Cyber Deterrence and US-Sino Cyber Relations

Regarding US-Sino cyber relations, can deterrence function in cyberspace?

By

GEORGIA LETITIA POLLOCK LEACH

A thesis submitted in partial fulfilment of the requirements for the Masters of Research in Security Studies in the Department of Security Studies and Criminology and Macquarie University, Sydney, Australia.

Due date: 10 January 2017

Thesis Supervisor: Dr Ben Schreer

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

To study the applicability of deterrence theory to the case study of US-Sino cyber relations. This thesis will attempt to determine the utility of cyber deterrence as a management tool as well as its effectiveness in cyberspace.

As the relationship between the US and China is arguably one of the most important to the international community its stability is important. Yet in recent years US-Sino relations has been detrimentally affected by a series of cyber incidents; some notably stemming from the 2013 Mandiant Report.[1] The international community is becoming progressively more reliant on the cyber domain to conduct affairs ranging from trade and economics to critical infrastructure. However, the increase in connectedness has subsequently led to an escalation in vulnerability and susceptibility to exploits for malicious purposes.[2] As the US and China have greater capabilities to undertake operations within the domain, cyber contests are of increasing concern.[3]

Deterrence theory is explored as a method to dissuade costly attacks and as a management tool for the political relationship. However, the literature on cyber deterrence is young; it needs further analysis and definitional clarity. This thesis will explore the scale and method used for various cyber incidents in an attempt to examine a more holistic picture of US-Sino relations within the domain. The infancy of cyberspace has resulted in an environment where the boundaries of acceptable behaviour are still being explored. There is a significant disconnect between the perceptions of accepted norms of the US and China within the domain. The possibility of cyber war as well as the use of the cyber domain to conduct large-scale damaging attacks should be considered. The question remains can deterrence apply to the cyber domain and if so to what extent? Moreover, is there a difference in applicability of deterrence when considering the severity of a cyber-incident? This paper seeks to determine the utility of deterrence to the US-Sino political relationship and is applicability to the cyber domain.

[1] "APT1, Exposing One of China's Cyber Espionage Units', *Mandiant* 18 February 2013, <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf> (accessed 2 March 2017).
[2] L. Rainie, J. Anderson & J. Connolly, "Cyber Attack Likely to Increase", *PewResearch Center:* Internet, Science & Tech, 29 October 2014, available at< http://www.pewinternet.org/2014/10/29/cyber-attacks-likely-to-increase/> (accessed 2 February 2016).
[3] R. A. Clark & R. Knake, *Cyber War: the Next Threat to National Security and What to do About it,* New York, Harer Collins, 2010, p. 76.

DEDICATION

For my parents and family, thank you for your continued support and encouragement.

ACKNOWLEDGEMENTS

I wish to thank my thesis supervisor, Dr Ben Schreer for his wisdom, guidance and endless patience. I would also like to thank my collegues and senior academics of the Department of Security Studies and Criminology for their support, kindness and assistance throughout this process.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

Quote: "There is perhaps no relationship as significant to the future of world politics as that between the US and China….How these two powers manage their relationship will likely be a key determinant of not only their own political and economic futures, but also wider global stability and prosperity."

- The Brookings Institute[4]

Research Question: *Regarding US-Sino Cyber Relations, can Deterrence Function in Cyberspace?*

Chapter Introduction

This thesis will examine the utility of deterrence theory within the cyber domain. The project will look specifically at the case study of cyber relations between the United States of America (US) and the People's Republic of China. It will determine whether, and to what degree deterrence is applicable to cyberspace. In doing so, the research will investigate cyber incidents ranging in scale and method, to establish if and at what level deterrence could possibly work. The applicability of classical deterrence theory to cyberspace will be assessed against available data of cyber incidents from the case study of US-Sino cyber relations. The research will explore the discourse on cyber deterrence before outlining the debate on US-Sino cyber relations. It will then determine the utility of deterrence theory to the cyber aspect of the US-Chinese political relationship. The project aims to determine the effectiveness of deterrence to the cyber domain and to identify how it is (or could be) used as a management tool for US-Sino cyber relations.

---

[4] K. Lieberthal and P. W. Singer, *Cybersecurity and US-China Relations,* John L. Thornton China Centre at Brookings, 21st Century Defense Initiative, February 2012.

Research Aims

This thesis will examine the utility of deterrence within US-Sino cyber relations. The changing nature of the political relationship between the US and China affects the way both nation-states adopt and implement methods of strategic deterrence, particularly with regard to cyber relations. The problem of recurring intrusive cyber incidents is hindering the progress of the political relationship and compounding areas of tension experienced elsewhere (for instance, China's perceived military expansion in the South China Sea). This evolution in dynamics raises new questions about the future of US-Sino relations as well as the development of cyber strategies. The research project will contribute to the academic debate by determining the utility of cyber deterrence. The thesis will put forward three key arguments regarding cyber deterrence within the context of US-Sino cyber relations.

- First, that deterrence can function in cyberspace.
- Second, that beyond a specific threshold of cyber incident, deterrence is likely to hold.
- Finally, that given these assertions, deterrence within the context of US-Sino relations will function at the more damaging levels of possible state cyber interaction. That is to say, cyber incidents beyond a perceived threshold of acceptable and bearable cost between the US and China are likely to be deterred.

The project will subsequently argue that deterrence is unlikely to function successfully in cyberspace if it is conducted solely in the cyber domain. For instance, if key elements of deterrence such as the communication of the threat and the subsequent retaliation are conducted solely through cyberspace it is unlikely to be successful. This argument directly tackles inconsistencies and weaknesses present in the current discourse, which will be put forward in the literature review. Broad-spectrum deterrence, which includes digital measures in addition to physical measures, is put forward as a more effective deterrent strategy to mitigate the risk posed by cyber incidents. This statement correlates with deterrent measures already implemented to lessen the danger of severe cyberattacks. It is the current

practice of the US government (given policy statements [Presidential Policy Directive-41][5] and Department of Defense documents made public over the last decade). However, cyber incidents that fall below a specific threshold continue to prevail due to different reasons. These reasons include but are not limited to different perspectives on accepted behaviour and norms within the domain, state interests and finally the unique characteristics of cyberspace that allow cyber incidents to proliferate with ease.

The research will also argue that should either the threshold of acceptability be surpassed, by the US or China, that retaliation not be taken in the form of a cyber-attack. The thesis aims to illustrate how malicious code employed in retaliation can disseminate and be used against the country of origin later. The project will also explain how this dissemination of malicious code could detrimentally affect the stability of the cyber environment.

Research Design

The project will employ a qualitative research method to examine available data of cyber incidents within the broader context of US-Sino cyber relations. This methodology has been adopted for its usefulness in analysing phenomena and clarifying information that is of disciplinary value.[6] In choosing the case study focusing on US-Sino cyber relations, a number of considerations were made. Firstly, that the interaction of the US and China in cyberspace is relevant to the debate on global cybersecurity. Secondly, that there is information available on cyber incidents between the US and China to conduct the necessary research. Finally, that the case study is appropriate given the constraints of the research project.

In undertaking the research, the project has adopted a US perspective. The thesis will focus on cyber incidents perpetrated against the US with a high degree of evidence suggesting Chinese government involvement. It will touch on US policy and legislation currently in place to prevent and mitigate the

[5] Presidential Policy Directive/ PPD-41, "Presidential Policy Directive – United States Cyber Incident Coordination", 26 July 2016, accessed on 1 March 2017, available from < https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>

[6] C. Lamont, *Research Methods in International Relations*, Sage Publishing, London, 2015, pp. 17-20.

risk of foreign cyber incidents. The use of open source information will form the basis of evidence presented and the thesis will rely primarily on secondary source material.

Employing a case study method, focusing on US-Sino relations, provides a clear avenue to examine cyber incidents and to understand the contextual relevance of the information.[7] The research will investigate cyber incidents in the US-Sino case study focussing on attacks with a high degree of attribution to China. The incidents put forward range in scale, severity of impact and intention. They have been chosen to illustrate the range of interactions between the US and China in cyberspace. Taken from international relations and the field of strategic studies, this approach will provide the rational for defining key concepts and terminology.

Finally, the project brings to light the need to explore the barrier between acceptable and unacceptable cyber incidents. It calls for greater debate on how best to prevent cyber-attacks that inadvertently cross the threshold of acceptable cost.

Scope and Structure

As the research focuses on nation-states, key assumptions have been made regarding their behaviour within the international political sphere. These assumptions form the theoretical framework of the thesis and were employed to better understand state behaviour within the research context. The project assumes that nation-states adhere to the theoretical principles of neo-realism and are inherently self-interested.[8] The project asserts that nation-states function rationally in an anarchical system and that their actions are motivated by self-interest.[9] Although the thesis asserts state-behaviour aligning with neo-realism it acknowledges that solutions presented realistically be drawn from more than just one school of thought. In providing possible avenues to better manage the political relationship, the thesis includes options, which correlate more closely with liberalism and constructivism as opposed to neo-realism.

[7] J. W. Creswell, *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*, (2nd ed.). Thousand Oaks, SA: Sage, 2007, pp. 35-41.

[8] Neo-realism or structured realism departs from Hans Morganthau's publications on classical realism. The theory first outlined by Kenneth Watlz in the *Theory of International Politics* (1979) states that the international system is defined by both anarchy and the distribution of capabilities. States behave according to self-interest and that their interests are paramount in relation to the interest of other nation-states.

[9] K. N. Waltz, *Theory of International Politics*, 1ST Edition, Addison-Wesley Publication & Co. 1979, pp.17-21.

This assertion correlates with different strands of deterrence theory. For deterrence to function within a political context both the defender and the challenger must be considered rational actors able to acknowledge the potential damage of a communicated threat. If either actor behaves in a manner contradictory to this, the result would be a situation in which deterrence could not be applied or where deterrence was guaranteed to fail. In employing this framework, the project undertakes a critical analysis of deterrence theory as it has been applied to US-Sino cyber relations.

In applying a qualitative methodology, clear caveats have been set to assess the validity of arguments examined. The majority of information gathered for the project is secondary source material provided by academic publications analysing theory in conjunction with relevant events in the field. Academic publications included in this thesis have met certain criteria; such as relevance of argument, proof of argument and a clear reference to other salient academics in the field. The project will examine the current literature on cyber deterrence, incorporating classical deterrence theory in its various strands. It will then examine the literature on cyberspace and the technical aspects of cyber incidents before advancing a theory on cyber deterrence.

The guidelines of the project such as time constraint and word count are limiting and affect the choice of information presented. Other considerations include the character of the debate on cyber security and the availability of relevant information. The political aspect of the cyber debate affects the utility of possible actions as well as avenues for negotiation. Due to the nature of statecraft, information pertaining to events within the context of US-Sino cyber relations and capabilities is difficult to research. Key information needed to test the applicability of deterrence theory tends to be classified, unacknowledged or unknown. Understandably, nation-states prefer to keep their cyber capabilities secret. Acknowledging the existence of a capability could result in either an arms race or attempts to mitigate the effectiveness of the capability rendering it useless.

Accessing information from the Chinese perspective is also problematic, as an authoritarian state with rigorous legislation protecting state interests the revelation of intrusions perpetrated against them is difficult to come by. Furthermore, the secrecy surrounding Chinese cyber intrusion programs and

capabilities are also closely guarded, as are those of the US government. Unless a cyber-intrusion is revealed by either the attacker, defender or a third party, information pertaining to a cyber-incident is rare. In addition, there has been an issue of secrecy and confusion in the development of effective cyber policy; as is evident by the lack of development and lateness of development of US policy. For instance, the Presidential Policy Directive-41 was implemented in mid-2016 despite years of cyber incidents.[10] In addressing these limitations, the project has conducted comprehensive research and critical analysis.

Thesis Outline

The thesis project is formulated in a logical manner. After providing a brief overview of the topic, it begins with an in-depth examination of the literature. Discussing the discourse on deterrence, cyberspace and the application of cyber deterrence to US-Sino cyber relations. In doing so the project will outline the relative strengths and weaknesses present in the current debate. The thesis will then provide an in-depth account of US-Sino cyber relations, focussing on Chinese perpetrated attacks against the US. The project will then address the key issues raised throughout the research process and articulate the projects contribution to the discourse. It will highlight the limited utility of deterrent norms and mechanisms, the issue of accurately determining the efficacy of deterrence and the probable success of broad-spectrum deterrence in dissuading severe cyberattacks. Finally, the thesis will address the thesis premise. The project will summarize the findings and discuss their implications before establishing what questions remain unresolved for the academic community.

[10] Presidential Policy Directive/ PPD-41, 2016.

