, to meet with leaders of adversarial states without preconditions (Uchegbu Fall 2010). Subsequent speeches in Cairo and Berlin outlined Obama's vision for a world order that differed in tone and unassuming nature from that which prevailed during the administration of his predecessor. The unilateral approach that was the Bush doctrine was replaced by the Obama approach which elevated international organizations such as the UN to a place of dominance signaling his administrations intent to respect and operate according to internationally accepted norms of behavior. Obama

often speaks about his desire to 'engage' new partners in global governance sharing his vision for international politics that is based on "shared interests among nations" (Wright 2010). Based on his rhetoric alone, one can hardly accuse President Obama of stoking up tension between the U.S. and China and his foreign policy prerogatives as President continue to support this theme. Upon his return from Beijing in September 2011, U.S. Vice President, Joe Biden, sought to allay fears that a rising China poses a strategic threat to the United States and its interests. Proponents of this position pointed to the potential bi-polarity, similar to that which attained during the Cold War, which would pit U.S. and Chinese interests directly against one another. According to Biden, as "trade and investment" continue to bind the U.S. and China together, each country will retain a stake in the other's success ensuring that cooperation and dialogue will determine mutually beneficial outcomes and not conflict (Biden 2011).

In a joint statement at the end of January 2011 visit to the U.S.; President Hu Jintao joined his American counterpart in expressing the two countries' commitment towards a "positive and comprehensive" relationship. Assuring each party regarding their major concern, the United States reiterated that "it welcomes a strong, prosperous and successful China that plays a greater role in world affairs. China welcomes the United States as an Asia-Pacific nation that contributes to peace, stability and prosperity in the region" (Kissinger 2012). This statement indicates the perception of both leaders with regards to the methods of addressing the tensions that exist between Beijing and Washington preferring dialogue to conflict. While I caution against naiveté in assuming conflicting positions to this statement does not exist in either Beijing or Washington, we

simply do not have any evidence to substantiate claims to the insincerity of both leaders towards this commitment.

Theoretical Perspectives - Realism

Another approach to the review of the possibility of war between the U.S. and China is to utilize two of the dominant perspectives in the analysis of foreign policy and international relations: realism and liberalism. According to realists, the state, as the unitary actor in international politics, is putatively perceived as an actor who is of necessity, "preoccupied with the balance of power" (Mearsheimer 2001; Jackson & Sorenson 2010). The 'power' in question is clearly defined as military force and the various political and military iterations to which it can be employed: deterrence, nuclear weapons, war, armed intervention, etc.. From this point of departure, Mearsheimer builds this theory into what he describes as 'offensive realism' resting on the assumption that great powers "are always searching for opportunities to gain power over their rivals" (Mearsheimer 2001; Jackson & Sorenson 2010). Perceived from this unique standpoint, it is easy to assume a war between the U.S. and China as all but a foregone conclusion. But not so fast. In describing states' strategy for survival, Mearsheimer highlights the importance of the balance of power to states. Power, both in its absolute and relative terms, is of great importance to states and they will do what they must to ensure that the distribution of power is maintained, and where shifts occur, it tilts the balance in their favor especially relative to other states (Mearsheimer 2001). This is most important in the case of super powers that harbor desires of hegemonic domination. Acting rationally, the dominant great power in this dyad, the United States, will perceive war with China negatively. This is because such an occurrence will exert a toll on the U.S. upsetting the

current balance of power, and exacting a cost that can be viewed as a relative loss of power compared to rival states who are seeking either regional or global hegemony. The Chinese on their part, weary of the effects a major confrontation a war with the U.S. will have on their ambitions for regional dominance, will shy from escalating a potential conflict with the U.S.

There are those who do not subscribe to the assessment above pointing to the continued Chinese military build up as indications of an imminent confrontation. According to the U.S.-China Economic and Security Review Commission, China has embarked on a series of steps to modernize its military thereby presenting a potential threat to U.S. national security interests. In its 2010 report to Congress, the commission states that "China is modernizing its air and missile forces and improving its capabilities to conduct offensive air and missile operations" expanding China's ability to "operate outside of its borders and reach U.S. regional allies, such as Japan, as well as U.S. forces in the region" (U.S.-China Economic and Security Review Commission 2010). American strategists who fear this Chinese military build up are informed by realist thinking which believes that "the measures a state takes to increase its own security usually decrease the security of other states" (Mearsheimer 2001). This is what realists consider as the 'security dilemma' which was made popular by the 1950 work of John Hertz in the journal *World Politics*. Erstwhile American diplomat, Henry Kissinger, cautions on the folly of expecting the world's second largest economy not to "translate its economic power into increased military capacity" (Kissinger 2012). As Mearsheimer tells us, the basis of military power is economic power (Mearsheimer 2001), and China is being rational in applying its economic might towards building up its military capacity. Based

