REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
11-04-2015	Master of Military Studies Research Paper	September 2014 - April 2015

4. TITLE AND SUBTITLE

Force and Diplomacy in the Cyber Age

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)

Quinn, Brian M., Lieutenant Colonel, USAFR

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

N/A

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

N/A

14. ABSTRACT

Global regulation of cyber has not matched adaptation and now presents a new kind of security dilemma. Leaders in Washington and Beijing need to address this issue and establish a framework of rules or risk a potential escalating crisis. The United States and China should lead the effort to establish the regulations and norms of an international cyber standard through a bilateral agreement to avoid a conflict stemming from an escalating crisis in this domain. This agreement will help foster the familiarity and trust required of this century's two major Asia-Pacific powers.

15. SUBJECT TERMS

Cyber-diplomacy; cyber treaty

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Marine Corps University/Command a
Unclass	Unclass	Unclass	UU	33	**19b. TELEPHONE NUMBER** *(include area code)* (703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

Force and Diplomacy in the Cyber Age

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

Lieutenant Colonel Brian M. Quinn, USAFR

AY 14-15

Mentor and Oral Defense Committee Member: MATTHEW Flynn
Approved: _____
Date: 4/6/15

Oral Defense Committee Member: J.N. Gardner
Approved: _____
Date: 4/6/2015

Kevin Glathar, LtCol - USMC
4/6/15

Executive Summary

Title: Force and Diplomacy in the Cyber Age

Author: Lieutenant Colonel Brian M. Quinn, United States Air Force Reserve

Thesis: The United States and China should lead the effort to establish the regulations and norms of an international cyber standard through a bilateral agreement to avoid a conflict stemming from an escalating crisis in this domain.

Discussion: Cyber has transformed nearly every aspect of modern life and now connects approximately 42 percent of the world's population. The inherent transparency and speed open new markets, foster efficient trade, and allow for global collaboration. These factors have resulted in positive effects on global economic growth and development. Technological innovations have been militarized to create comparative advantages throughout the course of history. Cyber is no different and has been referred to by some as the fifth domain of warfare. The United States has been the dominant power in the Pacific but now faces a rising China. The balance of power politics that is emerging is dangerous and cyber is a domain where the two powers compete. Global regulation of cyber has not matched adaptation and now presents a new kind of security dilemma. Leaders of both countries need to address this issue and establish a framework of rules or risk a potential escalating crisis. Rational choice theory advocates would espouse that the two powers would act logically to avoid conflict and realize mutually beneficial gains. The historical record and advances in the science of decision-making may challenge this position. Scientific study has indicated that the amygdala, the portion of the brain associated with emotion, affects decision-making involving risk. As human emotions affect decision-making, choices are made with bias and may not reflect logical consistency. The belief that a conflict is "improbable" has historically increased the risk taking of nation-states. Additional evidence suggests that a narrative fallacy associated with "exceptionalism" may also encourage risk. The inherent anonymity of the Internet favors the offensive, a trait that has historically encouraged the assumption of risk in warfare. A framework for normative behavior is required to mitigate this risk. Richard Clarke and Robert Knake prescribe a framework for a treaty in their 2010 book, *Cyber War*, which will serve as the baseline for my proposed agreement.

Conclusion: A bilateral treaty between the United States and China to establish the standards and norms of cyberspace will help foster the familiarity and trust required of this century's two major Asia-Pacific powers. Consensus between Washington and Beijing will be a key step in avoiding falling into Graham Allison's "Thucydides Trap."

DISCLAIMER

Table of Contents

Page

Acknowledgements

Foremost, I would like to thank my research advisor, Dr. Matthew Flynn, for his help with this project. He provided key elements of direction, assistance, insight, and wit that made this experience enjoyable. Additionally, I'd like to thank my professors from this academic year, Dr. Lynn Tesser and Dr. Richard DiNardo. They provided sound guidance throughout the course and presented the complex security studies and war studies material in a thought-provoking and engaging style. I'd also like to thank my military faculty advisor, United States Marine Corps Lieutenant Colonel Kevin Glathar, for fostering an encouraging atmosphere in the conference group. My teammates in conference group eight made this a journey that I'll never forget; tailwinds to all! Finally, I'd like to thank my proofreader and source of encouragement, my wife, Claire.

INTRODUCTION

The Internet is at the core of the greatest transformation of humanity over the past twenty years. Internet users have increased from an estimated 16 million in December 1995 to over 3 billion by June 2014.[1] This platform connects over 42 percent of the world's population.[2] Cyber has altered nearly every aspect of human life and is considered the fifth domain of warfare by some. International regulation has not matched the rate of adoption to this technology and presents a significant diplomatic challenge to the great powers of the twenty-first century. This lack of governance is undermining the benefits of transparency, speed, and collaboration in the increasingly connected global economy. President Barack Obama's 2011 "International Strategy for Cyberspace," establishes hostile acts in cyberspace as *casus belli*.[3] The absence of specific terms and international standards make this unilateral proclamation somewhat dangerous. The United States and China, the two global economic leaders, have had difficulty coming to terms diplomatically and share a mutual history of nefarious cyber activity. Noted political scientist Graham Allison refers to the delicate balance of this relationship as the "Thucydides Trap."[4] He observes that since 1500, "11 of 15 cases . . . in which a rising power rivaled a ruling power, the outcome was war."[5] Allison stresses that preventing war in this case will require a generation-long, super-ordinary effort by leaders of both countries.[6] In his 2014 work *World Order*, Henry Kissinger notes that China is profoundly affected by an awareness that they did not participate in making the existing rules of the international system but expect to become centrally involved as they grow in stature.[7] As such, Washington and Beijing should lead the effort to establish the regulations and norms of an international cyber standard through a bilateral agreement to avoid a conflict stemming from an escalating crisis in this domain. This step will foster the relationships necessary to collaborate on a broad range of issues between the two powers that was identified as

the potential world of "Fusion" and humanity's "most plausible best-case outcome" in the National Intelligence Council's recent study, "Global Trends 2030: Alternative Worlds."[8]

LITERATURE REVIEW

The cyber lexicon continues to grow as the domain matures, and this paper will use the following terminology, except when directly quoting an individual or statute. Gary McGraw's "Three Headed Cyber Cerberus" consists of cyberwar, cyber-espionage, and cyber-crime; terms that are often used interchangeably by politicians and the press.[9] Richard Clarke and Robert Knake's definition of cyberwar as, "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."[10] I will use this nomenclature in my analysis. Similarly, I will use their definition for cyber-espionage as, "the unauthorized entry by a nation-state onto the networks, computers, or databases of another nation for purposes of copying and exfiltrating sensitive information."[11] Both appear in their 2010 book, *Cyber War*. INTERPOL defines cyber-crime in three broad areas: "attacks against computer hardware and software, financial crimes, and abuse." [12] This definition will serve as my standard for cyber-crime. INTERPOL recognizes the evolving nature of cyber-crime and estimates the burden on these new trends to be "running to billions of dollars" of damage to the global economy.[13] Governance of this domain will be defined by the UN Secretary General's Working Group on Internet Governance's standard as, "the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet."[14] With the specific terminology defined a look at existing research in this field will help to formulate an informed cyber position.