CHAPTER 2

BRIEF OVERVIEW

Chapter Introduction

Arguably one of the most important relationships in international relations is that of the US and China. Both nations have sizable economies, militaries and territory, and are able to exert substantial influence in the international political sphere. Since the establishment of the People's Republic of China in 1949, the relationship between the two powers has been plagued by mistrust and confrontation.[11] The emergence of cyberspace as a new domain for conducting international affairs has further strained the relationship.[12] Both counties have decidedly different interpretations of accepted norms and the place of deterrence in cyberspace.[13] This has led to a significant disagreement over acceptable behaviour within the cyber domain. The rhetoric surrounding cyber security and the prevalence of attacks perpetrated by both nations suggests that the current political situation between the US and China is critical. However, there is yet to be a comprehensive strategy implemented by either China or the US to deter malicious activities in cyberspace. Despite entering into agreements and mounting defence systems (further explored in Chapter 4), both countries are yet to adequately address the vulnerabilities of becoming increasingly reliant on the proper functioning of cyberspace.[14]

The implementation of effective policy in cyberspace has been difficult. The cyber domain has components in both the digital and physical realms with the digital aspect often considered intangible and difficult to reconcile using conventional tactics. This unfamiliarity has given rise to both a lack of understanding of the domain as well as substantial hype regarding the prospective dangers of cyberspace. As cyber has emerged as a new domain for conducting conflict, theorists have

[11] Y. Xuetong, *The Instability of China-US Relations*, "The Chinese Journal of International Politics", Oxford Journals, Vol. 3, 13 August 2010, pp.263-292.
[12] K. Lieberthal & Wang Jisi, *Addressing U.S.-China Strategic Distrust*, "John L. Thornton China Center Monograph Series", Brookings Institute, Vol. 4, March 2012, pp. xi-xxi.
[13] S. Warren, M. C. Libicki, & A. S. Cevallos, *Getting to Yes with China in Cyberspace*, RAND Corporation, 2016, pp.vi-xiii.
[14] P. Morgan, "Applicability of Traditional Deterrence Concepts and Theory to The Cyber Realm", *Proceedings of a Workshop of Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*, University of California, Irvine, 2010, pp. 55-56.

questioned and explored methods to deter and defend against cyber incidents. Naturally, deterrence theory has been examined to fill the gap. Deterrent strategies have been extensively used throughout history to mitigate the threat of severe conflict; from its employment by the ancient Greek General Thucydides to its use by Cold War strategists, the practice has played a significant role in conflict avoidance strategies.[15] Deterrence refers to the endeavour of preventing an opponent from attacking an actor by use of threats of unacceptable consequences in retaliation.

The expansion of the cyber domain has resulted in a changing strategic landscape in the international political sphere and China's behaviour is often at odds with Western perceptions. However, historically the US has remained silent on the issue of intrusions perpetrated against it, in what is believed to be, an attempt not to draw attention to its own foreign cyber intrusion operations. In this changing political climate, the struggle for information dominance is paramount and cyber plays a key role in its evolution. As the research will demonstrate, much of the hype surrounding the prospective dangers of cyberspace are unfounded. However, there is significant evidence to suggest that military competition within the domain between the US and China is intensifying. As both nation-states have historically used deterrent methods to ensure the protection of their respective political interests the resulting situation is one where increased importance has been placed on the possible applicability of deterrence to cyberspace.

The research indicates that there are distinct levels of cyber incidents, which can be categorized by both method and scale. With regard to the US and China it becomes clear that the political relationship manifests differently at different levels of cyber interaction. This is due to distinctly different perceptions of accepted norms (arguably more related to ideas of constructivism as opposed to neo-realism) within the domain as well as the respective political interests of the US and China. Additionally the roles of key bodies within the US, such as Cyber Command and the National Security Agency (NSA), have also contributed to how the relationship has manifested.

[15] Ibid.

At the lower levels of cyber interaction, this disparity in viewpoints has publically frustrated both nation-states and led to an increasingly tense political atmosphere. In recent years the US Department of Defense (DoD) has published considerable documents addressing the development and implementation of a coherent and comprehensive deterrent strategy though it has proven ineffective at the lower levels. At present neither nation-state wishes to enter into an escalated cyber conflict. This has become apparent in recent years by efforts made to gain binding agreements on cybersecurity.[16] The historical exchange of cyber incidents between the US and China has been a constant irritant but arguably the cost incurred has been bearable. These assertions track with the current political interests of both nation-states and potentially suggest that at the higher levels of cyber interactions deterrence could work.

[16] G. Shih, *China, US Holds Talks to Bridge Cybersecurity Differences,* "The Daily Star", 14 June 2016, available from < http://www.dailystar.com.lb/News/World/2016/Jun-14/356847-china-us-hold-talks-to-bridge-cybersecurity-differences.ashx>, accessed 15 June 2016.

CHAPTER 3

LITERATURE REVIEW

Chapter Introduction

Within the sphere of international relations, deterrence has been common practice for centuries; from Thucydides to Thomas Schelling. However, it was not until after World War II that it began to be used as the ultimate recourse for the prevention of total war. It was at this time that the costs of war began to reach the theoretical threshold of acceptability.[17] This proposes that the combination of war duration and increasing destructive and lethal technology makes conducting warfare too costly. Although the current cyber debate is arguably, yet to reach that threshold the proliferation of incidents and the increased militarisation of the domain has popularised the concept of cyber deterrence. However, there are issues with applying deterrent theories to the cyber domain; namely difficulties of attribution, threat communication and an accurate understanding of possible costs incurred. Other difficulties in applying the theory revolve around the domain its self. The physical makeup of cyberspace allows for scalability, asymmetry, a significant lag in retaliatory attack time and benefit offensive as opposed to defensive capabilities. The following chapter provides an overview of the literature and a brief summary of its relative strengths and weaknesses.

Deterrence Theory

Although there are numerous deterrent theories the foundational elements are rudimentary; a threat made by a defender (actor) to a challenger (opponent) must be credible, based on capability, and will. The challenger must receive and understand the threat and their compliance in refraining from an attack is considered as maintaining the status quo. In order for deterrence to function, a credible threat has to be clearly communicated by the defender and an attack clearly attributed to the challenger. For credible deterrence, a defender must be prepared to enforce a threat using deterrent

[17] P. Morgan, *Deterrence Now*, Cambridge University Press, 2016, p.5

mechanisms such as punishment and denial. An attack can be met either with punishment in the form of offensive action or denial in the form of defensive action; usually to a protected entity. As deterrence is often used to maintain stability and security, it is often discussed in conjunction with balance of power, which focuses on the resultant implications of the aspiration for power by nation-states. [18] It outlines how nation-states wanting to maintain or surpass the status quo inevitably create an environment (referred to as the balance of power) whereby policies are created to maintain it.[19] As the literature on deterrence theory is extensive, this thesis will briefly cover the major thinkers and key components necessary for the research project.

In *The Requirements for Deterrence* published in 1954, William Kaufmann outlined what he believed were the key concepts needed for deterrence to function in international relations.[20] He articulated three distinct features a challenger needed to be convinced of. Firstly, they needed to be sure that a defender possessed an effective military capability and secondly, that they could impose unacceptable harm in using that capability.[21] Finally, Kaufmann stated that a challenger had to be sure that a defender would impose unacceptable costs if attacked.[22] There are two types of costs that are categorised by the effect of an action: unacceptable and unbearable. An unacceptable cost is severe damage that a nation-state could recover from but would undoubtedly result in significant retaliation, whereas an unbearable cost refers to damage that a nation-state could not recover from (i.e. the Cold War concept of mutually assured destruction [MAD]).

A leading academic on the topic, Patrick Morgan, used Kaufmann's metrics to help further develop his own understanding of deterrence theory. He outlined what he identified to be key aspects of the theory present during the Cold War: severe conflict, assumption of rationality, retaliatory threat, unacceptable costs, credibility of threat and finally the concept of deterrence stability.[23] These aspects were necessary for deterrence to function as a strategy during the Cold War. Morgan further

[18] L. Freedman, 'General Deterrence and the Balance of Power', *Review of International Studies*, Vol. 15, No. 2, Special Issue on the Balance of Power, April 1989, pp.199-210.
[19] H. J. Morgenthau, *The Balance of Power,* "Essential Readings in World Politics", editors K. A. Mingst & J. L Snyder, 5th edition, W.W. Norton & Company, Inc. London, 2014, pp. 99- 105.
[20] W. Kaufmann, *The Requirements for Deterrence*, Centre for International Studies, Princeton University, 1954.
[21] Kaufmann, 1954.
[22] Kaufmann, 1954.
[23] Morgan, 2016, pp.8-41.

differentiated between two types of deterrence, which had earlier been suggested by Khan (1960):[24] general and immediate.[25] He stated that general deterrence was where a defender maintained broad capabilities to dissuade a challenger from considering an attack whereas immediate deterrence was crisis focused. Immediate deterrence occurred when a challenger was already contemplating or plotting an attack; a defender not only maintained capabilities but issued threats to that specific challenger.[26] With regard to US-Sino cyber relations, the concept of immediate deterrence will be addressed later in this thesis.

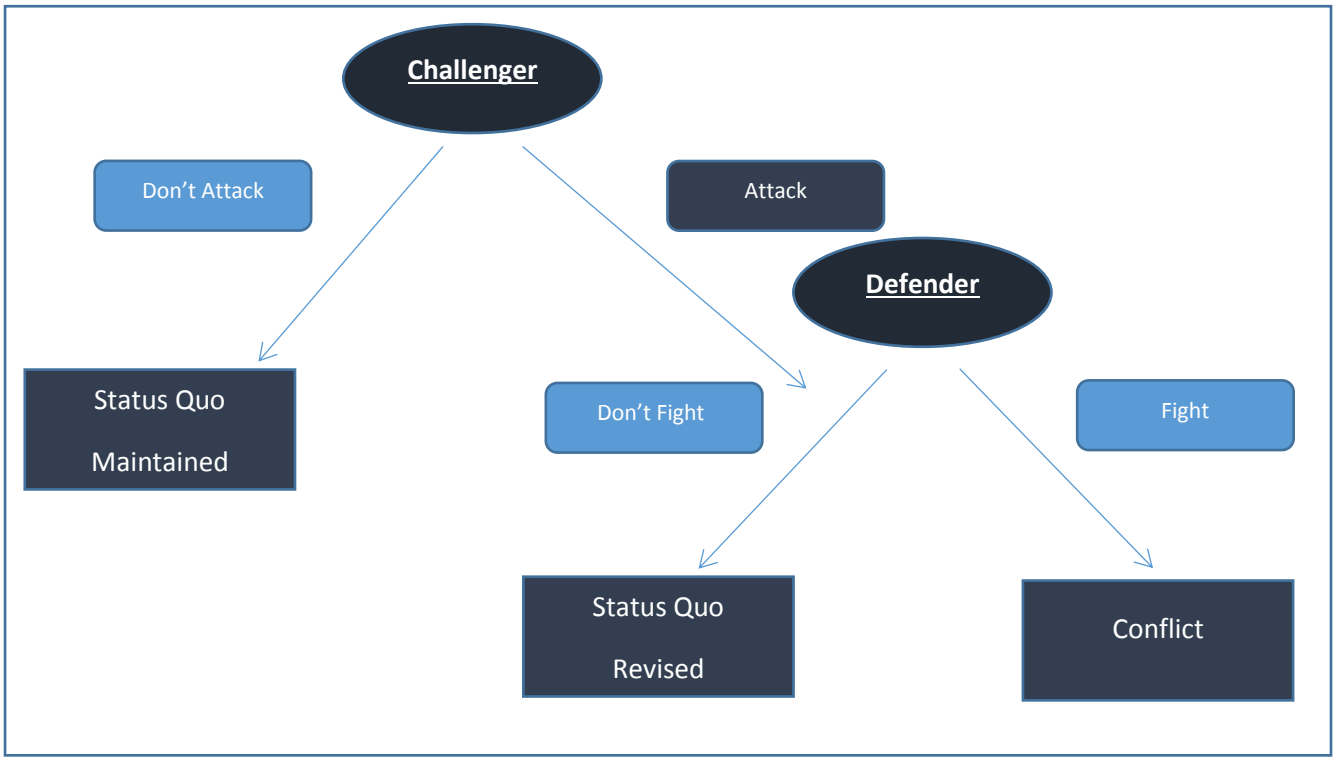

Fig. 1 Model: Classical Rational Deterrence[27]

Aside from general and immediate deterrence, there is also deterrence via defence and deterrence via retaliation (denial and punishment). These two concepts feature in many general works on deterrence by scholars including Lawrence Freedman[28] and Robert Jervis.[29] Generally, deterrence utilizing a

[24] H. Kahn, *The Nature and Feasibility of War and Deterrence,* RAND Corporation, 20 January 1960, pp. 1-48.
[25] Morgan, 2016.
[26] Morgan, 2016.
[27] J. D. Fearon, "Selection Effects and Deterrence," *International Interactions*, Taylor & Francis, Vol. 28, 2002, p.11.
[28] L. Freedman, *The Evolution of Nuclear Strategy*, New York, St. Martin's Press. 1981.
[29] R. Jervis, "Deterrence Theory Reconsidered", *World Politics*, 39, 1979, pp.289-324.

strong defence is designed to make an attack too costly or too difficult to perpetrate;[30] whereas deterrence via retaliation requires an actor to retaliate, most often through use of force, following an attack by a challenger that had been either specifically or generally threatened not to attack. Both forms have strengths and weaknesses and are often used in combination to increase the effectiveness of the deterrence posture.

The literature also highlights varying methods of deterrence other than threats. Freedman points out how deterrence by way of attacking an opponent has also been widely used in history. An actor employs the tactic of causing acceptable harm to their opponent to communicate their willingness to engage physically should the threat be ignored.[31] This tactic adds credibility to the threat, though it can also lead to escalation.