on the realist perspective, one can assume that China, a rational actor, is building up its military capacity for its defense and not solely for a potential offensive action against the United States. Within China, there is a palpable concern regarding possible U.S. intervention in on-going disputes between China and its neighbors. Oil and gas reserves discovered in the South China Sea has led to increased tension between China and other littoral states – Indonesia, Malaysia, Philippines and Vietnam – over access to these waters and the resources therein. The American position challenges China's maritime claims while expressing support for the claims of these other nations stoking Chinese fears of a meddlesome America. Added to that, the Chinese have long feared an American defense and continued support for Taiwan which China considers a part of its sovereign territory. The Chinese strategy for Taiwan includes the use of military force to reign in Taiwan's ambitions for independence and China will rely on its growing military might to fend off potential interference by the U.S. in Taiwan.

Taking the review of Chinese military expenditure a step further, we can make assumptions as to their perceived priorities at this time. The 2012 Chinese budget outlining military and security spending suggests that domestic concerns, rather than foreign aggression are of greater worry to Beijing. The budget calls for an 11.2% increase in military 'defense' spending from 2011 figures for a total of $106 billion (Perlez 2012; Buckley 2012). The U.S., on the other hand, continues to question the veracity of the published account of China's military spending. In 2011, the Pentagon estimated that China would spend "$160 billion" instead of the announced $95.6 billion. The most interesting factor however, is that the Chinese increase in domestic security spending is higher than the amount budgeted for military defense. A total of $111 billion –an increase

of 11.5%- has been set aside for spending on police, militia and other security arms (Buckley 2012). A majority of this increase is dedicated to combating rising domestic instability due to among other things, an educated and growing middle class, greater connectivity and less favorable growth rates in the Chinese economy. By contrast, the total Pentagon budget for 2013 amounts to $525.4 billion – a cut of about $5 billion from 2012 which far eclipses the combined Chinese defense and domestic military spend though it is important to note that "vital elements of the Chinese military buildup, including cyberwarfare" are not included in the budget (Perlez 2012). The Chinese ruling class is ever more focused on internal dissent especially as the number of "mass incidents" of unrest has increased from 8,700 in 1993 to about 90,000 in 2010 (Buckley 2012). Neither the military spending nor the statements from Chinese leaders portray the image of a nation preparing for war with a super power such as the United States. Please see Figure 2 for a comparative list of defense budgets from 2011.

Given this wide variance in military spending between the U.S. and China, Clarke and other experts have warned that in the event of war with a major super power such as the U.S., China will seek to leverage their asymmetric power preferring cyber warfare to conventional war –or Kinetic war which is the U.S. military's preferred term. This warning is buttressed by the development of offensive capabilities in cyberspace which has emerged as a major area of interest for the PLA (Clarke & Knake 2011). To this end, the Chinese military spending alone does not tell the complete story of their military's preparedness for war. Based on Pentagon reports, the Chinese have "designed cyber weapons that have never been seen before and no defenses designed to stop" (Clarke & Knake 2010). Ten examples of such weapons and techniques listed by the Chinese can be

found in Table 2. As the U.S. debates its strategic approach towards Cyberspace, "China is increasingly developing and fielding advanced capabilities" (Lord & Sharp 2011; Clarke & Knake 2010). China's focus goes beyond collecting sensitive information, to developing the capabilities of the Peoples Liberation Army (PLA) to inflict economic harm, damaging critical infrastructure and influencing the outcome of conventional armed conflicts. In a future conflict with another major power, Chinese defense strategists will likely view cyber attacks as an attractive option. Cyber attacks will offer the Chinese a measure of asymmetric balance to the far more superior conventional might of the U.S. military (Clarke & Knake 2010; Lord & Sharp 2011). Informed by the considerations of *realpolitik*, we may safely deduce that the rational choice for both the U.S. and China is de-escalation of conflicts in general. This is not to say that further intrusions of American cyberspace cannot be expected of the Chinese, rather, it is expected that the U.S. will not respond to such intrusions through kinetic actions. Regardless of the wide spectrum of issues the U.S. and China may differ upon, Kissinger tells us that conflict between the two states still remains a "choice" (Kissinger 2012) and not an inevitable outcome.

Theoretical Perspectives - Liberalism

The second theory which assesses the possibility of war between the U.S. and China is liberalism. Liberals believe in the "promotion of global order through expanded political and economic ties" (Genest 2004). As the theory goes, the creation and success of international order is largely dependent on four main factors; (1) the role of international institutions, (2) international rules and norms for behavior of states, (3) the increasing economic interdependence between nations, and (4) technological

advancements and the growth of global communications (Genest 2004). According to Richard Rosecrance, states, in the past, have sought power by means of "military force and territorial expansion" (Jackson & Sorenson 2010). In the contemporary world however, 'economic development' and 'foreign trade' are more 'adequate' and 'less costly' ways for highly industrialized states to achieve prominence and prosperity. He goes on to add that the "costs of using force have increased and the benefits have declined" (Jackson & Sorensen 2010).