Recognized as the genesis of the term cyberwar, RAND Corporation researchers John Arquilla and David Ronfeldt authored their defining piece, “Cyberwar is Coming!,” in a 1993 *Comparative Strategy* article. The authors identify the information revolution as the next major shift in the nature of war that will enable innovators to avoid attrition warfare and facilitate decisive victory. This work introduces the terms netwar and cyberwar into the lexicon of theorists and policymakers. Netwar is largely non-military and represents “information-related conflict at a grand level between nations or societies.” Alternatively, cyberwar is focused on conducting military operations according to information-based principles and “turning the balance of information and knowledge in one’s favor.” Properly applied concepts associated with this Military Technology Revolution, a term the authors borrowed from the Soviet notion of a Scientific Technology Revolution, could compensate for problems associated with distance and reduced force posture. Arquilla and Ronfeldt are careful to point out that their ideas are speculative and require further discussion while suggesting that the information revolution could be changing the nature of war. They illustrate this potential change with a brief history of warfare focused on Western nation-states beginning in the 16th century. In all cases, destruction of enemy forces through violence has been a prerequisite for achieving the “aims of war” otherwise referred to as political objectives. Conversely, using the non-Western Mongol defeat of the Khwarizm as an example of a bloodless victory, the authors suggest that cyberwar may be able to achieve victory without destroying an enemy’s force.[15] The debate focused on Clausewitz’s requirement of violence to define war, and the non-Western approach continues today especially as it relates to cyber.

The terms in play reflect the state of much of the literature. One can find useful, and necessary attempts to better understand this emerging arena of international policy, but the direct

ties to the impact of that field on cyber diplomacy are underdeveloped, to say the least. An effort that becomes a laborious task of piecing together disparate assertions and analysis emerges as one attempts to understand the diplomatic tools one might utilize to avoid a pending clash between the United States and China. This study will bring much-needed order to a part of this field in need of greater clarity.

THE PENDING CLASH

Richard Clarke and Robert Knake co-authored the book, *Cyber War*, in 2010, where they detail the threat to US national security interests and explain the vulnerabilities of the western hyper-connected society in a sensationalized manner. They use historical events and published military papers to illuminate the fact that potential adversaries have long embraced cyber as an asymmetric advantage to exploit in a conflict with any conventional opponent. Furthermore, they discuss the bureaucratic challenges inherent in the US system of government to effectively address threats to national security. Existing stovepipes between the military, intelligence, and private sector communities present challenges to implementing a holistic US cyber strategy. This book served to raise public awareness of cyberwar through an alarmist hypothetical scenario but also provided a prescriptive approach for policymakers to consider going forward. Clarke's proposed roadmap reflects his experience negotiating agreements on a number of issues as part of the four administrations spanning Presidents Reagan through George W. Bush. He proposes a Cyber War Limitation Treaty (CWLT) for the United States to pursue with its key allies as the framework for a new international standard.[16] The analysis in this MMS advocates the use of the CWLT as the basis of a bilateral agreement between the United States and China, and therefore it will be explained in detail later. Clarke's advocacy became part of the mainstream dialog in 2011 at Secretary of Defense Leon Panetta's Senate Armed Services

Committee confirmation hearing. During this hearing, Panetta predicted, echoing Clarke's warning, "the next Pearl Harbor that we confront could very well be a cyberattack."[17] So no matter the sensationalism that critics believe limits the book, it has made an impact reaching the policy level.[18] Of course, Panetta's declaration underscores the seemingly reckless pronouncements regarding cyberwar. Given the high political profile of some of those making these statements, the danger of finding a sound diplomatic standing in cyberspace is all the more difficult. A stumbling toward war could well be the result of not curbing this alarmism.

How to forestall war, to curb what looks like an inevitable conflict when seen from the present and looking backward, this approach to international affairs is slowly being tied to US-Sino relations. Christopher Coker, a Professor of International Relations at the London School of Economics, analyzed the present strategies of Beijing and Washington in his 2015 work, *The Improbable War*. Coker's title is reflective of historian Jack Beatty's theory that World War I was "improbable." This "improbability" stemmed from the Great Powers feeling that war was highly unlikely leading them to assume risk and subsequently doing too little to avert conflict. Coker draws a parallel between European thinking leading up to the Great War and the predominantly held idea of present leaders in China and the United States that a future great power war is also improbable. Coker analyzes historic cases involving an inescapable spiral into conflict through the underlying narratives of the major players and the human complexities of politics as they relate to the limits of logic. He believes that growing Chinese nationalism, relationships between the PLA and the Chinese Communist Party, and intense desire to overtake the West are potential drivers of future conflict. These drivers are all reflective of Coker's principal cause of great power conflict: competition. He references the threat of Allison's "Thucydides Trap" and is led to conclude, "politics and war are often very illogical." Coker

challenges Clausewitz's role of violence in war and concludes that war is not always violent. Coker cited Napoleon's successful campaign at Ulm in 1805 as an example of a strategic victory in the absence of a violent battle in Western military history. Coker then points to the influence of Sun Tzu's thinking in Chinese culture. He further theorizes that the Chinese will look to achieve their political objectives leveraging both the cyber and space domains in any conflict. Coker ends by concluding that while conflict is not "inevitable," both powers must avoid putting too much faith in making consistent rational decisions that are in their respective best interests. He sees a constructive dialog and accountability between Washington and Beijing as requirements for a peaceful future.[19]

Investigative journalist and New American Foundation fellow on future wars Shane Harris' 2014, *@ War*, documents the rise of a US "military-internet complex." Interviews with government officials, military personnel, corporate executives, subject matter experts, and open-source documentation inform Harris' work. Harris documents the rise of the National Security Agency's (NSA) efforts to conduct cyber "information warfare" beginning in 1996. He uses a series of case studies to suggest that a cyberwar, involving the United States, is presently ongoing. Harris uses the rapid growth of the Defense Industrial Base Cyber Security/Information Assurance Program that began in 2011 with 20 corporate members to an estimated 100 by the end of 2014 to explain the growing link between the government and private industry. Harris ascertains that NSA's efforts to gain cyber superiority through a 2013 $25 million budget to purchase zero-day vulnerabilities from morally questionable "hacker" organizations such as Vupen, is creating a world-wide cyber "arms race." Harris points to a 2009 corporate "hack back" that implicated the Chinese government in the theft of proprietary Google technology that resulted in an interesting diplomatic situation. Public statements from Google that revealed their

findings went against an opinion in Washington that the relationship between the two powers was too fragile and the risk of conflict too high to publicize the information. A 2012 denial of service attack on US banks caused a significant disruption in the financial sector. Financial executives pressed the NSA to act on their behalf to stop the attacks on a previously identified critical infrastructure. NSA officials told the executives that they would not use their stockpile of cyber-weapons unless threats existed to the transactional infrastructure or accounts data. As a result, banks have become more actively involved in their defense and are now one of the biggest buyers of zero-day vulnerabilities themselves.[20] Zero-day exploits are inherently offensive in nature leading Harris to question the future norms of behavior and their strategic implications in the ungoverned, "free-fire" expanses of cyberspace.