Historically there have been many occasions where both the US and China have utilized deterrence to help manage their political relationship in the past. With regard to deterrence by defence, both nations have endeavoured to fortify their territories with military capabilities to deter an attack. Historically, US capabilities have far excelled that of the Chinese.[32] Defence by retaliation was widely used throughout the Cold War by the threat of a nuclear retaliatory strike from both sides. And deterrence via attack was used during the Korean War (1950) when the Chinese launched several attacks against United Nations (UN) forces to indicate their preparedness to fight should they cross into North Korea.[33] However, it should be noted that both historically and in the present US capabilities far excel those of the Chinese.

A prominent feature of the discourse on deterrence outlines the psychological component referring to the relationship between the defender and the challenger. It is difficult to accurately assess whether or not deterrence is successfully functioning even if a challenger appears to have been dissuaded from attacking. Two comprehensive publications, which have attempted to address this issue are Huth and Russett (1990), Lebow, and Stein (1990a). Huth and Russet's paper offered guidelines to test

[30] Morgan, Patrick, "Applicability of Traditional Deterrence Concepts and Theory to The Cyber Realm", *Proceedings of a Workshop of Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy*, University of California, Irvine, 2010, pp. 55-56.
[31] Freedman, L. "Britain: The First Ex-Nuclear Power", *International Security*, Vol.6, No. 2, Fall, 1981, pp.80-104.
[32] G. J. Ikenberry, M. Mastanduno & W. C. Wohlforth, "Unipolarity, State Behaviour, and Systemic Consequence", *World Politics*, 61, No. 1, January 2009, pp. 1-27.
[33] H. Yufan & Z. Zhihai, "China's Decision to Enter the Korean War: History Revisited", *The China Quarterly*, 121, February 2009, pp. 94-115.

deterrence theory and used a variety of case studies to demonstrate the application of these guidelines.[34] Lebow and Stein's work focused on the importance of psychology of choice and bias in understanding risk within strategy.[35] The primary criticisms by Lebow and Stein against the Huth and Russett publication were mainly concerned with the case selection rather than the method applied for analysis.[36] Despite some disagreement, there are significant areas of overlap in the conclusions offered. Challenger motivation was central to the success or failure of deterrence in both publications.[37]

Deterrence theory generally assumes actors behave rationally and take into consideration the behaviour and choices of others. This correlates with Zagare and Kilgour (2000) who discuss how given the constraints of deterrent systems that demand rationality, a challenger would usually cooperate.[38] However, this tends not to be the case in practice as Lebow and Stein and Huth and Russet surmised. Lebow and Stein's findings reflect rational choice theory[39] which places more onus on the behaviour of individuals when considering the aggregate social outcome. Lebow and Stein further develop this line of thinking by distinguishing between actors who are risk-prone, gain-maximisers as opposed to risk-averse, loss-minimizers.[40] They state that assumptions regarding defender and challenger rationale are important as much of the success or failure of deterrence rests on motivation. This concept will be further explored later in this chapter.

Cyberspace

In a world where both the individual and the state are becoming increasingly reliant on the proper functioning of the cyber domain, its security is paramount.[41] A definition offered by the US Department of Defence and the Cyber Defence Centre of Excellence states:

[34] P. Huth & B. Russett, "Testing Deterrence Theory: Rigor Makes a Difference." *World Politics,* Vol. 43,1990, pp. 466-501.
[35] R. N. Lebow & J. G. Stein, *We All Lost the Cold War*¸ Princeton University Press, 1994, p. 223.
[36] F. P. Harvey, *The Future's Back: Nuclear Rivalry, Deterrence Theory, and Crisis Stability After the Cold War,* McGill-Queen's Press, 1997, p.95.
[37] Morgan, 2016.
[38] F. Zagare & D. M. Kilgour, *Perfect Deterrence*, Cambridge University Press, 2000, pp.16-28.
[39] An analytical framework used to understand and model economic and social behavior which states that collective social behavior results from individual actors making individual decisions.
[40] R. N. Lebow & J. G. Stein, World Politics, *Rational Deterrence Theory: I Think, Therefore I Deter*, Cambridge University Press, 1989, p.209.
[41] Ducheine, Osinga & Soeters (Eds.), *Cyber Warfare: Critical Perspectives*, T.M.C. Asser Press, The Hague, The Netherlands, 2012, p. 2.

Cyberspace is a global domain within the information environment. It consists of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers.

- US Department of Defence, 2011[42]

This definition illustrates the complexity and enormity of the field. Computer systems now include a variety of 'smart' devices all part of a collective known as the *internet of things*; a network of physical devices from smart phones to vehicles which are embedded with electronics and software that allow them to collect and exchange information.[43] The permeation, prevalence, importance and vulnerability of cyberspace have led to its definition as a new domain of conflict within military doctrine.[44] The ability to utilise significant resources (time, knowledge, testing grounds…etc.) and access sophisticated technologies unavailable to the public allow countries to discover, develop and exploit at an increased level of complexity. This section will focus on literature discussing cyber incidents and components of the debate relevant to the US-Sino case study.

Important features of the cyber discourse focus on how incidents are perpetrated and why they proliferate. Considering these features, it is appropriate to categorize cyber incidents by two metrics; method and scale. The following table classifies cyber incidents by methods used.

[42] US Department of Defense, *Joint Publication 3.0, Joint Operations,* Washington, DC, 2011, viewed 12 March 2016 <www.dtic.mil/doctrine/new_pubs/jointpub_operations.htm>.
[43] G. Fortino & P. Trunfio (Eds.), *Internet of Things Based on Smart Objects: Technology, Middleware and Applications*, Springer International Publishing Switzerland, Italy, 2014, p. V.
[44] D. J. Betz & T. Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power*, Routledge, London, 2011, p.9.

***Table 1 Methods for Cyber Incidents*[45]**

Type of Incident	Example 1	Explanation
1. Vandalism	Website Defacements	SQL injection or cross-scripting to deface websites.
2. Denial of Service	DDoS (Distributed denial of service)	Botnets used to effectively shut down websites with high traffic.
3. Intrusion	Trapdoors or Trojans, Backdoors	Remotely injected software for intrusions and theft.
4. Infiltrations	Logic bombs, worms, viruses, packet sniffers, keystroke logging	Different methods are used to penetrate target networks. Can be either remotely used or physically installed.
5. APT's	Advanced persistent threats	Precise, sophisticated methods that have specific targets. Move slowly to avoid detection, can be vandalism, DDoS, intrusions, or infiltrations.
6. Vandalism and Denial of Service	Cyber disputes	Combined incidents of vandalism and DDoS.
7. Intrusions and Infiltrations	Cyber disputes	Combined incidents of intrusions and infiltrations.

This table illustrates the various methods used in incidents that can occur in the cyber realm. There are a number of ways in which a malicious actor may choose to achieve their goal (vandalism, infiltration…etc.), though they are not limited to the employment of specific tactics. The exploitation of certain vulnerabilities in the pursuit of certain goals will require specific tools that may limit an actor's choice in tactics used. Aside from this, the adoption of certain methods tends to depend on factors such as popularity, available resources and convenience.

Buchanan (2016) often describes this process using a life cycle model. The use of stages of life to discuss technology and innovation is common in the literature and relates to Moor's Law, which

[45] B. Valeriano & R. C. Maness, *Cyber War Versus Cyber Realities*, Oxford University Press, 2015, p.85.

stipulates that computer hardware virtually doubles in capacity every two years.[46] Buchanan states that the life cycle of cyber threats begins with discovery followed by introduction, growth, maturation and finally, decline.[47] Buchanan's model seeks to explain the proliferation of certain exploits adding that those exploits, which conform to the life cycle model, tend to target widely used software platforms, be accessible, user friendly and not particularly sophisticated. Although Buchanan's argument focusses primarily on non-state actors it can be readily applied to nation-states; particularly regarding more common cyber incidents at the lower end of severity, such as basic intrusions. Buchanan notes the danger in cyber retaliation, highlighting the lack of control over malicious code once utilised. He aptly raises concern for the potential impact on the cyber environment. Conversely it is appropriate to illustrate the range of damage that can be inflicted by a cyber-incident.

Table 2 Severity of Scale of Cyber Incident[48]

Severity	Explanation	Examples
Category 1	Minimal damage	State Department website down, probing intrusions.
Category 2	Targeted attack on critical infrastructure or military	Financial Sector attack, DoD Hacked.
Category 3	Dramatic effect on nation-states specific strategy	Stuxnet, stolen plans of the F-35.
Category 4	Dramatic effect on a nation-state	Power grid knocked out, stock market collapse. Inlcuding 2015 Ukrainian powergrib hack.
Category 5	Escalated dramatic effect on a nation-state	Catastrophic effects on nation-state as a direct result of a cyber incident.

The vast majority of cyber incidents can be placed in categories 1 and 2 with a few rare examples such as Stuxnet (the 2010 cyber-attack on the Iranian nuclear program believed to have been

[46] G. L. Kovacich, *The Information Systems Security Officer's Guide: Establishing and Managing a Cyber Security Program*, Butterworth-Heinemann, 3rd Edition, 2016, p. 72.
[47] B. Buchanan, 'The Life Cycles of Cyber Threats', *Survival: Global Politics and Strategy*, February- March 2016, Vol. 58, pp. 39-58.
[48] Valeriano et al. 2015, p.85.

constructed by an American-Israeli partnership) [49] in category 3. To date there has been no open source information on cyber incidents classified as category 4 or 5. However, it should be noted that the 2015 December attack on the Ukrainian power grid could technically be considered as a category 4 attack.[50] Malicious hackers suspected to have originated in Russia were able to compromise three energy distribution companies temporarily disrupting supply for between 1 to 6 hours.[51] The attack affected around 230,000 people and was the first known successful hack of power grid.[52] However, given the state of affairs between the suspected challenger and defender at the time, the attack resulted in no significant retaliation.

With the exception of the above incident it is expected that a cyber-incident at categories 4 or 5 would incur severe ramifications affecting both the stability of the cyber environment and the international political sphere. As stated in the introduction this dissertation assumes that given neo-realism, nation-states act rationally; an unprovoked attack surpassing that threshold would contradict rational behaviour and risk escalation resulting in both digital and physical conflict. Due to the potential damage of category 4 or 5 cyber incidents and the gravity of their political implications, they are often the topic of debate with many scholars contributing to the discourse.

Of note, regarding cyber warfare, Dr Thomas Rid argues that it has not taken place nor will it. His argument is based on Clausewitz's three main elements for defining war.[53] Firstly, war has a violent character where by an opponent attempting to escalate violence to the extreme, usually results in casualties. Secondly, it's instrumental character where both a means (by virtue of force or threat of force) and an end (where an opponent forces an adversary to acknowledge and accept defeat), are present. Finally, the third element relates to the political nature of war. It states that war is not a single act, but is strategically considered and politically motivated.[54] Rid argues that as no cyber-attack fits all three criteria then cyber war has not taken place. He continues to elaborate suggesting that due to

[49] R. Langer, "Stuxnet: Dissecting a Cyberwarfare Weapon", *IEEE Security & Privacy*, Vol. 9, Issue 3, May-June 2011, pp.49-51.
[50] K. Zetter, "Everything we Know About Ukraine's Power Plant Hack", *Wire Magazine*, 20 January 2016, accessed 2 March 2017, available from < https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/>
[51] Ibid.
[52] Ibid.
[53] T. Rid, Cyber War Will Not Take Place, *Journal of Strategic Studies*, 35:1, 2012, pp.5-32.
[54] C. Von Clausewitz 1832, 1980, p.29.

the nature of cyberspace a cyber-attack could not fit the criteria of Clausewitz's three main elements for defining war.

Despite his argument many scholars continue to debate to possibility of cyberwar along with the prospect of categories four and five cyber incidents; notably Martin Libicki who will be discussed later in the section covering cyber deterrence.

The apparent failure of deterrent strategies at categories 1 and 2 correlates with the lower severity of impact and thus perceived accompanying costs. This in turn reflects the emphasis placed by Lebow and Stein on challenger motivation. At the more severe end of the spectrum, there are multiple factors, which could be contributing to a lack of incidents. The most obvious factor being that an attack of this nature would undoubtedly result in severe political consequences. Without provocation, there is arguably little political gain to be made from such an attack. Despite the proliferation of malicious exploits, it would also require significant cyber capabilities, which now, though highly speculated are unproven. There is however consideration to be made regarding the emergence of possible risks.

As cyber weapons and tactics evolve, nation-states may begin to take bigger risks edging closer and closer towards the threshold acceptability. It is also possible that a challenger, in pursuit of their interests will unwittingly cross the threshold resulting in an undesired escalation. As Kello (2013) notes cyber incidents are "*expanding the range of possible harm and outcomes between the concepts of war and peace – with important consequences for national and international security".*[55] Kello's assertion raises important questions about how the activities of nation-states can be kept within the boundaries of acceptability unless explicitly desired.

From a defensive capacity, cyber security focuses on the protection of information systems. It is concerned with theft and damage to software and hardware, as well as information stored. It is also focused on protecting systems from disruption or misdirection of services provided.[56] Securing cyber infrastructure has both hard and soft components. Controlling the physical access to hardware is

[55] L. Kelo, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft", *International Security,* Vol. 38, No. 2 (Fall 2013), p. 8.
[56] M. Gasser, 'What is Computer Security' in *Building a Secure Computing System*, Van Norstrand Reinhold, New York, 1988, pp. 3-6.

fundamental but it is only one part of protecting the system. Security measures that focus on software access tend to be more challenging to implement and breaches are far more difficult to detect. Control measures such as encryption, password protection and firewalls, air gapping and access control are basic components of cyber security.