The two main branches of liberal theory –liberal institutionalism and economic liberalism – support the argument that war between the U.S. and China, due to the current U.S. posture on cyberspace, is not imminent. Liberal institutionalism, which is preoccupied with institutionalizing global cooperation, has been boosted by Chinese accession to international organizations such as the World Trade Organization –where international norms are developed. In arenas such as this and the United Nations Security Council (UNSC), the U.S. and China maintain an avenue for continued interaction that will forestall any calamitous event due to lack of cooperation. Desirous of maintaining its position as a 'good state' in the international community of states, each country's actions will be constrained –within the system– to act according to putatively accepted norms of state behavior and international law. Economic liberalism on the other hand, emphasizes the "economic ties between nations as a basis for establishing and preserving order" between states. A major tenet of the liberal perspective is the interdependence theory which asserts that 'states who engage in free trade with each other rarely do go to war with one other'(Genest 2004). Cooperation, one of the basic assumptions of liberal ideology, informs the *'interdependence'* strand of liberalism. This cooperation and

interdependence is most exemplified in the rapidly growing trade between the U.S. and China. Based on this perspective, we can conclude that the United States and China will not engage in conventional warfare in the near future. The formation and success of the European Union is based largely in part of this liberal theory and it has continued to unite and promote peace within Europe since the signing of the treaty of Paris on April 15, 1951 (McCormick 2008).

As is often the case in international relations, multiple theoretical approaches can be applied in analyzing event offering theories in support of a preferred opinion. As demonstrated above, realist and liberal theories both offer explanations why the conflict between the U.S. and China is unlikely as a result of the International Strategy for Cyberspace offered by President Obama. It must be said however, that the liberal theory of cooperation and engagement is the ascendant theory which embodies all the challenges confronting both states, as well as avenues for their amicable solution –averting conflict.

Conclusion

In the aftermath of the analysis above, describing the Obama strategy as lacking the necessary disincentive to deter states, and especially China, from attacking U.S. cyberspace and cyber interests, one can only assume that the attacks will continue to occur. Despite the continued intrusions, it will be very difficult for the United States to effectively attribute the attacks to a particular nation state further complicating attempts to deter specific actors. With regards to perceived threats to U.S. cyberspace from China, and the potential for a kinetic response from the U.S., the dyadic relationship between the United States and China entangles both nations in such ways that neither state will desire a break in relations. Record levels of trade have brought about unprecedented levels of cooperation and economic boon for both the U.S. and China and both countries are desirous of maintenance of the status quo which, *inter alia*, has brought economic prosperity and wealth. Although contentious issues still remain for both sides to iron out, various theoretical arguments and empirical evidence suggest that these will not be enough to escalate the tensions between both countries to the point of military confrontation. Both countries maintain high level contacts affording them opportunities to address their concerns through diplomacy and dialogue. Despite numerous differences spanning multiple issue areas, conflict between the U.S. and China still remains a choice and not an inevitable one at that.

The Obama strategy fails to offer a sufficient deterrent for states -and non-state actors alike- who may wish to attack U.S. cyberspace and critical interests therein. This monograph has established that the document, however grand its intent, and aggressive its adopted language may seem, will not lead to a conventional war between the United

States and China. The question then for a possible study remains the overall intent of the strategy. How can the U.S. develop an effective deterrent strategy that states would actually recognize and fear?

Respective of the highly fluid nature of this phenomenon, American strategists should focus on an active revamping of the shared values of cyberspace with a greater emphasis on shoring up of inherent vulnerabilities –deterrence by denial. The incentive for the Chinese to continue to exploit American cyber vulnerabilities remains at an all time high. The low cost of obtaining these highly valuable data through cyber espionage, the degradation of U.S. defenses through the strategic deposition of crippling malware and logic bombs, all combined with the low risk of detection and attribution; provide an incentive for continued intrusions. For all of these reasons, one can expect the rational calculations of the Chinese to lead to a continued assault and exploitation of U.S. cyberspace. Unfortunately, the attempts made by consecutive U.S. administrations to deter would be cyber attackers have proved to be futile. The 'stick' or threat of punishment, for reasons enumerated above, is ineffective and does not convince perpetrators of imminent reprisal. Moreover, choosing to defend private owned networks through public means removes the inventive for private owners to guard their networks against intrusions. Cyberspace is a unique medium which requires a unique perspective regarding its defense and protection.