The plausibility and the very existence of cyberwar itself have been challenged by countering schools of thought and can be summed up by the positions of two faculty members at King's College. Professor Thomas Rid contends that cyber attacks do not constitute an act of war because the violence delivered via a cyber action is both "indirect and unqualified" which differs from the violence, force, and power implied in Clausewitz's *Gewalt*. Attacks are "indirect" because the code has no inherent explosive properties to target the foundation of violence, the human body, directly. As a result of this indirect nature, the force associated with cyber attacks does not represent the sovereign legal order and, therefore, remains "unqualified." Rid contends that the vast majority of cyber attacks are sabotage designed to reduce violence by temporarily disabling economic or military machinery in a cost-efficient manner. Conversely, Dr. John Stone boldly contends, "Cyber war will take place!" Specifically, he addresses the "bloodless" nature of cyber attacks as it relates to force, violence, lethality, and Clausewitz. Stone explains, "all war involves force, but force does not necessarily imply violence - particularly if violence implies

lethality." His logic concludes that since force can be used to destroy inanimate objects it is not always lethal. Stone uses the effects-based operations of the US Army Air Corps efforts against German ball-bearing factories in Schweinfurt as a historic example of this relationship. Rid's assertion of these operations as merely sabotage is deconstructed using this case study as well. Stone contends that the Liddell Hart's indirect, liberal Western way of war and sabotage are not mutually exclusive events. He addresses the case that Clausewitz specifies war as an act of force versus violence as a borderline, philosophical matter and asserts that actions in cyber constitute acts of war.[21] Of note, the discourse analyzed has been heavily focused on the Western theory of war and may not be relevant to Chinese policymakers. The differences between the Western and non-Western theories illuminates as this analysis progresses.

The Global Economy and Information Technology

Understanding the intertwined nature of trade and influence between the United States and China is central to any discussion of international relations regarding the two countries. According to the US Census Bureau, the total US trade of goods with China in 2013 was $562 billion representing 14.6% of total US foreign trade, second only to neighboring Canada.[22] China is currently the largest foreign holder of US Treasury Bills with holdings valued at nearly $1.27 trillion as of August 2014.[23] The International Monetary Fund (IMF) estimates the 2019 nominal gross domestic products (GDPs) of the US and China to be $22.1 and $15.5 trillion respectively, exceeding 30% of gross world product.[24] All forecasting concludes that the United States and China will be the predominant individual actors in the global market for the foreseeable future. A 2013 research study conducted by PricewaterhouseCoopers projects that China will surpass the United States in purchasing power parity by 2027 with an accompanied shift of global economic power to the Asia-Pacific region.[25] This data suggests an inexorable link between that the fates of

the two economic great powers to both each other and the security of the region. Cyber is a fundamental contributor to the increased globalization of trade by providing a means to increase the speed of transactions and innovation throughout the developed world.

A Harvard University study on information technology (IT) investment and its effect on production concluded that IT was the most significant driver of increased worldwide productivity since 1989. The researchers chose 1989 as a starting point because it signified the fall of global communism and 1995 as the subdivide because it represented the beginning of a sharp decrease in the price of semiconductors and associated IT equipment. Analysis of 110 countries attributes nearly half of the 38% increase in GDP for the period of 1995-2003 as compared to the economy of 1989-1995 to IT capital investment.[26] Cyber creates opportunities to share information, leverage expertise and create efficiencies across the spectrum of human endeavors.

Cybersecurity is now a major concern to society as Internet criminality, corporate espionage, and government cyber-spying have become part and parcel of a hyper-connected world. The 2014 World Economic Forum study estimates that major technology trends could create between $9.6 and $21.6 trillion in value for the global economy.[27] However, it also estimates that if attacker capabilities outpace the ability to defend networks the corresponding slowdown in innovation would have an aggregate negative economic impact of around $3 trillion of unrealized value through 2020.[28] Major stakeholders in the global economy need to share a common framework for the security of this global common. Liberalism and neoclassical economic theory informed by Milton Friedman and Gary Becker's Chicago school of economics rational choice theory would espouse that the major agents of the global economy would act logically to realize these mutual gains. The science of decision-making and a study of history indicate that this might not always be the case.

Rational Decision Making, Risk, and War

Graham Allison's, *Essence of Decision: Explaining the Cuban Missile Crisis*, is considered a seminal work in western international relations since its 1971 release. Allison presented three conceptual models to analyze inter-state level decision-making using the Cuban missile crisis as a case study. Model I, the rational actor model, applies neoclassical economic theory to international relations and explains government actions as rational decisions designed to maximize strategic goals.[29] Model II, the organizational process, explains government behavior as the output of large sub-organizations following standard patterns of behavior that constrain the choices of individual actors and result in predictable behavior.[30] Finally, Model III or the governmental politics model explains decisions as a product of the bargaining between the individual stakeholders and the internal politics of the system they represent.[31] Allison highlights limitations of Model I through four major shortfalls.[32] Allison's criticism is summarized in his conclusion that:

> Given any action, an imaginative analyst should always be able to construct some rationale for the government's choice. By imposing, and relaxing, constraints on the parameters of rational choice . . . analysts can construct a large number of accounts of any act as a rational choice.[33]

Analysis of Allison's models elicit questions from both critics and acolytes when applying them to international politics. Bendor and Hammond in a 1992 article, "Rethinking Allison's Models," conclude that all three models require substantial reformation.[34] Much of their critique is based upon the "considerable progress in the understanding of game theory and rational choice models, in the appreciation of the role of uncertainty and incomplete information, and in development of insights about organizations, hierarchy, and bureaucratic politics" in the twenty years following Allison's original work.[35] Advocates of rational choice theory maintain that Allison's representation of Model I was inadequately developed, and "set up in order to be knocked

down."[36] Rational choice theory has maintained relevance in Western international relations theory despite criticism relating to its inherent bias towards Western values, and its disregard for culture and history.[37] For these reasons, an impetuous application of the rational actor model in US-Sino relations may not be prudent.

Nobel laureate and social scientist Herbert Simon recognized human limitations in decision-making in the 1950s; he referred to this condition as "bounded rationality."[38] Simon presented this as an alternative to the rational choice theory that had previously dominated economic and political science models. Simon proposed that individuals and organizations are challenged by imperfect information, cognitive limitations, and finite time when making a decision.[39] These challenges lead agents in complex situations to rely on heuristics that often compel them to select a satisfactory choice vice an optimal one; he referred to this phenomenon as satisficing.[40] Using Simon's ideas as a baseline, Daniel Kahneman has used empirical evidence to challenge the rational actor assumption further. Kahneman won the 2002 Nobel Prize for his research on behavioral economics and prospect theory. A significant portion of his research centers on the framing effect cognitive bias on decision-making. A 2006 University College London Institute of Neurology's study biologically validates Kahneman's theory. Researchers measured human brain activity as individuals faced decisions. They found that the amygdala, the portion of the brain associated with emotion, was active in framing subjects' decisions.[41] Specifically, they biologically supported Kahneman's theory that humans are more risk averse when faced with something to gain and more willing to accept risk when faced with a loss.[42] In summary, emotions affect decision-making, decisions do not follow a logical consistency, and the framing effect may render human choices irrational.[43]

In 1898 Jean de Bloch, a Polish financier and military theorist, concluded that great power war in Europe was "impossible" or irrational because it would "cause humanity a great moral evil . . . civil order will be threatened by new theories of social revolution."[44] As the nations of Europe were stumbling into the Great War in 1913, Norman Angell proclaimed:

> "international finance has become so interdependent and so interwoven with trade and industry that the intangibility of an enemy's property extends to his trade. It results that political and military power can in reality do nothing for trade."[45]

Despite the irrationality of the choice and interwoven economies of Europe, the leaders of the great powers decided to engage in a major conflict in July of 1914 that ultimately resulted in over 37 million casualties.[46] In the absence of rational actors and economic dependencies to thwart Allison's Thucydides Trap, we must look into the cultures that will inform the heuristics of the twenty-first century's great powers.