Finally, a critical aspect of cyberspace is its unique architecture. The cyber domain is comprised of both digital and physical components that constantly interact. Jarno Limnéll stipulates that it is crucial to understand the interaction between the two worlds. He classifies the relationship into a framework of four categories with the classification stemming from the place of execution to the place where the damage occurs.[57]

Table 3 The Cyber – Physical Relationship[58]

Classification	Explanation	Examples
Cyber-Cyber	Refers to incidents where both the execution and resultant damage occur solely in the digital realm.	DDoS attacks, website defacement and the majority of viruses as well as information theft.
Cyber-Physical	The current literature would indicate that this is the most worrisome category and encompasses cyber-attacks that result in kinetic damage.	Such as knocking out a power grid, opening the slush gate of a dam, causing a meltdown at a power plant or other examples such as Stuxnet.
Physical-Cyber	Incidents of this nature focus on affecting the physical to cripple the cyber component.	For instance, physically damaging a server, sabotaging key components such as fans to increase the heat and crash a system or (an example provided by Limnéll) cutting crucial sea cables.
Physical-Physical	This category discusses how incidents that are executed and remain in the physical realm affect the cyber realm.	In his publication Limnéll discusses the importance of people, highlighting how if talented hackers were targeted it would prevent them from operating in cyberspace. He draws on the example of the US in 2015, targeting Junaid Hussain a cyber specialist working for the Islamic State (ISIS) terrorist organisation.

[57] J. Limnéll, "The Cyber Arms Race is Accelerating – What are the Consequences?" *Journal of Cyber Policy*, 1:1, 8 May 2016, pp.50-60.
[58] Ibid.

These four categories (first outlined by Tuija and Rauno Kuusisto, 2015)[59] highlight the importance of the cyber-physical relationship and how that connection affects strategy.

Cyber Deterrence

Though young the literature on cyber deterrence is extensive with many seeking to solidify their position in the emerging field. Will Goodman aptly states there are three contributing factors to the scholarship of cyber deterrence; the prospect of future cyberattacks (including cyberwar), the past success of deterrence theory in international relations and finally the comparatively low cost of implementing deterrent strategies.[60] The discourse ranges from those advocating for the applicability of deterrence to the cyber domain, to others completely rejecting the idea. Despite these differences, some trends can be distinguished. Through examination, it becomes clear that the vast majority of literature discusses Cold War nuclear deterrent principles in two capacities. Firstly, that it provides important lessons for the debate on cyber deterrence and secondly that it facilitates the scaffolding for effective cyber deterrence. This is an important aspect of the debate that has influenced the rhetoric of deterrence in cyberspace and also indicates how cyber threats are perceived.

Professor James Der Derian first coined the term cyber deterrence in a 1994 article published in Wired Magazine.[61] Originally, Der Derian postulated the deterrent capacity of network technologies on the physical domains in battle.[62] It was not until 1996 that academic Richard Harknett concentrated the debate of cyber deterrence to conflict occurring within cyberspace itself.[63] Since then numerous academics have contributed to the discussion forming a solid theoretical framework. The body of work can be broadly categorised into three areas; those that suggest deterrence could function in cyberspace, those that reject the concept and scholars that contribute to the debate but do not adopt a set position.

[59] T. Kuusisto & R. Kuusisto, 'Cyber World as a Social System', in M. Lehto & P. Neittaanäki (ed.), *Cyber Security: Analytics, Technology and Automation*, Springer, 2015, pp. 31-43.
[60] W. Goodman, "Cyber Deterrence: Tougher in Theory than in Practice", *Strategic Quarterly*, Fall, 2010, p. 103.
[61] J. Der Derian, "Cyber Deterrence", *Wired Magazine*, 2.09, September 1994, accessed 28 February 2016, available from https://www.wired.com/1994/09/cyber-deter/.
[62] Ibid.
[63] R. J. Harknett, "Information Warfare and Deterrence", *Parameters*, Autumn 1996, pp.93-107.

With regard to the first category, there are a number of scholars of note. Patrick Morgan, previously introduced for his work on deterrence theory has published his take on applying traditional concepts of deterrence to the cyber realm. In his work, Morgan outlines key aspects such as deterrence during the Cold War, the issue of credibility, necessary components for success and problems of stability before placing them into the context of the digital realm.[64] Appropriately, Morgan highlights how deterrence during the Cold War was essentially used to manage the political climate. Other deterrent theorists such as Joseph Nye also discuss the links between nuclear deterrence and cyber security.[65] Morgan differs from Nye by stating that the analogy is negative, being extreme in nature. Though, Morgan is quick to point out the difference between the nuclear and cyber debates (being unalike in both magnitude and character),[66] the utility of deterrence as a management tool is still relevant and will be further discussed in the following section.

Morgan also states that good cyber deterrence would require five components; the ability to immediately respond to and detect a cyber-attack, contingent defences of increasing severity to deal with attacks at the higher categories of cyber incidents, the capacity for a proportional retaliation, greater redundancy in digital resources and finally international agreement and the effective control of cyber weaponry.[67] These five components correlate with other publications on cyber deterrence.

One of the key issues of deterrence in cyberspace is threat communication. As Jervis (1979) notes, successful deterrence is dependent on signal interpretation.[68] Jervis states that deterrence theory assumes that a challenger has received and decoded a message conveying a threat.[69] However he also states that due to potential misinterpretation and faulty communication it is likely that a challenger may behave in a manner unexpected by the theory.[70] Again, this correlates with what others have said regarding the assumption of rationality and the psychological component of deterrence. This raises concern for the success of deterrence within cyberspace, as threat communication may be difficult. The current literature tends to suggest that the most appropriate means of mitigating the issue of threat

[64] Morgan, 2010.
[65] J. Nye, *Diffusion and* "Cyberpower", In J. Nye (Eds.), *The Future of Power* (pp.113-151). New York: Public Affairs. 2011.
[66] Morgan. 2010.
[67] Morgan, 2010.
[68] R. Jervis, *Review Article, Deterrence Theory Revisited*, Cambridge University Press, 1979, pp.15-20.
[69] Ibid.
[70] Ibid.

communication is to explicitly state the intent to retaliate within policy and to retaliate after the occurrence of a cyber-incident. However, both approaches have issues of clarity, proportionality and effectiveness.

In his book *Cyberdeterrence and Cyber War*, Martin Libicki discusses the same issues raised by Morgan though arguably in more detail.[71] Like Morgan, Libicki illustrates the differences in cyber deterrence as opposed to other types. Although Libicki broadly agrees with the concepts outlined by Morgan for successful cyber deterrence there is a difference in their arguments. Notably, Libicki states that the prospect of an international control of cyber weaponry is dim. Libicki recognises that as most technologies have the potential for dual usage (to be used for a legal purpose as well as malicious ones) it is difficult for lawmakers and nation-states to both legislate affectively and apply export controls. Accords such as the Wassenaar Arrangement have been established to promote transparency and greater responsibility targeting conventional arms and dual-usage goods in order to prevent the development and enhancement of military capabilities.[72] However, the ability of such Accords to prevent or limit diffusion of cyber exploits remains unclear. Realistically it is virtually impossible to prevent the diffusion of cyber exploits within the domain especially if the exploit has gained popularity of publicity through its usage.

Libicki also seeks to address issues plaguing the applicability of deterrence to cyberspace, particularly with regard to attribution. He asserts that clear attribution is unnecessary for effective deterrence, he states that a challenger must be persuaded that their actions will provoke retaliation.[73] This correlates with Lebow and Stein's notion of deterrence being an inherently psychological relationship between the defender and the challenger.[74] Additionally, Libicki outlines how adequate cyber defences would add further credibility to a cyber-deterrence posture. Although this would increase the cost of the deterrent strategy, it is highly probable that it would also improve the efficacy of deterrence.

[71] M. Libicki, "Cyberdeterrence and Cyber War", *RAND Corporation* Project Air Force, 2009.
[72] The Wassenaar Arrangement: On Export Controls for Conventional Arms Dual-Usage Goods and Technologies, 2016, viewed 5 April 2016, <http://www.wassenaar.org/>
[73] Ibid.
[74] Lebow et al. 1994.

However, as his work is part of research contracted by the US Air Force it has a distinctive military feel to it. It primarily discusses deterrence via punishment and defines cyber incidents as a "*deliberate disruption or corruption by one state of a system of interest to another state.*"[75] Notably, it does not include network exploitation and thus does not discuss the issue of cyber espionage which is a crucial component of the current cyber climate between the US and China. The military influence of the research has resulted in an argument that focuses realistically on the prospect of cyber warfare and appropriate strategies. By focussing the debate of cyber deterrence on the higher categories of cyber incidents, many of the issues influencing the failure of deterrent measures at lower levels no longer apply. These issues include a perception of low political cost, unclear attribution and scalability.

From a technical perspective, there is a significant amount of literature. Scholars such as Hanna Samir Kassab delve more deeply into the mechanical aspects of cyberspace suggesting the possible creation of a *'virus wall'* to act as a deterrent mechanism.[76] This parallels arguments made by John Mallery[77] and Chris Demchak.[78] Mallery discusses the concept of *work factors* that play into the technical discussion of cyber protection[79] whilst Demchak outlines a strategy of *security resilience* to mitigate the risk of surprise cyber-attacks.[80] Most scholars with a practical understanding of the cyber domain tend to agree that deterrent measures can be put in place.

Whilst on the other side of the debate, Valeriano and Maness (whose table's categorising cyber incidents via method and scale featured earlier in this chapter) argue that the use of deterrence in cyberspace is a misapplication of the theory.[81] Instead, they advocate for the concept of cyber restraint as an operational process.[82] They claim that *"immediate direct deterrence between two parties often*

[75] Libicki, 2009, p. 23.
[76] H. S. Kassab, 'In Search of Cyber Stability: International Relations, Mutually Assured Destruction and the Age of Cyber Wargare', pp.59-76, J-F. Kremer & B. Müller (ed.) in *Cyberspace and International Relations: Theory, Prospects and Challenges*, Geneva, Switzerland, 2014.
[77] J. C. Mallery, published in summary form in Demchak, "Resilience, Disruption, and a 'Cyber Westphalia': Options for National Security in a Cybered Conflict World." 2011.
[78] C. Demchak, *'Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security'*, University of Georgia Press, Athens, 2011, pp.174-185.
[79] Mallery, 2011.
[80] Demchak, 2011.
[81] Valeriano et al. 2015, pp.54-65.
[82] Ibid.

fails" because nation-states that attempt to increase their security position through the use of threats and the creation of alliances often fail to illicit concessions from a perceived challenger.[83]

Mirroring this argument, former practitioners such as Rhea Siers highlight the confusion with regard to the utility of deterrence in cyberspace and the inherent problems of applying theory to practice. She argues that deterrence could not prevent the penetration of critical cyber networks by malicious actors.[84] Other scholars such as Maj Lee Hsiang Wei suggest that the adoption of a cyber-deterrent strategy would be both difficult and costly.[85] He focusses on the issues plaguing cyber deterrence, such as attribution, diminished capability to retaliate and the desire to avoid escalation. Maj states that the obstacles outlined in his argument *"weaken the will to retaliate and diminish the capability to retaliate".*[86]

Furthermore, Valeriano and Maness focus on dismantling the alarming rhetoric associated with the current cyber debate; highlighting how a lack of practical understanding of cyberspace has led to the propagation of perceived cyber threats.[87] This correlates with Patrick Cirenza's argument discussing how the use of the nuclear analogy is inherently flawed.[88] In his article, Cirenza addresses the separate components linking the nuclear-cyber discourse. He outlines how the proliferation of cyber actors drastically affects the implementation of specific strategies as well as the accuracy of cyber risk assessments.[89] Cirenza concludes his argument by stating that a *"hybrid"* strategy (essentially broad-spectrum deterrence involving both digital and physical measures) could potentially overcome the obstacles of mitigating cyber incidents.[90]

Cyber Deterrence and US – Sino Relations

This concept of broad-spectrum deterrence features prominently in the literature with regard to the applicability of cyber deterrence to US-Sino cyber relations. In recent years, the relationship

[83] Ibid.
[84] R. Siers, M. D Silber & D. B. Garrie, "Cyberwarfare: Understanding the Law, Policy and Technology", (ed. 2015-2016), LegalWorks, pp. 3.1.
[85] L. H. W. Maj, "The Challenges of Cyber Deterrence", *Pointer, Journal of the Singapore Armed Forces*, Vol. 41, No. 1, 2015. Pp.1-22.
[86] Ibid.
[87] Valeriano, et al. 2015, pp.1-3.
[88] P. Cirenza, "The Flawed Analogy Between Nuclear and Cyber Deterrence", *Bulletin of the Atomic Scientists*, 22 February 2016, Accessed 27 July 2016, available from < http://thebulletin.org/flawed-analogy-between-nuclear-and-cyber-deterrence9179>
[89] Ibid.
[90] Ibid.

between the two countries has arguably been tense, with much of the discourse highlighting the effect of state sanctioned cyber incidents on the political relationship. The debate ranges from discussions on China's use of cyber espionage for economic gain to the growing strategic importance of cyberspace for future military conflict.