The greatest opportunity for the U.S. lies in the continued development of acceptable international norms of behavior within cyberspace and this should be done -in concert with other nations, and particularly China. This norm building effort should be done consistently with the process of updating domestic cyber security systems to reduce

their vulnerabilities to attacks. While tensions stemming from the increased violations of U.S. (and quite frankly, Chinese) cyberspace will not lead to an escalation of conflict up to an outbreak of conventional war, resolving the current tensions will have significant "spillover" effects (Lieberthal & Singer 2012) on other areas of mutual cooperation between the U.S. and China. The bellicose rhetoric emerging from both Beijing and Washington will be reduced once the opacity within the sphere of cyberspace is eliminated or reduced. This will afford the U.S. and China the opportunity to move forward on other pressing areas where cooperation is required.

To achieve the desired objectives –eliminating threats to cyberspace, establishing internationally accepted norms of behavior and maintaining stability through cooperation, the U.S. policy should focus on these 3 areas;

1. The immediate U.S. effort should focus on enhancing cyber defenses with particular regard to protecting critical infrastructure networks. A public/private partnership should be developed ensuring wide participation and benchmarking to reduce the cost of compliance. This should be the short-term goal of the U.S. policy.
2. In the long-term, the U.S. should work with states such as China in creating internationally acceptable norms regarding behavior in cyberspace. It is a fact that the most powerful states typically create such norms and the U.S., desiring cooperation with China, will have to accommodate Chinese views and interests if it is to successfully implement an international strategy for cyberspace.
3. The U.S. should be specific in stating its intentions to use conventional force in retaliation against cyber attacks. This specificity should apply to methods of

attribution; levels of attacks that will warrant kinetic response; and how much force that will be used in retaliation. Removing these ambiguities will paint a clearer picture for would-be attackers which a deterrence policy should elucidate.

As a medium, such as land, sea, air and space, cyberspace represents another avenue for states to express their hostilities towards one another. Deterring attacks within this medium will involve an articulation of intent to defend this medium, which this strategy accomplishes; and a demonstration of the willingness to do as stated. This paper concludes that the U.S. is yet to convince would-be attackers of its ability to accurately attribute responsibility for attacks allowing it to effectively direct retributive action as punishment. A thorough comprehension of the gravity of kinetic actions suggests that the U.S. will not consider it without full convictions that they are addressed to the proper responsible party.

If the logical intent of this strategy is to commence conversation and activities towards the institution of internationally acceptable norms of behavior, it has certainly achieved that objective. The debate is now being held all around the world with a wide recognition for the need to act on the issue. But the acceptance or viability of the deterrent factors as stated by the document is still far from a foregone conclusion and the United States needs to shore up its defenses against cyber attacks to protect against intrusions that compromise the integrity of its critical network infrastructures.

Appendix

Table 1. Major Cyber Attacks

Name	Year	Alleged Source	Fallout
Titan Rain	2003-2007	China	Ongoing series of attacks penetrating the networks of the U.S. departments of Defense, Energy, State and Homeland Security, as well as those of defense contractors, and downloading terabytes of data. The attacks were traced and discovered to have originated in Guangdong China.
Shady Rat	2006-2012	China	Called the "biggest cyberattack of all time", the five-year old hacking campaign infects computers at targeted organizations with a 'Trojan horse' masquerading as an innocuous email attachment. The 49 victims included the International Olympic Committee, the United Nations, ASEAN, companies in Japan, Britain, Indonesia, Denmark, Singapore and a few others, as well as the governments of the U.S., Canada, Taiwan, South Korea and Vietnam. 13 U.S. defense contractors were also targeted.
Estonia	2007	Russia	One of the most devastating attacks ever unleashed on a country, the Estonia attack followed the controversial decision to remove a Soviet ware memorial in Tallinn, the capital. The operaiton was a DDOS attack which took down the websits of Estonia's major banks, government websites and news portals.
The August War	2008	Russia	During the August 2008 Russia-Georgia war, key Georgian websites, including the pages of President Mikheil Saakashvili, the Ministry of Foreign Affairs, and the Ministry of Defense, as well as numerous corporate and media sites, were taken down by cyberattacks.At one point the Parliament's site was replaced with photos comparing Saakashvili to Hitler.
Ghostnet	2009-2012	China	Massive electronic spying discovered by Canadian researchers to have infiltrated 1,295 computers in 103 countries. Responding to a request by the office of the Dalai Lama, the researchers found that the ministries of foreign affairs and embassies in Iran, Bangladesh, Indonesia, India, South Korea, Thailand, Pakistan and Germany had all been affected.
Stuxnet	2010	Israel	Discovered in June 2010, the Stuxnet worm exploits a vulnerability in Windows to attack Siemens industrial systems, such as those used in nuclear power plants. While systems in several countries, including the United States, were affected, Iran was the worst hit, with over 16,000 computers infected. The virus seemed to be specifically targeting Iran's nuclear program, leading to suspicions that it had been designed by Israel.
India	2012	China	The hacking and release of emails belonging to the U.S.-China Economic and Security Review Commission containing documents purpoting to show Indian military intelligence plans to target the commission. Though the emails were real, the documents were found to be fake with investigators focusing on China as the most likely source of the breach.