"Turning the Map Around"

The debate concerning the feasibility of *Gewalt* in cyber, previously reviewed through the writings of Professors Rid and Stone, underlies the discussion of Western military philosophers. Despite this discourse, the adage reminding military planners that, "the enemy gets a vote" is appropriate to any discussion of international relations and requires further analysis to prevent a mirror-imaging bias. Sun Tzu's *The Art of War* written around 500 B.C. is considered the foundation of non-Western military theory and has a significant influence on Chinese culture. The central tenant of winning without fighting can best be summed up by Sun Tzu's writings on offensive strategy.

> Thus, those skilled in war subdue the enemy's army without battle. They capture his cities without assaulting them and overthrow his state without protracted operations.[47]

This strategy differs greatly from the Clausewitz dominated Western military tradition. Coker points out this difference by noting that the word *Li*, or force, only appears nine times in the

thirteen chapters of Sun Tzu's work.[48] The Chinese emphasis on an indirect, non-violent means to prevent an enemy from imposing their will greatly explains their emphasis on militarized cyber.

This non-Western view of war coupled with a widespread belief that China only goes to war in "self-defense" make recent US strategic level foreign policy decisions threatening from a Chinese perspective. A prominent Chinese military scholar contends that virtually all of China's wars throughout the 4,000 years of the dynastic era have been internally focused.[49] Furthermore, this same scholar asserts that since 1949 all eight Chinese "military actions" have been waged in self-defense.[50] This opinion may be contrary to the Western interpretation of the Sino-Vietnamese War in 1979 but is reflective of the PLA's strategic culture. The recent US foreign policy "pivot" to Asia, as well as the growing dialog and military procurements, focused on the Air-Sea Battle fuel this national insecurity. The perception of the United States as an expansionist power has helped propagate the popular Chinese military idea of "active defense."[51] This concept, indoctrinated in PLA officers justifies the use of a preemptive strike as a measure of self-defense.[52] This idea is somewhat troubling due the aggressiveness of its nature. It is not the intent of this paper to analyze the complex Chinese civil-military relationship, but the PLA is a reflection of the society that it represents. This fact coupled with an expanding defense budget does historically imply more military influence on national strategic culture. China's military spending is estimated to have increased at an average rate of 12.9% annually since 1989.[53]

The divergence of cultural and political ideals is the central challenge to United States and Chinese diplomatic relations. Kissinger explains American thinking to be pragmatic, focused on immediate change, and reliant on an agenda of practical, deliverable items.[54] Conversely, Chinese thinking is conceptual, evolutionary, and based on future analysis of general

principles.[55] The terminology between the two great powers is also varied resulting in different meanings for the terms "information" and "cyber attack."[56] Common to both is the experience of fundamental domestic adjustments and belief that they are unique.[57] The internal challenges coupled with Mahnken's tenet of Chinese strategic culture that states, "war is costly, destructive, and leads to internal dissension," set a situation for fruitful negotiations.[58] Further analysis of the contrasting cultures of the two countries exposes the core of Allison's super-ordinary requirement of leaders in Washington and Beijing.

Exceptional Narratives and Risk

Nassim Taleb's "narrative fallacy" helps explain differences in worldview between the two powers.[59] In his work *Black Swan,* Taleb describes this misconception as, "our vulnerability to over-interpretation and our predilection for compact stories over raw truths."[60] American Exceptionalism, the view of being the "Shining City on a Hill" that can do no wrong, dates back to John Winthrop's 1630 sermon entitled, "A Model of Christian Charity." This narrative persists in the modern American psyche despite international concerns relating to Eric Snowden's leak of US government cyber-surveillance programs. China expresses its own folklore of exceptionalism as the "Middle Kingdom" that is continually under attack from foreign barbarians. This feeling remains prevalent despite a 2014 US federal indictment of five senior Chinese People's Liberation Army (PLA) officials on cyber-espionage charges. Coker warns, "belief in a country's exceptionalism may even encourage risk-taking."[61]

Despite these differences, political leaders in China and the United States both espouse positive sum outcomes for interaction in the Asia-Pacific region. Kissinger points out that the last two American presidents have made agreements with their Chinese counterparts to create a strategic partnership in the Pacific, but have failed to do much post-proclamation.[62] Cyber has

been an issue where these leaders have struggled to reach a consensus. As a result of publically documented cyber-crimes and -espionage originating from China, President Obama warned in June 2013 that cyber "was going to be a very difficult problem in the economic relationship and was going to be an inhibitor to the relationship . . . reaching its full potential."[63] NSA's alleged stockpile of over two thousand zero-day exploits for use against China coupled with a 2013 Mandiant report implicating the PLA as Advanced Persistent Threat 1 demonstrate a lack of cyber governance.[64] The Mandiant report implicates the PLA in the theft of intellectual property from 141 organizations spanning 20 major industries since 2006.[65] Cyber is at the forefront of security concerns for relations between the two powers and the security of the Asia-Pacific region.

Cyberspace and Risk

The nature of the Internet makes forensics of a cyber-attack challenging. Too often, it is very difficult to determine the intentions or sponsorship of the actor behind the attack. Open source writing on this subject suggests that the analysis of tactics, techniques, and procedures of cyber-hacks have revealed virtual fingerprints and identities. Nonetheless, there have been many documented cases of attacks involving both the United States and China that have fostered a mutual distrust. Cultural differences aside, the definitions of cyber-"crime", "-espionage", and "war" are ill-defined and subjective making the terms of any agreement difficult. The five-year long Shady RAT operation targeted more than 70 global companies, governments, and non-profit organizations beginning in 2006.[66] A single actor, largely thought to be China, exfiltrated multiple petabytes worth of information ranging from designs of classified US military technologies, corporate energy exploration data, and International Olympic Committee files.[67] Chinese officials adamantly deny these accusations calling them a reflection of a US "Cold War

mentality" narrative of a bipolar, zero-sum world order while pointing out that China, by raw numbers, is the world's largest victim of cyber attacks.[68] The absence of a common understanding and lack of trust are increasing the probability of an escalating crisis.

A recent Brookings Institute's study draws parallels between the 2011 US Department of Defense strategic cyber doctrine and the 1960s nuclear deterrence doctrine of "flexible response" that arguably led to the Cuban missile crisis.[69] Policymakers need to address this similarity to avoid repeating the lessons of the past. Kissinger emphasizes the need to elaborate on cyber doctrine and establish a framework for organizing the global cyber environment.[70] He goes further to predict that, "absent some articulation of some rules of international conduct, a crisis will arise from the inner dynamics of the system."[71] The inner dynamics of the system favor the offensive in an unprecedented manner, which historically has raised the incentive to act unscrupulously. The common interests of China and the United States require a bilateral agreement for the regulation of this domain.