A number of publications debate the behaviour of the US and China within cyberspace with the discourse often mentioning deterrence and restraint in conjunction with norms. This reference to informal understandings of behaviour within cyber-society echo the assertions put forth by Huth and Russett and, Lebow and Stein with regard to the importance of perception and the psychological nature of strategy (deterrence in particular).

A 2012 publication by Kenneth Lieberthal and Peter Singer from the China Centre at Brookings discusses how deterrent norms are needed to gain greater global stability in the cyber realm.[91] They outline the significant challenges in reaching a consensus, as both countries perceive accepted behaviour within the domain differently.[92] Although, appearing constructivist in nature the utility of norms also abides by the concept of behaviour governed by state interest as in neo-realism. They state that norms currently built into the cyber domain need to be made more explicit and in order to avoid unintentional conflict and escalation, deterrent norms must be discussed and agreed upon openly.[93] This correlates with previous statements made in this dissertation regarding the question of threshold and the imperative to understand cyber boundaries.

In 2016, the RAND Corporation published a report also discussing the concept of norms and focused on how the US could potentially secure a cyber-agreement with China.[94] It outlined the concept of deterrent norms and how each country viewed acceptable behaviour within the cyber domain. The report highlighted the key issues of controversy between the two countries and posited two concepts: *red deterrence* (based on China's practice within cyberspace) and *blue deterrence* (based on the behaviour of the US in the cyber domain). Red deterrence based normative behaviour on the inherent

[91] K. Lieberthal & P. W. Singer, *Cybersecurity and U.S.-China Relations*, John L. Thornton China Centre at Brookings, February 2012, pp. 1-52.
[92] Ibid, p.7.
[93] Ibid, p.25.
[94] S. W. Harold, M. C. Libicki & A. S. Cevallos., *Getting to Yes with China in Cyberspace*, Santa Monica, C.A.: RAND Corporation, 2016, p.x.

power balance and reflected the interests of states, whilst blue deterrence regarded the concept of norms as a set of commonly agreed-upon conventions acting as boundaries preserving the common good.[95] This correlates with previous publication by organisations such as the UN notably expanding the discussion on norms and the cooperation of nation-states to prevent malicious practices within the domain.

The concept of norms is a common trend in the literature with other scholars such as Tim Stevens (2012) and Joseph Nye contributing to the discourse. In the debate on US-Sino, cyber relations the inclusion of norms tends to focus on lower scale cyber incidents where explicit deterrent threats may not function successfully given the evaluation of costs incurred. The issue of cyber espionage, cyber intrusion and theft of information are some examples that fall within the boundaries of acceptable cost and accepted methods of statecraft. For instance, one of the primary issues for US-Sino cyber relations is the usage by China of information achieved through cyber espionage to pursue economic gains. This has had a considerable effect on the political relationship, as the US perceives this as an inappropriate use of espionage tactics and will further be discussed in Chapter 4.

At the more severe levels of cyber incidents, the concept of broad-spectrum deterrence is repeatedly discussed. Will Goodman (previously introduced for his three contributing factors to the scholarship of cyber deterrence) states that major powers, such as China, have reformed their military strategies to encompass cyber features.[96] Goodman goes on to discuss how deterrence is feasible and asserts that the evolution of cyber tactics and the shift from countries to incorporate cyber characteristics into military strategies on a scale that would indicate the preparation for future conflict requires careful consideration.[97]

James Lewis, from the Centre for Strategic and International Studies, draws attention to the unlikely possibility of a purely cyber conflict (this assertion relates to Limnéll's understanding of the cyber-

[95] Ibid.
[96] Goodman, 2010.
[97] Ibid.

physical relationship).[98] In 2010, Lewis stated that a cyber-attack on critical infrastructure could prompt a kinetic response referring to the concept (using US government terminology) as *cross-domain* deterrence (also referred to as broad-spectrum deterrence).

Richard Kugler who states that the US reserving the right to kinetically respond to a cyber-attack is appropriate reinforces this concept.[99] He further outlines how the proliferation of malicious cyber methods has resulted in a general deterrent environment with *tailored* (immediate deterrence) components. Kugler also argues that cyber deterrence would function best if three deterrent mechanisms (deterrence by denial of benefits, by the imposition of costs and by offering incentives for restraint) are simultaneously employed.[100] His asserts that nations such as China may use the threat (or actual use) of cyberattacks to achieve broader political gains and leverage the US. [101] As they are currently positioning themselves as *strategic challengers*, it is appropriate for the US to employ tailored deterrent components incorporating the three deterrent mechanisms.

The literature discussing cyber deterrence in conjunction with US-Sino cyber relations is multi-faceted. At the more common levels of state-to-state cyber interaction, the discourse features the concept of deterrent norms prominently; whereas at the more severe levels of potential interaction the need for a comprehensive broad-spectrum deterrent strategy is raised. The discourse often highlights the importance of understanding perception and state interest, particularly with regard to US interpretation of Chinese cyber behaviour.

Chapter Summary

The overview of literature set forth in this chapter has been designed to outline the breadth of the discourse, drawing attention to its range and highlighting areas of particular importance to the thesis

[98] J. A. Lewis, *Cyber War and Competition in the China-U.S. Relationship*, Centre for Strategic and International Studies, Remarks delivered at the China Institutes of Contemporary International Relations, May 2010, p.3.
[99] R. Kugler, "Deterrence of Cyber Attacks", in F. D. Kramer, S. H. Starr & K. Wents (eds.), *Cyberpower and National Security*, Washington, D.C., 2009, pp.309-342.
[100] Ibid.
[101] Ibid.

premise. The body of work discussing cyber deterrence and US-Sino cyber relations features relative strengths and weaknesses, which need to be considered.

Despite the extensive literature on deterrence theory, encompassing the various strands, there is a consensus on the foundational components of functional deterrence. Kauffman's concept of the three aspects a challenger needed to be convinced of (retaliatory capability, the ability to impose unacceptable costs and a defender's will to retaliate) tends to be universally agreed upon. There are also distinct similarities between how different scholars distinguish between general and immediate deterrence as well as deterrent methods such as by denial or by punishment. The literature tends to diverge when discussing aspects for the practical application of deterrence. For instance the criticism made by Lebow and Stein against the Huth and Russett publication focused on the case selection rather than the method applied for analysis.[102]

On the other hand, the literature on cyberspace encompasses a myriad of different approaches. Buchanan's life cycle model for understanding the diffusion of cyber threats aptly raises concerns regarding the behaviour of states within the cyber environment and the risk of adverse effects from the pursuit of capabilities.[103] He specifically addresses the effect of cyber incidents on the health of the cyber environment and chooses to focus his argument on the evolution of threats.

Whereas Tables 1 and 2, featuring models put forward by Valeriano and Maness, focus on method and scale of incident highlighting the danger of inflammatory rhetoric. The first table highlights possible methods for cyber incidents (Table 1) but arguably lacks technical depth.[104] It falls short of providing a rounded description of the variety of the practical methods utilised in the cyber domain. Conversely, Table 2, which focusses on the categorisation of scale of cyber incidents, gives a suitable description of range of incident and threshold of acceptability.[105] The final table, setting forth Limnéll's observation of the cyber-physical relationship identifies an important feature of the debate

[102] Morgan, 2010.
[103] Buchanan, 2016.
[104] Valeriano et al, 2015.
[105] Ibid.

rarely raised by other scholars.[106] However although he outlines the four categories well, he fails to provide a clear understanding of incident scale.

Regarding cyber warfare, Rid's argument against the likelihood of it taking place now or in the future is overly theoretical. It fails to consider that modern warfare realistically encompasses elements across multiple domains. Two case studies often used as examples of cyber war (though both highly contested), Estonia 2007 and Georgia 2008, were in reality *multi-domainal* in nature. Although the cyber aspect of both conflicts was extensive, it was still in addition to conventional military force.

With regard to the issue of cyber deterrence, again Valeriano and Maness have proved useful raising valid concerns regarding the perceived danger of cyber threats and the corresponding hype in cyber rhetoric.[107] However, their assertion that the concept of cyber deterrence would be a misapplication of deterrence theory because the usage of threats cannot work in the cyber conflict paradigm overlooks the importance of the cyber-physical relationship and the reality of cross-domain conflict and threat communication.

Finally, the literature on deterrence and US-Sino cyber relations tends to naturally group itself into two categories. The first focusses on the current issues affecting the political relationship (the disagreement on norms and accepted behaviour in cyber space, China's usage of espionage for economic gains, the issue of state cyber sovereignty…etc.). In this category, the literature sets forth options for achieving international agreement and improving bilateral relations through the development of international cyber norms. The second grouping of work has two components the first discussing cyber as a component of military capabilities and the second focussing on the hypothetical possibility of cyber in an severely damaging offensive capacity (such as a kinetic cyber-attack in a non-military environment). This category puts forward arguments specifying the need for cohesive deterrent measures encompassing multiple deterrent mechanisms as well as broad-spectrum deterrence needed to mitigate this level of cyber threat. Although the literature tends to reflect a distinction between levels of severity of scale of cyber incident it lacks definitional clarity.

[106] Limnéll, 2016.
[107] Valeriano et al, 2015.

This distinction in scale of cyber incident can also be seen in Libicki's work on cyber deterrence choosing to focus the debate at the more damaging end of incident scale. An area where he suggests clear attribution is unnecessary given the correct signalling of a defender's intent to retaliate.[108] The benefit of focusing the debate on cyber deterrence at the more severe levels of cyber incidents is that deterrence is more likely to work given the challenger's evaluation of costs incurred – it is assumed that challenger offence advantage would begin to curve as defender damage becomes greater and risk of retaliation increases.

The literature suggests that the functionality of cyber deterrence to specific political relationships (US-Sino cyber relations in this case) tends to be based on multiple factors and case specific. These factors include scale and method of attack, defender will and capability to retaliate, challenger interest and clear communication of threat. However testing the effective utility of deterrent measures in cyberspace remains a difficult task, with no clear avenue set forth in the literature.

[108] Libicki, 2009.

CHAPTER 4

CASE STUDY: US-SINO CYBER RELATIONS

Chapter Introduction

In recent decades a growing body of literature has discussed the possibility of an alleged *'power shift'* between the West and the East with a specific focus on the US and China.[109] There are a number of contributing factors to the debate with the rise of China's economy being a principle component. Despite this discussion, a power sift may not necessarily be occurring as the supposed shift is heavily reliant on varying methods of calculating state power. However, it is the perception of a shift that has given rise to an environment of increased competition and placed greater emphasis on the importance of US-Sino relations. The evolution of cyberspace and its growing importance to nation-states has resulted in an atmosphere of strategic distrust between the US and China. Revolving around the utility of cyberspace by both nations, this atmosphere has become a central concern for US-Sino relations.[110] Both the US and China have different interpretations of the place of cyber within state affairs. Each has different views on how best to legislate the domain domestically, its incorporation into military doctrine and how their respective populations interact with the domain. There is also disagreement over what constitutes acceptable norms and procedures in cyberspace internationally.

The infancy of the domain has resulted in an environment where countries are still experimenting and testing the limits of acceptable behaviour. Nations-states rely on the proper functioning of cyber space. How the US and China manage their relationship and reconcile their differences in cyberspace will set the standard for the international community. Reaching an agreement on norms or cooperative implementing mechanisms will outline what cyber incidents (categories 1 to 3 of the cyber incident scale) will be tolerated by other nation-states.[111] At the other end of the scale the applicability of broad

[109] C. Pan, *A Conceptual Corrective to the "Power Shift" Narrative*, Deakin University, 2013, pp.1-21.
[110] Lieberthal et al. 2012, pp. 1-52.
[111] Ibid.

deterrent methods to cyberspace will also provide a clear indication of the cyber threshold (the point at which a retaliatory attack from a cyber incident would be highly likely).

This chapter will provide an in-depth account of US-Sino cyber relations and the applicability of cyber deterrence as a means of managing the relationship. It will focus on Chinese perpetrated cyber incidents against the US and explore how each country has incorporated cyber components into both their military and state affairs. The information put forward in this chapter will demonstrate the history of the relationship as well as different levels of cyber incidents to establish if and at what level deterrence could possibly function. The applicability of cyber deterrence to US-Sino cyber relations will be assessed against available data of incidents with a high probability of Chinese government sponsorship.

History of Relations

Cyber relations between the US and China have historically been turbulent. The rapid expansion of cyberspace, a domain few clearly understood, led to an increase in hype and inflammatory rhetoric. In 1998, Pentagon computer networks came under attack over a series of days.[112] It was concluded that the attack was of Chinese origin and the US Department of Defence was advised to begin contemplating a cyber-counter strike in retaliation. However, it was soon discovered that the sustained attack was not perpetrated by China but instead by a number of teenagers in Cupertino, California effectively testing their luck.[113] The readiness to retaliate without a clear attribution or the consequences a retaliatory strike could have on both the relationship and the cyber environment indicates the level of distrust that previously existed within the relationship. Despite several scholars, commenting on the recent breakdown of relations there is evidence to suggest that the relationship has always been marred by mistrust.