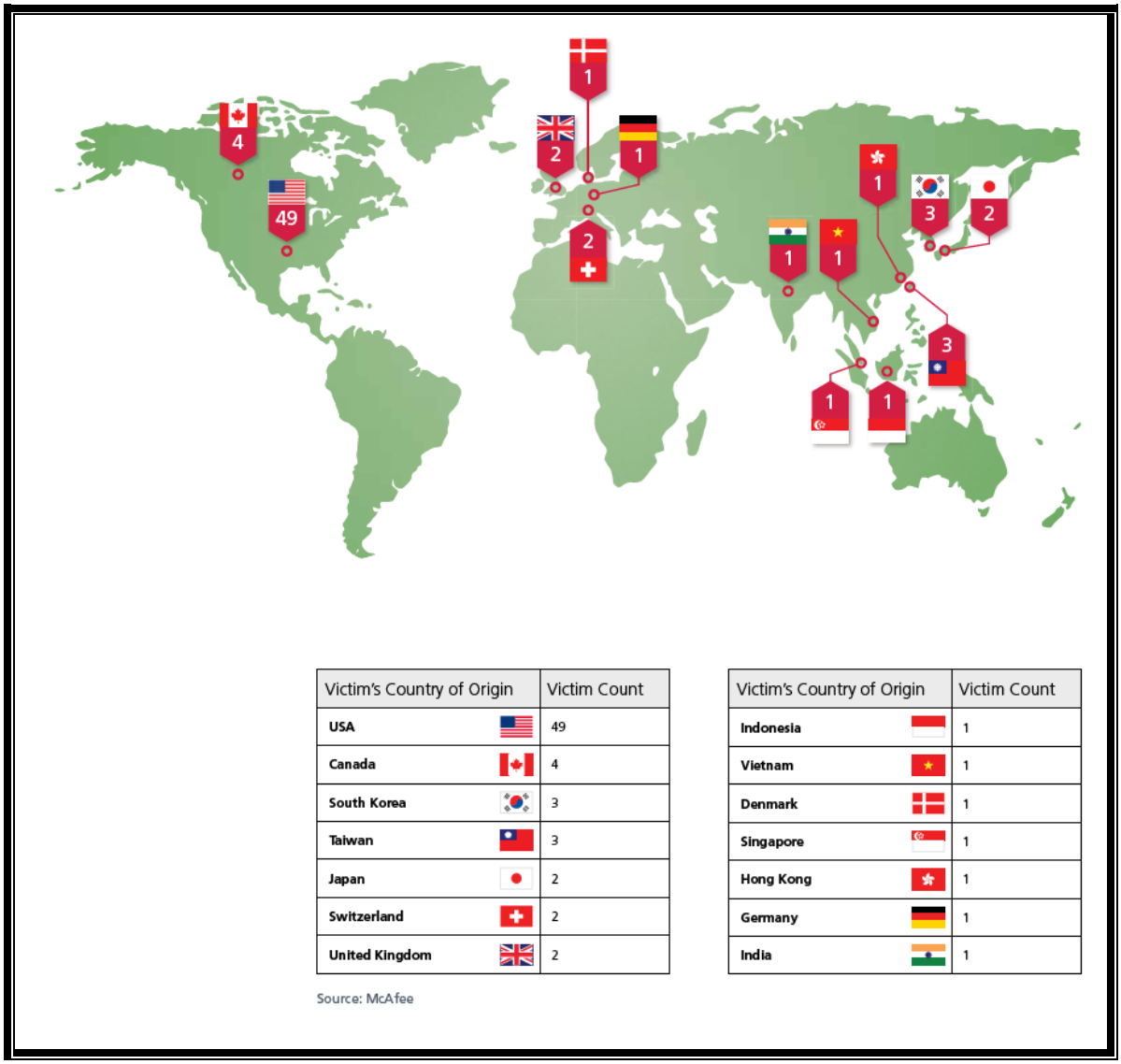
* Source; Keating, Joshua. *"Shots Fired; 10 Worst Cyberattacks."*

Table 2

Examples of Chinese Cyber Weapons and Techniques
- Planting information mines
- Conducting information reconnaissance
- Changing network data
- Releasing information bombs
- Dumping information garbage
- Disseminating propaganda
- Applying information deception
- Releasing clone (*Sic*) information
- Organizing information defense
- Establishing network spy station