COMING TO A CONSENSUS

The framework for a cyber treaty exists in agreements concerning transnational activities and use of global commons. The 2001 Council of Europe's Convention on Cybercrime treaty is the first multinational effort to address Internet based crime. As of February 2015, 44 countries have ratified this treaty.[72] The convention's main objective is to, "pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation."[73] Internet crimes that the convention focuses on include copyright infringements, computer fraud, child pornography, and network security.[74] Authorities that address the search of networks, interception of data, and international cooperation make this treaty controversial.[75] The mutual assistance provisions do not require

dual criminality causing concerns of human rights activists.[76] Despite this issue, the US Senate ratified the treaty in 2006.[77] The application of standards pertaining to global commons presents a challenge in cyber because data routes through servers that exist in sovereign countries, unlike airways or sea-lanes. Additionally, international regulations require identification and credentials to operate in the existing commons. This regulation is designed to ensure order and proper management of the global commons. The freedom associated with the Internet's inherent cloak of anonymity has made the establishment of order in cyberspace burdensome. Existing models of cooperation on issues such as arms control, public health, environmental, and global finance regimes targeting worldwide terrorism could also serve as a baseline of a dialog.[78] Proposals for cybersecurity presently focus on defensive fail-safes, offensive threats, fundamental restructuring of cyber, or some combination of all.

Richard Clarke advocated for a Cyber War Limitation Treaty (CWLT) beginning in 2010.[79] His experience working on arms control treaties greatly informs his strategy, and he proposes a treaty that incrementally increases in scope as confidence grows. His proposed treaty includes provisions to provide cyber governance through:

> "-establish a Cyber Risk Reduction Center to exchange information and provide nations with assistance;
> -create as international-law concepts the *obligation to assist* and *national cyber accountability*. . .;
> -impose a ban on first-use cyber attacks against civilian infrastructure, a ban that would be lifted when (a) the two nations were in a shooting war, or (b) the defending nation had been attacked by the other nation with cyber weapons;
> -prohibit the preparation of the battlefield in peacetime by the emplacement of trapdoors or logic bombs on civilian infrastructure, including electric power grids, railroads, and so on; and
> -prohibit altering data or damaging networks of financial institutions at any time, including the preparation to do so by the emplacement of logic bombs."[80]

Clarke suggests that the United States should coordinate this treaty with its key allies in advance of suggesting it as an international standard at the UN.[81] This MMS proposes that policymakers

in the United States should use this as a template for a bilateral treaty with China in advance of pursuing it as the international standard. Permitted actions are an important point of this treaty. These actions include preparation of the battlefield and initial cyber attacks on military targets. The first-use clause is important because an outright ban would force a kinetic response if a nation were to retaliate to a cyber attack on its civilian infrastructure. The Cyber Risk Reduction Center would enforce the national cyber accountability and obligation to assist and account for the problems presented by non-state actors and hacktivists. Enforcement mechanisms could range across a broad spectrum of economic sanctions and would serve to underwrite compliance. A formalized understanding could grow in scope, and membership, as the signatories increased mutual trust and realized the positive sum economics of stability.

A belief in free expression, held as a natural right by Western society, underlies a reluctance to any restructuring of the Internet. Non-Western nations that do not value these freedoms, such as China, have introduced real-name cyber registration policies and regularly censor Internet content through government-controlled agencies.[82] The lure of winning the strategic ideological battle through an anonymous information campaign has created an ungoverned space that serves as a safe-haven for predatory behavior. Internet “safe zones” that restrict membership, require users to provide positive identification, and disclose their location could mitigate risks to vulnerable commercial sectors. Shane Harris refers to these areas as “online gated communities” in *@ War*.[83] These areas would not be impervious to infiltration but should diminish cyber-crime and help facilitate the last provision of the CWLT. A prototype of an “online gated community" exists in a recently developed $600 million private cloud system designed for use by the CIA.[84] This cloud system, developed for the CIA by Amazon Web Services, restricts access via proprietary hardware.[85] Protecting vulnerable industries by reducing

anonymity in certain areas of the web will not fundamentally change the structure of the Internet or limit individual freedoms but will serve to provide security and order.

The United States and China have benefited from their respective positions in the most economically dynamic region of the world. The Asia-Pacific Economic Cooperation (APEC) nations represent 40 percent of the world population and 53 percent of world real GDP.[86] However, uncertainty and a lack of transparency between the two are leading to a dangerous balance of power political landscape in Asia. In the previous century, a balance of power politics was the cause of two conflicts that inflicted considerable economic and social damage throughout Europe. A similar system in the Pacific will adversely affect common interests. The National Intelligence Council's, "Global Trends 2030: Alternative Worlds" identified a most plausible worst case scenario in what it referred to as "Stalled Engines."[87] This "potential world" is characterized by an increased risk of interstate conflict, an inward focus of the United States, and stalled globalization.[88] The process of working towards a cyber agreement can educate leaders of the perils and repercussions associated with this relatively new dilemma and prevent a cyber-generated crisis.[89]

The speed of diplomacy will always lag technological innovation and cyber operations highlight this point. There are debates on both sides of the Pacific against any agreement. The United States has consistently rejected treaties on cyber arms control dating back to the Clinton administration.[90] American cultural value for freedom of information and expression, as well as a perceived belief in superior capabilities, are central to this opposition. The implicit triumph of cyber warriors in executing the Stuxnet attack created a situation where the United States may now be a victim of its success. This effort signaled the beginning of international efforts to militarize cyber for offensive operations. A 2013 US Air Force budget request included a $4

billion effort to achieve "cyberspace superiority."[91] Superiority implies the freedom to operate in any given domain while denying that privilege to an adversary. Ironically, the quest to achieve and maintain a unilateral advantage is common to both parties. China refused to accept the Russian proposal to outlaw cyber warfare because it viewed cyber as an arena where it could successfully compete with the United States.[92] The tenet of Chinese military strategic culture that espouses the possibility of achieving a decisive victory over a superior adversary through secrecy and stratagem greatly informs this position.[93] The opinion of ceding a perceived advantage is flawed by both a failure to "turn the map around" with a capability that disproportionately favors the offensive and the decision to ignore existing economic ties. Most importantly it fails to recognize that there is a danger of sliding into a conflict based upon a misunderstanding.[94]

The intertwined economies of the United States and China have greatly benefited from the advantages of IT in the ever more networked global economy. Opportunities for growth have not come without challenges and cybersecurity is at the core of these issues. The relatively new concept of cyberwar is being interpreted and explored on both sides of the Pacific. Nations have historically adopted new technologies at different rates and applied the new capabilities in a manner that suits their culture and fits their strategic goals. A lack of understanding and defined terms is evident in the hyperbole of senior leaders and news media coverage in the West. The ungoverned expanse of cyber combined with beliefs on both sides of the Pacific that conflict is in Beatty's words, "improbable" has created a situation where risk taking has increased. There has been no real discussion of cyber among leaders in Washington and Beijing; public disclosures from corporate entities such as Google and Mandiant have raised awareness and forced diplomacy. Allison's requirement of a generation-long, super-ordinary effort by the leaders in

both countries has gone unheeded and increases the risk of falling into his Thucydides Trap. The historic record suggests that nations will not always act rationally to avoid conflict and realize mutual economic gains. Neurological evidence validates Kahneman's framing effect on decision-making, particularly as it pertains to risk and rationality. The additional risk inherent in the medium of cyber, increased through the strategic narrative of both countries and encouraged by the "improbable" chance of conflict must be mitigated through a framework of normative behavior. The 2001 Council of Europe's Convention on Cybercrime exists but has been slow to gain acceptance throughout the international community. As of February 2015, only 44 of the 206 UN recognized entities have signed on to this treaty. The inclusion of China in developing the international standard for cyber would address Kissinger's concern that Beijing expects to be involved in setting policy as it grows in international stature. The basis of CWLT is fundamentally agreeable in its protection of financial institutions and civilian infrastructure both of which are crucial to the continued growth of the global economy and prosperity throughout the Pacific. Current governance of cyber can be summed up with US CYBERCOM senior legal advisor and US Air Force Colonel Gary Brown's observation:

> "So far, the customary practice of nations in cyberspace seems to be, "Do unto others whatever you can get away with." Sadly, until a major player like the United States suffers a catastrophic cyber event, it appears likely to stay that way."[95]

A bilateral cyber agreement between the United States and China could signal the starting point of greater understanding between these two nations and serve as a global model for cooperation. Additionally, it could provide the diplomatic capital and familiarity necessary to come to terms on other crucial initiatives and serve as a springboard to realize the National Intelligence Council's best-case scenario potential world of "Fusion."[96] Something like Richard Clarke's proposed CWLT could serve as a point of departure with an understanding that the agreement could escalate to omnibus levels. A treaty between the world's two greatest economic

powers could expand to include other nations and be considered the international norm for cyber cooperation.

---

[1] "Internet Growth Statistics," *Internet World Stats*, last modified December 1, 2014, accessed January 7, 2015, http://www.internetworldstats.com/emarketing.
[2] "Internet Usage Statistics," Internet World Stats, last modified February 3, 2015, accessed February 17, 2015, http://www.internetworldstats.com/stats.htm.
[3] U.S. President, Factsheet, "International Strategy for Cyberspace," accessed January 10, 2015, http://www.whitehouse.gov/sites/default/files/rss_viewer/International_Strategy_Cyberspace_Factsheet.pdf.
[4] Graham T. Allison Jr., "Obama and Xi Must Think Broadly to Avoid a Classic Trap," *The New York Times*, June 6, 2013, accessed November 10, 2014, http://www.nytimes.com/2013/06/07/opinion/obama-and-xi-must-think-broadly-to-avoid-a-classic-trap.html.
[5] Graham T. Allison Jr., "Obama and Xi Must Think Broadly to Avoid a Classic Trap," *The New York Times*, June 6, 2013, accessed November 10, 2014, http://www.nytimes.com/2013/06/07/opinion/obama-and-xi-must-think-broadly-to-avoid-a-classic-trap.html.
[6] Graham T. Allison Jr., "Obama and Xi Must Think Broadly to Avoid a Classic Trap," *The New York Times*, June 6, 2013, accessed November 10, 2014, http://www.nytimes.com/2013/06/07/opinion/obama-and-xi-must-think-broadly-to-avoid-a-classic-trap.html.
[7] Henry Kissinger, *World Order*, (New York: Penguin Press, 2014), 225.
[8] National Intelligence Council, *Global Trends 2030: Alternative Worlds* (Washington, DC: Office of the Director of National Intelligence, 2012), ii.
[9] Gary McGraw, "Cyber War is Inevitable (Unless We Build Security In)," in *Journal of Strategic Studies*, 36:1, (London: Routledge, 2013), 110.
[10] Richard A. Clarke and Robert K. Knake, *Cyber War*, (New York: Harper Collins, 2010), 6.
[11] Richard A. Clarke and Robert K. Knake, *Cyber War*, (New York: Harper Collins, 2010), 285.
[12] "Cybercrime," *INTERPOL*, accessed February 10, 2015, http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime.
[13] "Cybercrime," *INTERPOL*, accessed February 10, 2015, http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime.
[14] "What is Internet Governance?," The International Federation of Library Associations and Instiututions, accessed February 18, 2015, http://www.ifla.org/node/7406.
[15] John Arquilla and David Ronfeldt, "Cyberwar is Coming!," *Comparative Strategy*, Vol 12, No. 2, Spring 1993, pp 141-165, (Oxford: Taylor & Francis, Inc., 1993), Reprint, (Santa Monica, CA: RAND Corporation, 1997), 24-25, 28, 30, 41, 44.
[16] Richard A. Clarke and Robert K. Knake, *Cyber War*, (New York: Harper Collins, 2010), 268-271.
[17] Anna Mulrine, "CIA chief Leon Panetta: The next Pearl Harbor could be a cyberattack," The Christian Science Monitor, June 9, 2011, accessed February 17, 2015, http://www.csmonitor.com/USA/Military/2011/0609/CIA-chief-Leon-Panetta-The-next-Pearl-Harbor-could-be-a-cyberattack.
[18] Thomas Rid, "Think Again: Cyberwar," *Foreign Policy*, February 27, 2012, accessed March 11, 2015, http://foreignpolicy.com/2012/02/27/think-again-cyberwar/.
[19] Christopher Coker, *The Improbable War*, (New York: Oxford University Press, 2015), 2, 4, 6, 8, 155, 162, 163, 176, 181.
[20] Shane Harris, *@ War*, (New York: Houghton Mifflin Harcourt, 2014), Prologue, 39, 95-99, 172, 196, 203.
[21] John Stone, "Cyber War Will Take Place!," in *Journal of Strategic Studies*, 36:1, (London: Routledge, 2013), 101, 103-105, 106-107, 139-142.
[22] "Top Trading Partners-December 2013," *United States Census Bureau*, accessed November 8, 2014, https://www.census.gov/foreign-trade/statistics/highlights/top/top1312yr.html.
[23] "Major Foreign Holders of Treasury Securities," *United States Treasury Department*, accessed November 8, 2014, http://www.treasury.gov/ticdata/Publish/mfh.txt.
[24] "World Economic Outlook Database, October 2014," *International Monetary Fund*, accessed November 8, 2014, http://www.imf.org/external/pubs/ft/weo/2014/02/weodata/weorept.aspx.
[25] *World in 2050*, (London: PricewaterhouseCoopers LLP Economics, 2013), accessed November 8, 2014, http://www.pwc.com/en_GX/gx/world-2050/assets/pwc-world-in-2050-report-january-2013.pdf.