[112] J. A. Lewis, *Computer Espionage, Titan Rian and China*, Centre for Strategic and International Studies – Technology and Public Policy Program, December, 2005.
[113] Ibid.

From the US perspective, the current state of affairs is the direct result of a series of malicious cyber incidents perpetrated by China. The first major attack attributed to the Chinese was the discovery of what the US government referred to as Titan Rain.[114] Discovered in 2003 and believed to have penetrated the system several years beforehand, Titan Rain was a series of coordinated cyberattacks on US systems.[115] The espionage ring was aimed at stealing sensitive military information from secured US defence systems. It was able to penetrate a number of secure facilities including US Army Information Systems Engineering Command at Fort Huachuca, Arizona, Defence Information Systems Agency in Arlington, Virginia, the Naval Ocean Systems Centre in San Diego, California and finally the Army Space and Strategic Defence installation, Huntsville, Arizona.[116]

The ease at which Titan Rain was attributed to Chinese hostile intelligence services raises concern. Scholars have drawn attention to the lack of security of Chinese networks making them an attractive platform for third country attacks. The impression of China as the *threat du jour* has also played a role. However, when considering the choice of targets, the sophistication of the penetration and the successful tracing of its origins to Southern China it is highly likely that Titan Rain is a Chinese state sanctioned cyber-attack against the US.[117]

China's lack of network security and its attractiveness for staging third country attacks, insuring false attribution, was raised again in 2006 after a series of cyberattacks on the US State Department. Specifically targeted was the bureau of East Asian and Pacific Affairs, which coordinates US diplomatic policy to countries such as China, Japan and North and South Korea.[118] An investigation into the incident suggested the hackers stole sensitive information and passwords and purposefully left *backdoors* to continue the intrusion later. It was noted that the department's classified systems were not penetrated by the widespread intrusions.[119] Although the attacks were speculated to have been Chinese orchestrated, the evidence was largely circumstantial. The Pentagon had released statements earlier in the year stating that the People's Liberation Army (PLA) was exploring the use

[114] N. Thornburgh, "Inside the Chinese Hack Attack", *Time Magazine*, New York, 25 August 2005.
[115] Ibid.
[116] Ibid.
[117] B. Graham, "Hackers Attack Via Chines Wed Sites", *The Washington Post*, Washington, D.C., 25 August 2005.
[118] C. Lagorio, "State Department Computers Hakced", *CBSNEWS*, 11 July 2006, available from CBSNEWS < http://www.cbsnews.com/news/state-department-computers-hacked/> (accessed 15 June 2016).
[119] Ibid.

of hacking as an offensive weapon.[120] Though it was also noted that the information targeted and the possibility of a third country attack could implicate North Korea.

In 2009, a Pentagon report outlined how the PLA emphasised the importance of information dominance in modern warfare.[121] It went on to highlight the gains made by the PLA in recent years with regard to the development of offensive nuclear, space and cyber warfare capabilities. It also stipulated that these capabilities gave China the potential to act globally.[122] The Pentagon report was published a week before the completion of a ten-month investigation by the Munk Centre for International Studies in Toronto into a cyber-espionage ring called GhostNet.[123] Unlike previous attacks speculated to have been orchestrated by China, GhostNet was a series of hacks spanning multiple countries. GhostNet was designed to scan systems for sensitive information, targeting embassies, international organisations and foreign ministries. Over a third of computer systems targeted contained sensitive information and were considered "high value".[124] GhostNet differed from previous attacks, as the hacks were not only designed to steal sensitive information. The infected computers gave the hackers continued access to the webcam and microphone effectively turning the infected network into live *bug*. Due to circumstantial evidence, the Toronto investigation stopped short of directly attributing GhostNet to China.[125]

The increased level of sophistication of GhostNet raised concern over the possible growing cyber capabilities of China and their perceived relentless hunt for information dominance. Originally believed to have occurred in 2009, though later revealed to have been breached as early as 2007, a series of National Security Agency (NSA) documents revealed that the plans for F-35 Lightning II joint strike fighter jet had been stolen by the Chinese.[126] The breach on defence contractor Lockheed Martin was extensive; it included the theft of over 50 terabytes of information (including F-22 data of

[120] Ibid.
[121] I. C. Smith & N. West, *Historical Dictionary of Chinese Intelligence*, Scarecrow Press, Toronto, 2012, p.101.
[122] Ibid.
[123] M. Moore, "China's Global Cyber-Espionage Network GhostNet Penetrates 103 Countries", *The Telegraph,* 29 March 2009, available from The Telegraph < http://www.telegraph.co.uk/news/worldnews/asia/china/5071124/Chinas-global-cyber-espionage-network-GhostNet-penetrates-103-countries.html> (accessed 20 June 2016).
[124] Ibid.
[125] Ibid.
[126] F-S. Gady, "New Snowden Documents Reveal Chinese Behind F-35 Hack", *The Diplomate*, 27 January 2015, available < http://thediplomat.com/2015/01/new-snowden-documents-reveal-chinese-behind-f-35-hack/> (accessed 24 February 2016).

an unspecified component to ease missile launch, and F-35 radar and engine schematics).[127] The F-35 is the US militaries most advanced fighter jet noted for its radar evading stealth technology.[128] It was designed to ensure US technological aviation supremacy for the next 20 years. A scaled model of the Shenyang J-31 Falcon Eagle revealed at the China International Aviation & Aerospace Exhibition in 2012 led US officials to believe that the stolen F-35 plans had been successfully reverse engineered.[129] The two jets have remarkably similar physical characteristics and the J-31 is a significant improvement on previous Chinese aviation technology.

Figure 1. **F-35 Lightning II top and the Shenyang J-31 Falcon Eagle bottom.[130]**

[127] B. Gertz, "China Hacked f-22, F-35 Stealth Jet Secrets", *The Washington Free Beacon*, 24 March 2016, available < http://freebeacon.com/national-security/china-hacked-f22-f35-jet-secrets/>, (accessed 28 June 2016).
[128] Ibid.
[129] AFP, "Latest China Military Hardware Displayed at Airshow", *Asia One News,* Singapore Press, 13 November 2012, available from < http://news.asiaone.com/News/AsiaOne%2BNews/Asia/Story/A1Story20121113-383169.html>, (accessed 28 June 2016).
[130] D. Majumdar, "America's F-35 Joint Strike Fighter vs. China's J-31, F-15SA and Russia's Su-35: Who Wins?", *The National Interest*, 20 September 2016, available from < http://nationalinterest.org/blog/the-buzz/americas-f-35-joint-strike-fighter-vs-chinas-j-31-f-15sa-17767>, (accessed 25 September 2016).

Table 4 Comparison of the F-35 and the J-31[131]		
	J-31 Falcon Eagle	**F-35 Lightning II**
Length	16.8 m	15.5m
Wingspan	11.5m	10.7m
Height	4.7m	4.2m
Take-off Weight (max.)	24947.6kg	31751.5kg
Weapons Load (max.)	7257.5kg	8164.7kg
Combat Radius	647nmi	690nmi

Despite exposing a serious security breach, the use of cyber espionage tactics to further military capabilities and access confidential information is by no means new to the US-Sino dynamic. However, of particular concern to the US were three cyber incidents all with high levels of attribution to the PRC. These incidents were particularly alarming and tested the boundaries of acceptable behaviour in cyberspace.

The first incidents occurred over a number of years (2006, 2011 and 2014) and were a series of reported cyberattacks against the US Chamber of Commerce conducted through Chinese servers.[132] The attacks were so severe that on several occasions the Chamber was forced to disable their email and internet access, which severely affected their ability to operate. [133] Former White House counter-terrorism adviser, Richard Clarke, spoke to ABC News in 2011 regarding the Chamber of Commerce cyber-attack illustrating the extent of the broader problem,

"The Chinese have attacked every major US company, every government agency, and NGO's. Their Attacking the Chamber of Commerce is part of a pattern of their attacking everything

[131] M. Weisgerber, "China's Copycat Jet Raise Questions About the F-35", *Defense One*, 23 September 2015, available from Defense One < http://www.defenseone.com/threats/2015/09/more-questions-f-35-after-new-specs-chinas-copycat/121859/>, (accessed 28 June 2016).
[132] E. Montalbano, "Virus Hits Part of U.S. Commerce", *Dark Reading,* Information Week IT Network, 3 March 2012, available from < http://www.darkreading.com/risk-management/virus-hits-part-of-us-commerce-dept/d/d-id/1102648>, (accessed 16 June 2016).
[133] Ibid.

in the US. If you're working on US-China Relations with an NGO, government agency, you can be sure the Chinese are reading your emails and on your computer".[134]

The second incident of note, Operation Aurora gained distinction because of the systems targeted as well as the use of multiple zero-day exploits (a vulnerability unknown to a software vendor exploited before the vendor becomes aware and attempts to fix it) exceeding previous cyber incidents (including Stuxnet).[135] In 2010, Google publically acknowledged that it had been hacked as part of Operation Aurora.[136] The incident was established to be a PLA backed cyber initiative perpetrated by cyber group's codenamed Sneaky Panda, the Elderwood Gang and the Beijing Group.[137] Operation Aurora targeted multiple organisations only a handful of which publically confirmed intrusions (suspected hacked organisations included Juniper Networks, Adobe Systems and Rackspace with suggestion of attacks against Yahoo, Symantec and Morgan Stanley).[138]

The third cyber incident was the prolonged attack against the Office of Personal Management (OPM). It revealed the most extensive theft of information in history. The OPM formally acknowledged that they had been the subject of an extensive data breach in 2015.[139] It was suspected that the attack resulted in the successful theft of around 22 million records.[140]

The extent of the attacks demonstrated two things; firstly, that the PRC was now broadly targeting institutions both governmental and corporate. The increased emphasis by the PLA on the importance on information dominance now clearly extends beyond high-level information targets. Secondly, that the PRC was pursuing information through cyber espionage for economic gains.

This was further emphasised by the release of the 2013 Mandiant APT1 Espionage Report which documented evidence of cyber attack's by the PLA, particularly by the Shanghai-based PLA Unit 61398. The report stipulated that the PLA had targeted over 141 organisations in the US as well as in

[134] P. Thomas, "Chinese Hack Into US Chamber of Commerce, Authorities Say", *ABC NEWS*, 21 December 2011, available from <http://abcnews.go.com/International/chinese-hack-us-chamber-commerce-authorities/story?id=15207642>, (accessed 16 June 2016).
[135] G. O'Gorman & G. McDonald, *The Elderwood Project*, Symantec Security Response, Mountain View, California, 2012, pp.1-13.
[136] K, Zetter, "Google Hack Attack was Ultra Sophisticated, New Details Show", *Wired Magazine*, 14 January 2010, available from <https://www.wired.com/2010/01/operation-aurora/>, (accessed 25 July 2016).
[137] O'Gorman et al. 2012.
[138] Ibid.
[139] B. I. Kderner, "Inside the Cyberattack That Shocked the US Government", *Wired Magazine*, International Frontiers, Security, 23 October 2016, available from Wired <https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/>, (accessed 16 June 2016).
[140] Ibid.

other English-speaking nations since 2006.[141] The report eventually lead to accusations made against five Chinese military officials accused of hacking US systems.

US Rhode Island Senator, Sheldon Whitehouse noted the risk of the intrusion, "*You stack all of that up and I think there's a case to be made that this may be the greatest transfer of wealth through theft and piracy in the history of the world and we are on the losing end.*"[142]

The following table briefly categorizes the cyber interactions of the majority of incidents put forward in this section.

Table 5 A Brief Look at the Cyber-Physical Interaction of the US and China

Cyber – Cyber (US perspective)	**Cyber – Physical**
○ Titan Rain 2003 ○ State Department 2006 ○ Lockheed Martin F-35, 2007 ○ Chamber of Commerce 2006, 2006 & 2011 ○ Operation Aurora 2010 ○ OPM Intrusion 2014 (acknowledged 2015)	Although there have been speculated cyber incidents between China and the US, that have resulted in kinetic damage there is no evidence to corroborate such claims.
Physical – Physical	**Physical – Cyber**
Both China and the US have undertaking intensive recruitment schemes to bolster cyber offensive capabilities and progress cyber defence posturing. - US programs such as *Hack the Pentagon* are designed to both test the strength of US systems as well as create a convenient recruitment platform.	○ US speculated physical hack into Huawei hardware targeting networking gear.[143]

[141] Mandiant Report, 2013.
[142] Thomas, 2011.
[143] C. Metz, "US to China: We Hacked Your Internet Gear We Told You Not to Hack", *Wired Magazine,* 31 December 2013, available from < https://www.wired.com/2013/12/nsa-cisco-huawei-china/>, (accessed on 3 March 2016).

Table 6 indicates the damage of cyber incidents put forward in this chapter of the US and China.