* Source; Clarke & Knake 2010

Figure 1. Operation Shady RAT – Targeted Countries



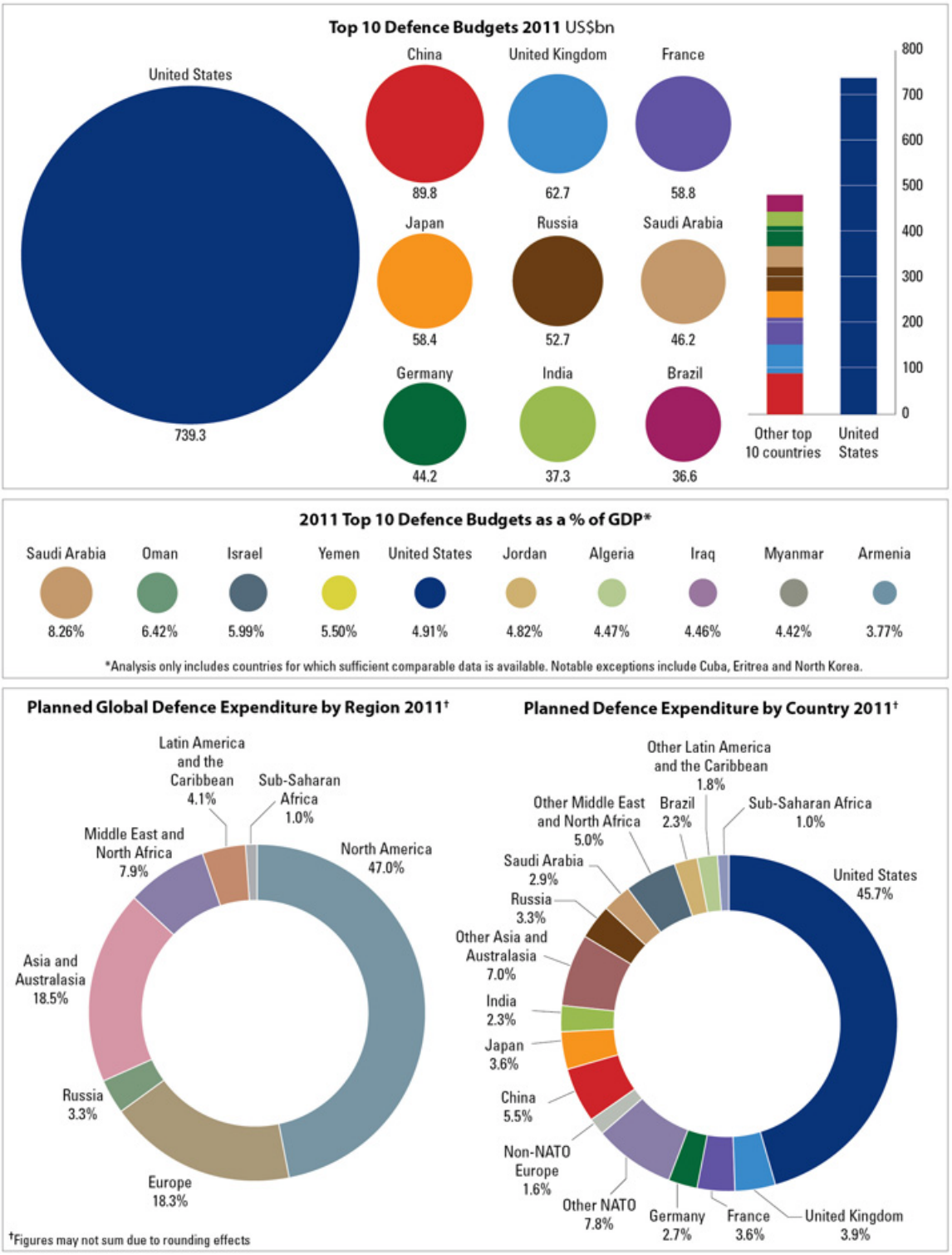
Victim's Country of Origin	Victim Count
USA	49
Canada	4
South Korea	3
Taiwan	3
Japan	2
Switzerland	2
United Kingdom	2

Victim's Country of Origin	Victim Count
Indonesia	1
Vietnam	1
Denmark	1
Singapore	1
Hong Kong	1
Germany	1
India	1

Source: McAfee

Source: McAfee

Figure 2. Comparative Defense Statistics – Defense Budgets By Region and Country



Source; Military Balance 2012. IISS

Figure 3. Projection of U.S and Chinese military spending

Source: The Economist

Glossary of terms

Cyberspace: computer networks which have been developed to manage this digital explosion; and the devices and systems which they control

Cyber war: Military operations conducted within cyberspace to deny an adversary, whether a state or non-state actor, the effective use of information systems and weapons, or systems controlled by information technology, in order to achieve a political end

Cyber Attack: A hostile act using computers, electronic information and/or digital networks that is intended to manipulate, steal, disrupt, deny, degrade or destroy critical systems, assets, information or functions