[26] Dale W. Jorgenson and Khuong Vu, *Information Technology and the World Economy*, (San Francisco: Federal Reserve Bank of San Francisco, 2005), accessed on November 9, 2014, http://www.frbsf.org/economic-research/files/6_ITAndWorldEconomy.pdf.
[27] *Risk and Responsibility in a Hyperconnected World* (Geneva: World Economic Forum, 2014), accessed November 9, 2014, http://reports.weforum.org/hyperconnected-world-2014/wp-content/blogs.dir/37/mp/files/pages/files/final-15-01-risk-and-responsibility-in-a-hyperconnected-world-report.pdf.
[28] *Risk and Responsibility in a Hyperconnected World* (Geneva: World Economic Forum, 2014), accessed November 9, 2014, http://reports.weforum.org/hyperconnected-world-2014/wp-content/blogs.dir/37/mp/files/pages/files/final-15-01-risk-and-responsibility-in-a-hyperconnected-world-report.pdf.
[29] Graham T. Allison Jr., "Conceptual Models and the Cuban Missile Crisis," *The American Political Science Review*, Vol. 63, No. 3 (Sep., 1969), 693-694, accessed January 18, 2015, http://www.jstor.org/stable/1954423.
[30] Graham T. Allison Jr., "Conceptual Models and the Cuban Missile Crisis," *The American Political Science Review*, Vol. 63, No. 3 (Sep., 1969), 698, accessed January 18, 2015, http://www.jstor.org/stable/1954423.
[31] Graham T. Allison Jr., *Essence of Decision: Explaining the Cuban Missile Crisis*, Boston: Little, Brown, 1971, 144.
[32] Graham T. Allison Jr., "Conceptual Models and the Cuban Missile Crisis," *The American Political Science Review*, Vol. 63, No. 3 (Sep., 1969), 695-696, accessed March 15, 2015, http://www.jstor.org/stable/1954423.
[33] Graham T. Allison Jr., "Conceptual Models and the Cuban Missile Crisis," *The American Political Science Review*, Vol. 63, No. 3 (Sep., 1969), 716, accessed March 15, 2015, http://www.jstor.org/stable/1954423.
[34] Jonathan Bendor and Thomas H. Hammond, "Rethinking Allison's Models," *The American Political Science Review*, Vol. 86, No. 2 (Jun., 1992), 301, accessed January 18, 2015, http://www.jstor.org/stable/1964222.
[35] Jonathan Bendor and Thomas H. Hammond, "Rethinking Allison's Models," *The American Political Science Review*, Vol. 86, No. 2 (Jun., 1992), 319, accessed January 18, 2015, http://www.jstor.org/stable/1964222.
[36] Jonathan Bendor and Thomas H. Hammond, "Rethinking Allison's Models," *The American Political Science Review*, Vol. 86, No. 2 (Jun., 1992), 319, accessed January 18, 2015, http://www.jstor.org/stable/1964222.
[37] Encyclopedia Britannica Online, "Theory of Rational Choice," accessed March 15, 2015, http://www.britannica.com/EBchecked/topic/467721/political-science/247913/Theory-of-rational-choice.
[38] Christopher Coker, *The Improbable War*, (New York: Oxford University Press, 2015), 28.
[39] Christopher Coker, *The Improbable War*, (New York: Oxford University Press, 2015), 28.
[40] Christopher Coker, *The Improbable War*, (New York: Oxford University Press, 2015), 28.
[41] Bernadetto DeMartino, et al., "Frames, Biases, and Rational Decision-Making in the Human Brain," *Science*, Vol. 313, no. 5787, pp 684-687, August 4, 2006, accessed January 19, 2015, http://www.sciencemag.org/content/313/5787/684.full?sid=4a92046a-6e53-453e-9728-bc5c70826019.
[42] Bernadetto DeMartino, et al., "Frames, Biases, and Rational Decision-Making in the Human Brain," *Science*, Vol. 313, no. 5787, pp 684-687, August 4, 2006, accessed January 19, 2015, http://www.sciencemag.org/content/313/5787/684.full?sid=4a92046a-6e53-453e-9728-bc5c70826019.
[43] Bernadetto DeMartino, et al., "Frames, Biases, and Rational Decision-Making in the Human Brain," *Science*, Vol. 313, no. 5787, pp 684-687, August 4, 2006, accessed January 19, 2015, http://www.sciencemag.org/content/313/5787/684.full?sid=4a92046a-6e53-453e-9728-bc5c70826019.
[44] Grant Dawson, "Preventing 'a great moral evil': Jean de Bloch's *The Future of War* as Anti-revolutionary Pacifism," Journal of Contemporary History, Vol 37, No 1 (Jan 2002), 5, accessed January 19, 2015 http://www.jstor.org/stable/3180743.
[45] Norman Angell, *The Great Illusion*, New York: G.P. Putnam's Sons, 1913, xi, accessed January 19, 2015, http://www.gutenberg.org/files/38535/38535-h/38535-h.htm.
[46] "World War I Casualty and Death Tables," *Public Broadcasting Service*, accessed January 19, 2015, http://www.pbs.org/greatwar/resources/casdeath_pop.html.
[47] Samuel B. Griffith, *Sun Tzu: The Art of War*, (New York: Oxford University Press, 1963), 79.
[48] Christopher Coker, *The Improbable War*, (New York: Oxford University Press, 2015), 160.
[49] Andrew Scobell, "China and Strategic Culture," (monograph, Strategic Studies Institute, U.S. Army War College, 2002), 8.
[50] Andrew Scobell, "China and Strategic Culture," (monograph, Strategic Studies Institute, U.S. Army War College, 2002), 8.
[51] Andrew Scobell, "China and Strategic Culture," (monograph, Strategic Studies Institute, U.S. Army War College, 2002), 12.

[52] Andrew Scobell, "China and Strategic Culture," (monograph, Strategic Studies Institute, U.S. Army War College, 2002), 12.
[53] "China's Defense Budget," *GlobalSecurity.org*, accessed February 14, 2015, http://www.globalsecurity.org/military/world/china/budget.htm.
[54] Henry Kissinger, *World Order* (New York: Penguin Press, 2014), 226.
[55] Henry Kissinger, *World Order* (New York: Penguin Press, 2014), 226.
[56] Kenneth G. Lieberthal and Peter W. Singer, *Cybersecurity and US-China Relations*, (Washington, DC: The Brookings Institution, 2012), vi-vii.
[57] Henry Kissinger, *World Order* (New York: Penguin Press, 2014), 226-227.
[58] Thomas G. Mahnken, *Secrecy and Stratagem: Understanding Chinese Strategic Culture*, (Sydney: Lowy Institute for International Policy, 2011), 16.
[59] Nassim Taleb, *The Black Swan*, (New York: Random House, 2007), 63.
[60] Nassim Taleb, *The Black Swan*, (New York: Random House, 2007), 63.
[61] Christopher Coker, *The Improbable War*, (New York: Oxford University Press, 2015), 29.
[62] Henry Kissinger, *World Order*, (New York: Penguin Press, 2014), 231-232.
[63] Wayne M. Morrison, *China-U.S. Trade Issues*, CRS Report for Congress RL33536 (Washington, DC: Congressional Research Service, July 10, 2014), 39, http://search.ebscohost.com/.
[64] Shane Harris, *@ War*, (New York: Houghton Mifflin Harcourt, 2014), 96.
[65] "APT1 Exposing One of China's Cyber Espionage Units," (Alexandria, VA: Mandiant, 2013), 3.
[66] Dmitri Alperovitch, *Revealed: Operation Shady RAT*, (Santa Clara, CA: McAfee, 2011), 2, accessed November 10, 2014, http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.
[67] Dmitri Alperovitch, *Revealed: Operation Shady RAT*, (Santa Clara, CA: McAfee, 2011), 2, accessed November 10, 2014, http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.
[68] Kenneth G. Lieberthal and Peter W. Singer, *Cybersecurity and US-China Relations*, (Washington, DC: The Brookings Institution, 2012), 4.
[69] Kenneth G. Lieberthal and Peter W. Singer, *Cybersecurity and US-China Relations*, (Washington, DC: The Brookings Institution, 2012), 30.
[70] Henry Kissinger, *World Order*, (New York: Penguin Press, 2014), 347.
[71] Henry Kissinger, *World Order*, (New York: Penguin Press, 2014), 347.
[72] "Convention on Cybercrime," *Council of Europe*, accessed on February 17, 2015, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG.
[73] "Convention on Cybercrime," *Council of Europe*, accessed February 15, 2015, http://conventions.coe.int/Treaty/en/Summaries/Html/185.htm.
[74] "Convention on Cybercrime," *Council of Europe*, accessed February 15, 2015, http://conventions.coe.int/Treaty/en/Summaries/Html/185.htm.
[75] "Convention on Cybercrime," *Council of Europe*, accessed February 15, 2015, http://conventions.coe.int/Treaty/en/Summaries/Html/185.htm.
[76] Declan McCullagh and Anne Broache, "Senate ratifies controversial cybercrime treaty," *CNET.com*, accessed February 15, 2015, http://news.cnet.com/2100-7348_3-6102354.html.
[77] "Convention on Cybercrime," *Council of Europe*, accessed February 15, 2015, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG
[78] Kenneth G. Lieberthal and Peter W. Singer, *Cybersecurity and US-China Relations*, (Washington, DC: The Brookings Institution, 2012), ix.
[79] Richard A. Clarke and Robert K. Knake, *Cyber War*, (New York: Harper Collins, 2010), 268.
[80] Richard A. Clarke and Robert K. Knake, *Cyber War*, (New York: Harper Collins, 2010), 269.
[81] Richard A. Clarke and Robert K. Knake, *Cyber War*, (New York: Harper Collins, 2010), 269.
[82] "Why China is trying to ban anonymity on social media," *The Week*, accessed February 15, 2015, http://www.theweek.co.uk/world-news/62096/why-china-is-trying-to-ban-anonymity-on-social-media.
[83] Shane Harris, @ War, (New York: Houghton Mifflin Harcourt, 2014), 225.
[84] Shane Harris, @ War, (New York: Houghton Mifflin Harcourt, 2014), 225.
[85] Shane Harris, @ War, (New York: Houghton Mifflin Harcourt, 2014), 225.
[86] "APEC Achievements and Benefits," *APEC: About APEC*, accessed November 16, 2014, http://www.apec.org/About-Us/About-APEC/Achievements-and-Benefits.aspx.