Table 6 Scale of US-Sino Cyber known Incidents

Severity	Explanation	Examples
Category 1	Minimal damage	State Department website down.
Category 2	Targeted attack on critical infrastructure or military	○ Titan Rain 2003 ○ State Department 2006 ○ Lockheed Martin F-35, 2007 ○ Chamber of Commerce 2006, 2006 & 2011 ○ Operation Aurora 2010 ○ OPM Intrusion 2014
Category 3	Dramatic effect on nation-states specific strategy	Stuxnet.
Category 4	Dramatic effect on a nation-state	No open source evidence of attacks of this scale and beyond.
Category 5	Escalated dramatic effect on a nation-state	

When examining Table 6 certain trends become evident. The first category of cyber incident tends to fall below a threshold of usefulness for nation-states. Cyber incidents of this nature act more as a nuisance than as a tool to improve state power. The vast majority of attacks take place in category 2. This indicates two possibilities: firstly, cyber incidents in this category are relatively easy to commit and secondly, that the nature of attacks in this category could indicate political interest. It suggests that at present it is not in the interest of either the US or China to initiate a more serious cyber-attack against one another. It also suggests that China places increased importance on information dominance.

With regard to category 3 the US employment of the Stuxent Worm is the only clearly attributable cyber incident at this level by either the US or China. However, as the cyber incident occurred in 2010 it is highly likely that China would have acquired the capability through diffusion. The diffusion of cyber threats will be further discussed later in this chapter. Finally, concerning categories 4 and 5 one thing remains clear. There is a significant lack of information pertaining to cyber incidents at the higher levels. Although there is a great deal of speculation suggesting that both the US and China

possess such capabilities there is little evidence to support this claim. Authors such as Libicki broadly discuss the possibility of cyber warfare without specifically stipulating the existence of such capabilities. Other scholar such as Rid famously exploit this lack of information stating that as there is little evidence the capability most likely does not exist. However, given the weaknesses present in certain computer systems (although disputed the vulnerability of SCADA controls is often referenced) it is highly likely that a severe cyber or kinetic attack would be possible for both the US or China. Nevertheless, the discussion on cyber capabilities raises the question of whether or not the proof of such capabilities would be necessary for deterrence to function in cyberspace.

The Pursuit of Agreement

In 2014 formal negotiations to resolve issues of nation-state behaviour in cyber space were broken off. The negotiations were halted due to the indictment by the US government of five members of the Chinese military accused of hacking a number of US companies.[144] The indictments including prominent hacker Wang Dong (also known as Ugly Gorilla) who was outed in the 2013 Mandiant Report.[145] The withdrawal of China was significant and demonstrated a pattern of growing tensions between the two leading powers. The guilty plea in March 2016 of Chinese businessman Su Bin, (also known as Stephen Su) to conspiracy to hack US defence contractor computer networks over the stolen F-35 plans along with other classified information have also contributed to the souring of the political relationship.[146]

The following September during President Xi Jinping's visit to the White House the issue of US-Sino cyber relations was revisited resulting in official talks held in June 2016.[147] Although the talks eventually led to an agreement, it was speculated that the recommencement of talks was a bid by China to avoid the prospect of sanctions.[148] A concerted effort made in recent years by the US to repair relations with China regarding cyber activities reflect the severity of the issue from the US

[144] B. Blanchard, "U.S. Sees Progress in Latest Cyber Talks with China, *Rueters*, Business Day, 14 June 2016, available from Reuters < http://www.reuters.com/article/us-china-usa-cyber-idUSKCN0Z00DN> (accessed 15 June 2016).
[145] Mandiant Report, 2013.
[146] Gertz, 2016.
[147] G. Shih, "China, U.S. Hold Talks to Bridge Cybersecurity Differences", *The Bid Story,* 14 June 2016, available from <http://bigstory.ap.org/article/a493922899424ecf988f5a917cd63458/china-us-meet-cybersecurity-talks-beijing> (accessed 15 June 2016).
[148] S. W. Harold, M. C. Libicki & A. S. Cevallos., "Getting to Yes with China in Cyberspace", Santa Monica, C.A.: RAND Corporation, 2016, p.x.

perspective and illustrate their desire to tackle concerns of state sponsored activities conducted in the cyber domain.[149] It should also be noted that decision makers are apprehensive at the merging of military and espionage cyber functions. Recent endeavours by both parties to maintain open dialogue reflect the desire to prevent the militarisation of cyberspace and parallels similar debates regarding space.

The US-Sino relationship within the cyber domain is dominated by a fundamental disagreement over universal norms and procedures; despite publications made by organisations such as the UN and the development of the concept of norms internationally. It is this difference in perception that has led to many of the disagreements between the two superpowers in recent years. Progress in the area has been further hindered by events outside the cyber domain such as: US trade sanctions against Chinese seamless steel tubes, the public criticism by former US Secretary of State, Hillary Clinton on Chinese internet censorship and a meeting between President Barack Obama and the Dalai Lama.[150] Not to mention US policy in the South China Sea and the 2012 Pivot. However, progressed has also been slowed by the continuation of cyber contests, such as cyberattacks and cyber espionage, perpetrated by both nation-states.

The disagreement over what constitutes applicable norms and procedures in cyberspace is significant and multifaceted. Although China's behaviour within the domain plays a considerable role in shaping the relationship from the US perspective, the same cannot be said for China. China is less concerned with US behaviour in cyberspace and sees it as a modest factor in their relationship.[151] These divergent perspectives affect the prioritization of grievances by both China and the US and hinder the progression of more effective methods for managing the relationship.

For the US there are significant issues regarding China and state sponsored behaviour in cyberspace. There is growing concern at the prospect of China's preparedness to launch a cyber-attack targeting

[149] Blanchard, 2016.
[150] X. Yan, "The Instability of China- US Relations", *The Chinese Journal of International Politics*, Oxford University, Vol. 3, No. 3, 13 August 2010, pp.263-292.
[151] S. W. Harold et al., 2016, p. viii.

US critical infrastructure.[152] In addition, the theft of intellectual property and proprietary business of corporate networks by Chinese cyber intrusions are a problem. As is the continued compromise of US government information for traditional espionage purposes (such as the 2015 cyber intrusion against the OPM).

In 2013 U.S. National Security Advisor, Tom Donilon stated *"…not solely a national security concern or a concern of the US government"* but also a serious problem for companies dealing with *"sophisticated, targeted theft of confidential business information and proprietary technologies…emanating from China on an unprecedented scale."*[153] Since then, China has

continued to conduct cyber intrusions with experts stating in the 9 June 2016 Congressional Commission that Chinese cyberattacks were at an all-time high.[154]

Figure 2. **NSA map of over 700 successful intrusions against US private of government entities over a five-year period emanating from China.[155]**

[152] Ibid.
[153] T. Donilon, "The United States and the Asia-Pacific in 2013", *Asia Society*, Washington, D.C.: White House, March 2013.
[154] Co-Chairs Commissioner P. Brookes & Senator B. Dorgan, "Hearing on Chinese Intelligence Services and Espionage Operations", *U.S.-China Economic and Security Review Commission*, Washington, D.C.: 9 June 2016, available from < http://www.uscc.gov/Hearings/hearing-chinese-intelligence-services-and-espionage-operations> (accessed 16 June 2016).

On the other hand, China's adopted 15-year strategy (2006-2020) to priorities the 'informatisation' of Chinese public services attempts so secure its national security through cyber means.[156] It could also be argued, that much of the Chinese thinking parallels US concepts of fighting and defending against attacks on computer networks. Though given the previous statement it is clear to see the difficulty in disentangling China's approaches to the cyber domain from the perceived national security threat caused by what the regime views as unchecked access to information from its population. Their concerns also relate to events taking place outside the domain than within it and primarily revolve around US restrictions, control and perceived interfering behaviour. From China's perspective, their grievances centre on three issues. Firstly, the restriction placed on market access for Chinese telecommunication companies, such as Huawei, are frustrating.[157] Secondly, China desires full control of accessible information by individuals within its borders. This endeavour is currently hampered by US financing of censorship-circumventing technology, which China sees as a trespass on its *cyber-sovereignty*. Finally, China takes issue with what they perceive is US hegemony within cyberspace. Much of the hardware and software supporting access and use to the internet in China is controlled by US companies.

Despite there being a disproportionate criticism of China's behaviour in cyberspace both the US and China have contributed to the current state of affairs. Information from the Chinese perspective is problematic, as an authoritarian state with rigorous legislation protecting state interests the revelation of intrusions perpetrated against them are difficult to come by. Furthermore, the secrecy surrounding Chinese cyber intrusion programs and capabilities are also closely guarded, as are those of the US government. Unless a cyber-intrusion is revealed by either the challenger, defender or a third party, information pertaining to cyber-attacks is rare.

---

[155] J. Murdock, "Shadow Warfare: The Cyber Relationship Between China and the US at 'Breaking Point'", V3, London, 25 August 2015, available from < http://www.v3.co.uk/v3-uk/feature/2423655/shadow-warfare-the-cyber-relationship-between-china-and-the-us-at-breaking-point>, (accessed 24 May 2016).

[156] T. Feakin, "Enter the Cyber Dragon – Understanding Chinese Intelligence Agencies' Cyber Capabilities", *Australian Strategic Policy Institute*, June 2013, Issue 50, accessed 2 March 2017, available from <https://www.aspi.org.au/publications/special-report-enter-the-cyber-dragon-understanding-chinese-intelligence-agencies-cyber-capabilities/10_42_31_AM_SR50_chinese_cyber.pdf>

[157] P. Brookes et al. 2016.

The Issue of Cyber Deterrence

The attractive utility of the cyber domain for malicious purposes is unparalleled. The speed at which scalability of threat can be achieved and the addition of offence advantage make cyber the perfect forum to reconcile the disparity in hard power distribution amongst states.[158] The F-35 was designed to give the US and its allies a leading edge in air power for the next two decades. However, the theft of the plans raises legitimate concerns over the viable maintenance of technological supremacy in an environment that caters to information theft. The necessary features for deterrence to operate: capability to retaliate and will to do so, and the ability to impose unacceptable costs along with a clear communication of a threat, are hampered by the attractive utility of cyberspace to gain political advantage.

The issue of asymmetry in cyberspace adds to its appeal. Unlike kinetic incidents, the effectiveness of cyber incidents is not dependant on resources, manpower or education. A country has the potential to impose significant damage through cyberspace irrespective of its other capabilities (such economic or military might). Buchanan (previously covered in the literature review) discussed the tendency of malicious cyber incidents to be based on previously developed code.[159] The cyber domain is an environment where behaviour and tactics are learned and continuously built on. In his article on cyber threat cycles, Buchanan used the example of the Heartbleed exploit attack on the Canadian Revenue Agency in 2014.[160] Originally thought to be the work of nation-state it was soon discovered that the attack was perpetrated by a teenage engineering student from London.[161] Although, nation-states do have superior cyber capabilities, are able to recruit widely and have resources; including time, testing grounds and superior technology compared to non-state actors. The progression of tactics in the cyber domain raises significant issues. The evolution of behaviour and tactics in the cyber domain, with regard to scalability and attribution are critical components in the discussion on the applicability of deterrence to cyberspace.

[158] Lieberthal et al. 2012.
[159] Buchanan, 2016.
[160] Ibid.
[161] J. Sims, "'Heartbleed' Canada Revenue Hacker Gets a Break", *Toronto Sun*, 20 July 2016, available < http://www.torontosun.com/2016/07/20/heartbleed-canada-revenue-agency-hacker-gets-a-break>, (accessed 31 July 2016).

Despite the advancement of cyber capabilities and a growing understanding of the domain, clear attribution of incidents is still difficult. The primary concern relating to state sponsored cyberattacks emanating from China is not necessarily their sophistication (especially in comparison to the cyber capabilities of both the US and Russia) but the sheer volume of incidents. Given the lack of Chinese network security, it is plausible that countries such as Russia (which have considerable cyber capabilities[162]) are using the Sino network as a false flag platform; although there is little research to corroborate this assertion.

Over the last decade, the US has improved its ability to clearly attribute cyber incidents. The indictment of the five Chinese military officials over state sponsored cyber incidents as well as the guilty plea from Chinese businessman, Su Bin, is an indication of the US' ability to attribute.

However, despite these advancements in attribution there is another problem with clear cost evaluation. If a cyber-incident remains within the interactions of cyber-cyber, it is difficult to gain a clear understanding of damage. For instance, the ability to evaluate the harm of cyber espionage is incredibly difficult. There is no tangible method of measuring future damage incurred by information stolen in the present. In addition, as cyber incidents are often difficult to detect a target may not be aware that damage is being done or after an incident is discovered how long the intrusion went unnoticed. The OPM intrusion was suspected to have first penetrated the system a year before discovery. If a defender cannot clearly evaluate the damage or worst still is unaware of the damage being done, then how are they able to action a proportional retaliatory strike?

When addressing the issue of proportional response, several problems crop up. Firstly, retaliation in cyberspace may not be so simple. A defender must decide on the method and the relative scale as well as have the capability to do so. Given that nation-states are constantly testing their own systems for weaknesses and correcting those weaknesses, both challenger and defender are not able to amass exploits as they would kinetic weapons. As such, the US may need time to develop and exploit

[162] R. F. Johnson, "Experts: The US has Fallen Dangerously Behind Russia in Cyber Warfare Capabilities", *The Washington Free Beacon*, 27 July 2016 available < http://www.businessinsider.com/us-behind-russia-cyber-warfare-2016-7?IR=T>, (accessed 31 July 2016).

vulnerability after a Chinese cyber incident has occurred. This would greatly increase the retaliatory time.