Cyber Security: The protection of computers, electronic information and/or digital networks against unauthorized disclosure, transfer, denial, modification or destruction, whether accidental or intentional

Cyber Norms: A set of shared beliefs that help define and govern behavior and conduct by state and non-state actors

Kinetic War: Military campaign deploying troops, armaments and ordinances in the aggressive resolution of conflict in physical space

Cyber Weapon: Offensive capabilities within cyberspace through which a user can compromise enemy networks gaining access and control of their networked infrastructure for purposes of espionage, destabilization or outright destruction of both civilian and military command and control systems

Malware: Malicious software disguised as innocuous programs and content which subversively grant a perpetrator unauthorized access to an infected computer leading to the exploitation of information and damage to information technology systems

Work Cited

1. Biden, Joseph. R. *"China's Rise Isn't Our Demise."* New York Times Op-Ed. 8 September, 2011. Pg. A29, New York Edition.
2. Buckley, Chris. "China Domestic Security Spending Rises to $111 billion." Reuters. 5 March, 2012. Web 12 March 2012 http://www.reuters.com/article/2012/03/05/us-china-parliament-security-idUSTRE82403J20120305 Retrieved March 12, 2012
3. Cashman, Greg and Leonard C. Robinson. "An Introduction to the Causes of War; Patterns of Interstate Conflict from World War I to Iraq". Rowan & Littlefield Publishers. Lanham, MD. 2007.
4. Clapper, James R. "*Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence*". 31 January, 2012. http://intelligence.senate.gov/120131/clapper.pdf
5. Clarke, Richard A. *"How China Steals Our Secrets."* New York Times Op-ed. 3 April, 2012. Pg. A27, New York Edition.
6. Clarke, Richard A. and Robert K. Knake. "Cyber War; the Next Threat to National Security and What to Do About It". Harper Collins, New York, NY. 2010
7. Economist. *"National Peoples Congress; Satisfy the People."* The Economist. 10 March, 2012. Web 15 March, 2012. http://www.economist.com/node/21549991

8. Economist. "*We Welcome Your Rise (sort of)*" The Economist. 15 February, 2012. Web. 3 March, 2012 http://www.economist.com/blogs/lexington/2012/02/xi-jinping
9. Economist. "*The New Colonialists.*" The Economist. 13 March, 2008. Web. 3 April, 2012. http://www.economist.com/node/10853534
10. Economist. "*China's Military Rise.*" The Economist. 7 April, 2012. Web. 12 April, 2012. http://www.economist.com/node/21552212
11. Genest, Marc A. "Conflict and Cooperation; Evolving Theories of International Relations". 2nd Edition. Thomson Wadsworth, Belmont Ca. 2004
12. Goldman, David. "*Cybersecurity Bill Passes, Obama Threatens Veto.*" CNN Money. 27 April, 2012. Web. 27 April, 2012. http://money.cnn.com//2012/04/27/technology/cispa-cybersecurity/index.htm?section=money_topstories&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+rss%2Fmoney_topstories+(Top+Stories)
13. Hille, Kathrin. "*US Seeks to Calm Beijing Containment Fears.*" Financial Times. 8 December, 2011. Web. 3 March, 2012. http://www.ft.com/intl/cms/s/0/6f00abee-216f-11e1-a19f-00144feabdc0.html#axzz1ouWUFWpM
14. Information Office of the State Council, the Peoples Republic of China. "*China's Peaceful Development.*" Chinese Government's Official Web Portal. Beijing, September 2011. Web. 3 March, 2012. http://english.gov.cn/official/2011-09/06/content_1941354.htm

15. International Institute for Strategic Studies (IISS). "*Military Balance 2012*." http://www.iiss.org/publications/military-balance/

16. Keating, Joshua, E. "Shots Fired; The 10 Worst Cyberattacks." Foreign Policy Magazine. 27 February, 2012. Web. 3 March, 2012. http://www.foreignpolicy.com/articles/2012/02/24/shots_fired?page=full

17. Kissinger, Henry A. *"The Future of U.S.-Chinese Relations."* Foreign Affairs 1 March 2012. Web 7 April 2012 http://www.foreignaffairs.com/articles/137245/henry-a-kissinger/the-future-of-us-chinese-relations?page=show

18. Krekel, Bryan; Patton Adams & George Bakos. *"Occupying the Information High Ground: Chinese Capabilities for Network Operations and Cyber Espionage."* Prepared for the U.S.-China Economic and Security Review Commission by Northrop Grumman Corp. Web. 7 March, 2012. http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf

19. Lieberthal, Kenneth and Peter W. Singer. *"Cybersecurity and U.S.-China Relations."* John L. Thornton China Center. 21st Century Defense Initiative, February 2012. Brookings Institution.