[87] National Intelligence Council, *Global Trends 2030: Alternative Worlds* (Washington, DC: Office of the Director of National Intelligence, 2012), ii.
[88] National Intelligence Council, *Global Trends 2030: Alternative Worlds* (Washington, DC: Office of the Director of National Intelligence, 2012), ii.
[89] Henry Kissinger, *World Order*, (New York: Penguin Press, 2014), 347.
[90] Richard A. Clarke and Robert K. Knake, *Cyber War*, (New York: Harper Collins, 2010), 219.
[91] Tom Gjelten, "First Strike: US Cyber Warriors Seize the Offensive," *World Affairs*, January/February 2013, accessed November 13, 2014, http://www.worldaffairsjournal.org/article/first-strike-us-cyber-warriors-seize-offensive.
[92] Abraham D. Sofaer, David Clark, and Whitfield Diffie, "Cyber Security and International Agreements," in *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy*, (Washington, DC: National Academy of Sciences, 2010), 192, accessed November 15, 2014, http://sites.nationalacademies.org/cs/groups/cstbsite/documents/webpage/cstb_059440.pdf.
[93] Thomas G. Mahnken, *Secrecy and Stratagem: Understanding Chinese Strategic Culture*, (Sydney: Lowy Institute for International Policy, 2011), 24.
[94] Henry Kissinger, *World Order*, (New York: Penguin Press, 2014), 347.
[95] Gary D. Brown, "Why Iran Didn't Admit Stuxnet Was an Attack," in *Joint Forces Quarterly*, issue 63, 4th Quarter 2011, 73.
[96] National Intelligence Council, *Global Trends 2030: Alternative Worlds* (Washington, DC: Office of the Director of National Intelligence, 2012), ii.

Bibliography

Allison, Jr. Graham T. *Essence of Decision: Explaining the Cuban Missile Crisis*. Boston: Little, Brown, 1971.

Allison, Jr., Graham T. "Obama and Xi Must Think Broadly to Avoid a Classic Trap." *The New York Times*, June 6, 2013. http://www.nytimes.com/2013/06/07/opinion/obama-and-xi-must-think-broadly-to-avoid-a-classic-trap.html?_r=0.

Arquilla, John and David Ronfeldt. "Cyberwar is Coming!" *Comparative Strategy*, Vol. 12, No. 2, (Spring 1993): 141-165.

Chertoff, Michael. *Homeland Security*. Philadelphia: University of Pennsylvania Press, 2009.

Clarke, Richard A., and Robert K. Knake. *Cyber War*. New York: Harper Collins, 2010.

Coker, Christopher. *The Improbable War*. New York: Oxford University Press, 2015.

Forsyth, Jr., James W., "What Great Powers Make It: International Order and the Logic of Cooperation in Cyberspace." *Strategic Studies Quarterly*, Vol. 7, No. 1, (Spring 2013): 93-113.

Gjelten, Tom. "First Strike: US Cyber Warriors Seize the Offensive." *World Affairs*, January/February 2013. http://www.worldaffairsjournal.org/article/first-strike-us-cyber-warriors-seize-offensive.

Harris, Shane. *@ War*. New York: Houghton Mifflin Harcourt, 2014.

Hughes, Rex. "A Treaty for Cyberspace." *International Affairs*, Vol. 86, No. 2, (March 2010): 523-541.

Kahneman, Daniel. *Thinking, Fast and Slow*. New York: Farrar, Straus and Giroux, 2011.

Kello, Lucas. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." *International Security*, Vol. 38, No. 2, (Fall 2013): 7-40.

Kissinger, Henry A. *World Order*. New York: Penguin Press, 2014.

Lieberthal, Kenneth G. and Peter W. Singer. *Cybersecurity and U.S.-China Relations.* Washington, DC: The Brookings Institution, 2012.

Mahnken, Thomas G. *Secrecy & Stratagem: Understanding Chinese Strategic Culture*. Sydney: Lowy Institute For International Policy, 2011.

Masters, Jonathan. "Confronting the Cyber Threat." *The Council on Foreign Relations*,

May 23, 2011. http://www.cfr.org/technology-and-foreign-policy/confronting-cyber-threat/p15577.

Morrison, Wayne M. *China-U.S. Trade Issues*. CRS Report for Congress RL33536. Washington, DC: Congressional Research Service, July 10, 2014. http://search.ebscohost.com/.

Moss, Kenneth B. *Challenges to International Regulation of Cyber Technology at War.* Copenhagen: Danish Institute for International Studies, May, 2014. http://en.diis.dk/files/media/publications/import/extra/pb2014-april_kenneth-b-moss_web.pdf.

Muir, Jr., Lawrence L. "Triangulating Cyberespionage for Better US Diplomacy." *The Diplomat*, August 2014. http://www.thediplomat.com/2014/08/triangulating-cyberespionage-for-better-us-diplomacy.

Offensive Cyber Capabilities at the Operational Level. Washington, DC: Center for Strategic and International Studies, 2013.

Rid, Thomas. "More Attacks, Less Violence." *Journal of Strategic Studies*, 36:1, (2013): 139-142.

Sofaer, Abraham D., David Clark, and Whitfield Diffie. "Cyber Security and International Agreements." In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy.* Washington, DC: The National Academies of Science, 2010.

Stone, John. "Cyber War Will Take Place!." *Journal of Strategic Studies*, 36:1, (2013): 101-108.

Taleb, Nassim N. *The Black Swan.* New York: Random House, 2007.

U.S. Department of Defense. *Military and Security Developments Involving the People's Republic of China 2013.* Washington, DC: Office of the Secretary of Defense, 2013.