20. Lieberthal, Kenneth and Wang Jisi. *"Addressing U.S.-China Strategic Distrust."* John L. Thornton China Center Monograph Series, No. 4. March 2012. Brookings Institution.

21. Lord, Kristin M. and Travis Sharp. Eds. *"America's Cyber Future; Security and Prosperity in the Information Age. Volume I*" Center for a New American Security (CNAS). June 2011

22. Lynn III, William. J. *Remarks on the Department of Defense Cyber Strategy*. National Defense University, Washington, D.C. Thursday, July 14, 2011. Web 3 April, 2012 http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1593

23. McAfee. "Revealed: Operation Shady RAT." McAfee White Paper. http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf

24. McCormick, John. "The European Union; Politics and Policies". 4th Edition. Westview Press, Philadelphia, Pa. 2008

25. Mearsheimer, John J. "The Tragedy of Great Power Politics". W.W. Norton & Co. New York, NY. 2001

26. Menn, Joseph. *"Chinese Hackers Hit Energy Groups."* Financial Times. 11 February, 2011. Web. 3 March, 2012. http://www.ft.com/intl/cms/s/0/8a4b497a-34b4-11e0-9ebc-00144feabdc0.html#axzz1mOoXYrdu

27. Nakashima, Ellen. *"In U.S. – Russia Deal, Nuclear Communication System May Be Used For Cybersecurity."* Washington Post. 26 April, 2012. Web. 27 April, 2012. http://www.washingtonpost.com/world/national-security/in-us-russia-deal-nuclear-communication-system-may-be-used-for-cybersecurity/2012/04/26/gIQAT521iT_story.html

28. Nye, Joseph S. *"Power and National Security in Cyberspace."* Contained in America's Cyber Future; Security and Prosperity in the Information Age. Vol. II. Center for a New American Security (CNAS). June 2011.
29. Nye, Joseph S. *"Why China is Weak on Soft Power."* New York Times Op-ed. 17 January, 2012. Web. 3 April, 2012. http://www.nytimes.com/2012/01/18/opinion/why-china-is-weak-on-soft-power.html
30. Obama, Barack. *International Strategy for Cyberspace; Prosperity, Security and Openness in a Networked World*. White House, May, 2011. Web. 18 February, 2012 http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
31. Paciotti, Brian. "Classical Theory, Deterrence Theory Rational Choice Theory, Routine Activities Theory." Fall 2005 Lecture. http://www.brianpaciotti.com/lecture%208%20FALL%2005.pdf
32. Perlez, Jane. "*Continuing Buildup, China Boosts Military Spending More than 11 Percent*." New York Times, 5 March, 2012. Pg A8, New York Edition
33. Perlez, Jane. "*Chinese Insider Offers Rare and Candid Glimpse of U.S.-China Friction."* New York Times, 3 April, 2012. Pg A4, New York Edition
34. Rotter, Andrew J. Hiroshima: "The World's Bomb". Oxford UP, Great Britain. 2008
35. Rummel, Rudolph. J. "Understanding Conflict and War". Wiley. 1981.

36. Smith, Gerry. *"Cybersecurity Legislation Gaining 'Momentum' in Congress."* Huffington Post. 1 February, 2012. Web. 4 April, 2012. http://www.huffingtonpost.com/2012/02/01/cybersecurity-legislation-congress_n_1247147.html

37. Stiglitz, Joseph E. "Making Globalization Work." W.W. Norton & Co. New York, New York. 2006.

38. The US-China Business Council (USCBC). *"US-China Trade Statistics and China's World Trade Statistics."* Web. 1 March, 2012. https://www.uschina.org/statistics/tradetable.html

39. Uchegbu, Chikere. "U.S. Foreign Policy: Since 2009." PAF G 631 – Theories of International Relations. UMASS Boston, December 2010.

40. United States Trade Representative (USTR). *2011 Report to Congress on China's WTO Compliance*. December 2011. Web. 4 March, 2012. http://www.ustr.gov/webfm_send/3189

41. Watkins, Mary. "The *Perpetrators of Cyber Attacks*." Financial Times. 17 February, 2011. Web. 7 March, 2012. http://www.ft.com/cms/s/0/99793d32-3aac-11e0-9c65-00144feabdc0.html#axzz1mOoXYrdu

42. Wines, Michael. *"With Allusion to Past Chaos, China Premier Urges Reform."* New York Times, Pg. A4. 15 March, 2012.

43. Wright, Thomas. "*Strategic Engagement's Track Record*." The Washington Quarterly, 33:3 pp. 35-60. Center for Strategic and International Studies, July 2010.

44. Zagare, Frank, C. and Marc D. Kilgour. “Perfect Deterrence.” Cambridge UP. Cambridge. 2000

45. Libicki, Martin, C. “Cyberdeterrence and Cyber War.” RAND Corporation – Project Air Force. Pittsburgh, PA. 2009