Secondly, there are significant dangers to both the defender and the cyber environment as a whole in exploiting vulnerabilities. Buchanan discussed the diffusion of cyber threats and how the cyber environment evolves.[163] The control often afforded to kinetic weapons does not apply to cyber weapons. Once a technique or exploit is used, it has the ability to diffuse to other actors (both state and non-state) and potentially be used against the country that originally employed it.[164] The choice to employ a specific technique by the US could diffuse and be used against it by China later. The 2010 Stuxnet cyber weapon was one of the most sophisticated cyber worms designed. Making use of a previously unprecedented four zero-day exploits, it targeted specific SCADA systems (industrial controls).[165] That said, the original implementation of the worm was difficult and required it to be physically injected into the targeted system. It was also limited as a one shot weapon given its usage of zero days. However, since its employment the Stuxnet malware has continued to evolve and is now being used by cyber criminals.[166]

The correlation between nuclear and cyber with regard to deterrence has been raise several times. However, the cyber incidents evident in the US-Sino case study tend to contradict the usefulness of the nuclear analogy to cyber deterrence. As previously stated in the literature review there are far more actors in cyberspace than are members of the *nuclear club*. In addition, there is a greater distinction in scale of incident. The employment by capable states of even a modest nuclear weapon would still do severe damage and would likely result in retaliation and possibly escalation. Lastly, the attractive utility of nuclear weapons is dwarfed by the possible advantages that could be gained through the malicious utility of cyber techniques and technologies.

[163] Buchanan, 2016.
[164] Ibid.
[165] P. Mueller & B. Yadegari, *The Stuxnet Worm*, University of Arizona, Department of Computer Science, 2012, available < http://www.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf>, (accessed 20 January 2016).
[166] T. Simonite, "Stuxnet Tricks Copied by Computer Criminals", *MIT Technology Review*, 19 September 2012, available < https://www.technologyreview.com/s/429173/stuxnet-tricks-copied-by-computer-criminals/>, (accessed 20 January 2016).

The final aspect adding to the complexity of applying deterrent measures to US-Sino cyber relations is clear threat communication. In his work, Jervis outlined the problems of signal interpretation and the risk of misunderstandings.[167] The US and China have distinctly different cultures and different interpretations of acceptable cyber behaviour. This chapter has outlined the differences between the two in their approach to cyber and its utility. The ability to communicate a clear threat as part of a deterrence posture by the US could be hindered by this gap in perspectives.

Chapter Summary

From the US perspective, China's continued efforts to gain unlawful access to US defence and corporate information is affecting the stability of their political relationship. On the other hand, the US pivot, its involvement in regional politics and the distribution by the US of censorship circumventing technology is a constant irritant for China. The Chinese lack of distinction between perceived national security threats (public access to information) and cyber behaviour indicates the rational and boundaries established by the regime to govern the domain domestically. The success of state sponsored cyber incidents by China against the US has also demonstrated a significant deficit in US cyber security.

The volume of category 2 cyber incidents in US-Sino relations suggests that information dominance is of increasing importance to China. This assertion in addition to the attractive qualities cyber offers for malicious purposes make it unlikely that an agreement on norms and deterrent mechanisms would hold. Given the difference of perspectives it is possible that either the US or China may unwittingly cross a threshold of acceptable cost increasing the probability of cyber escalation.

The information presented in this chapter raised three key questions regarding the applicability of cyber deterrence to US-Sino cyber relations. Firstly, that given the attractiveness of using cyber for malicious purposes how can China's behaviour be controlled. Secondly, how could deterrent mechanisms mitigate the risk of accidental breaches of the threshold of acceptability? Finally, despite political interest possibly influencing the prevalence of category 2 cyber incidents it is still highly likely that both the US and China are pursuing cyber capabilities with the potential to inflict more severe damage. As states

[167] Jervis, 1979.

have historically tested capabilities and as it is difficult to test cyber capabilities offline what is preventing the usage of category 4 and 5 cyber incidents?

CHAPTER 5

A FUNCTIONING CYBER DETERRENCE

Chapter Introduction

The relationship between the US and China is complicated with a great deal of discussion centring on its future and the possibility of conflict. However, considering the in-depth nature of US-Sino cyber interaction it becomes apparent that the debate on cyber deterrence is multifaceted. There is a clear distinction between different levels of cyber interaction. These levels tend to be grouped by the sophistication of the cyber incident and the scale of damage incurred. US-Sino cyber interaction at certain levels tends to be influenced by the political interest of the US and China, as well as an evaluation of cost. The prevalence of less damaging cyber incidents suggests that China has calculated the risk of retaliation as minimal against the significant political and economic gains to be made. Whilst a lack of more damaging incidents suggests that attacks beyond a certain magnitude are not in the interests of either the US or China. This assertion could also insinuate that a deterrence posture is successfully functioning beyond a specific threshold of damage.

This chapter will outline the importance of deterrent norms and mechanisms despite their limited utility to prevent category 1 and 2 cyber incidents. It will then discuss the danger of accidental escalation through the strategic employment of category 3 cyber incidents before outlining problems of accurately determining deterrence efficacy. The chapter will then address the likelihood of a functioning deterrent posture, influenced by political interest, for category 4 to 5 cyber incidents. In doing so it will highlight the danger of accidental escalation drawing on Jervis' concept of signalling and misunderstanding.[168] Finally, this chapter will address key issues in the current body of literature including a lack of understanding of the integration between the cyber and physical realm.

---

[168] Jervis, 1979.

Deterrent Norms and Mechanisms

Several pertinent questions were raised in the conclusion of the previous chapter. The issues discussed outline the significant gains to be made utilizing the cyber domain for malicious purposes. It also highlighted the resultant difficulty in realistically curbing its usage through the implementation of deterrent norms. This thesis has set forth many prominent views from scholars advocating for the utility of norms. However, there remains a need to critically address the technical advantage offered by cyberspace. If China's malicious cyber behaviour is to be stemmed, more clearly defined norms and mechanisms would need to be established.

The abundance of categories 1 to 2 cyber incidents is affected by a multitude of factors such as difficulties in attribution, scalability and cost evaluation. All of which hinder the applicability of deterrent norms. A culmination of political interest and advantage offered by the malicious usage of cyber tactics has affected the stability of US-Sino relations. Competition for regional influence as well as military and economic contests have also contributed to the current climate. As discussed in previous chapters, the cyber domain cannot be considered as separate from other domains of state interest. There is an intrinsic link between the cyber and the physical realm, which must be taken into consideration when addressing the politically motivated actions, which affect its stability.

Cyber specialist James Lewis has previously stated that the differences between the US and China have real military consequences and should not be considered as solely political.[169] As the potential for conflict is real, the approach to deterrence posturing at the lower levels needs to be far more informed. There needs to be a clear understanding of the limitations of the utility of norms as well as other factors influencing the stability of the relationship. Lewis went on to highlight the importance of consistent, long-term engagement for the US and China.[170] He emphasized the Cold War analogy and

[169] J. Oh, "Cyber Cooperation in Northeast Asia: An Interview with James Lewis", *National Bureau of Asian Research*, Policy Q&A, March 17, 2015.
[170] Ibid.

the difference in level of understanding achieved between the US and the Soviet Union before the end of the Cold War.[171]

As previously stated there are many weaknesses in adopting the nuclear analogy when discussing cyber deterrence, however, the progression of US-Soviet relations offers important lessons for the current situation between the US and China and their cyber interaction. Prolonged effort and continued negotiation enabled the US and the Soviet Union to attain an in-depth level of understanding of culture and political interest. Although there were, other factors, which helped, encourage the development of the relationship. In the *Anatomy of Mistrust*, by Deborah Welch Larson, she notes that strategic equality between the two nuclear powers helped efforts in trust building.[172] This equality does not exist between the US and China which has in part contributed to China's continued behaviour.

The 2016 RAND publication on cyber norms aptly outlined the problems in reaching a US-Sino cyber agreement.[173] It highlighted the key differences in political interest and motivations. Touching on Amy Chang's article *Warring State: China's Cybersecurity Strategy*,[174] the RAND publication stated there is currently little incentive for China to curb its behaviour; particularly regarding information theft.[175] Despite these issues, observations made by Lewis regarding engagement and understanding are pertinent to the discussion on deterrent norms in cyberspace.

The first question raised at the end of the previous chapter centres on two considerations. The question discussed the attractiveness of cyberspace and the realistic prospects of curbing China's behaviour within the domain. Essentially the need to mitigate the risk of escalation revolves around two prospects; the accidental breach of a defender's threshold of acceptability, through either damage incurred or volume of incidents from a challenger. Both of which have the possibility of resulting in escalation and an unintended conflict.

---

[171] Ibid.
[172] D. W. Larson, *Anatomy of Mistrust: U.S.-Soviet Relations During the Cold War*, Ithaca and London, Cornell University Press, 2000, pp.26.
[173] RAND, 2016.
[174] A, Chang, *Warring State: China's Cybersecurity Strategy,* Washingtong, D.C.: Center for a New American Security, December 2015, pp. 7, 10. Available < https://s3.amazonaws.com/files.cnas.org/documents/CNAS_WarringState_Chang_report_010615.pdf> (accessed on August 24, 2016).
[175] RAND, 2016.

In addressing the issue of cyber deterrence this thesis has discussed the advancements of cyber attribution as a key component. Although significant gains have been made by the US, China's capabilities are arguably not as strong. The difficulty in accurate attribution in cyberspace remains an obstacle. It raises concerns of nation-states possibly lowering the standards of attribution in a more forceful attempt to ensure the success of a deterrence posture. Which in turn could increase the risk posed by cyber incidents. This assertion challenges Libicki's statement that attribution may be unnecessary given clear signalling of retaliation by a defender.

Conversely, despite a challenger state (in this case China) calculating the incurred cost and likelihood of retaliation as minimal, an increased number of categories 1 and 2 cyber incidents may inadvertently cross the threshold of acceptability for the US. Especially if attacks appear to target the financial sector as opposed to government industry. As is evident from the case study in chapter 4, the sophistication in level of intrusion and sheer number of cyber incidents perpetrated against US companies and the financial sector has been a considerable irritant affecting the stability of US-Sino relations. Yet there appears to be little consideration given to the threat of conflict. This in turn may have specific implications for the construction of a functioning deterrence poster within the relationship. The superiority of organisations such as the NSA may have contributed to past acceptances of intrusions (earlier touched on in Chapter 2).

There is also a heightened risk of accidental breach by a miscalculation of cost through the utility of a more damaging cyber incident to achieve a political goal. The 2010 Stuxnet worm which was classified as a category 3 incident by damage caused,[176] was used to set back the Iranian nuclear program.[177] Although there were consequences for the incident, they were arguably mild in both damage and complexity given the immense amount of resources and trial and error dedicated to creating the worm.[178] This would most likely not be the case if such an incident were to occur between the US and China. Given the succinct global nature of the cyber domain, an impairment caused by two nations with significant capacity could seriously affect global security as well as

[176] Valeriano, et al. 2015.
[177] Langer, 2011.
[178] T. Gjelten, "First Strike: US Cyber Warriors Seize the Offensive", *World Affairs*, January – February 2013, Vol. 175 Issue 5, pp.33-43.

economic security. There is a danger that China's political interest and its understanding of US political interest may inadvertently affect its ability to accurately calculate the likelihood of a retaliatory strike in response to the employment of a cyber-tactic. The assumption that neither China nor the US desires a cyber-arms race or indeed conflict does not guarantee the absence of one. This correlates with Jervis' emphasis on signal misunderstanding and it becomes apparent that effective deterrence must encompass a plainly communicated threat clarifying the threshold of acceptability.

This section has established the significant limitations regarding the efficacy of deterrent norms and mechanisms within the cyber domain. However, notwithstanding these limitations there are substantial benefits for US-Sino relations through the establishment of norms. The pursuit of a cyber-agreement between the US and China has helped foster a more in-depth level of understanding regarding key disagreements. Continued and open lines of communication plays a crucial role in mitigating the risk of accidental escalation by either damage sustained or number of incidents of categories 1 to 3 cyber acts. Which correlates more closely with liberalism than neo-realism and ties in the Nye's remarks on the necessity of improving communication.

The Assumption of Capabilities

In recent years both the US and China have increased their funding for the development of cyber defence systems.[179] The proliferation of low level cyber incidents as well as growing public discussion on the potential threat of severely damaging cyberattacks have contributed to this development. Given this increase in funding, there is a high probability of both the US and China possessing cyber capabilities with the potential to inflict severe harm, particularly when considering the pursuit of policies such as the Chinese *'informatisation'*.[180] The employment of such capabilities would undoubtedly result in categories 4 to 5 cyber incidents. However, as addressed in the previous chapter, there is insufficient proof despite the likelihood of the existence of such capabilities. However, proof may not be necessary for cyber deterrence to function successfully.

[179] S. Lyngaas, "Pentagon Fret's Over China's Cyber Capabilities", *FCW The Business of Federal Technology*, 8 May 2015, available from < https://fcw.com/articles/2015/05/08/china-cyber-report.aspx>, (accessed on 25 August 2016).
[180] ASPI, 2013.

Although deterrence theory tends to stipulate the necessity of a defender's possession of the capability to retaliate and the will to do so, the conclusions offered by both Lebow and Stien, and Huth and Russet highlight the importance of the psychological component of deterrence.[181] The relationship between the defender and the challenger plays a key role in the success of deterrence. Challenger motivation was also found to contribute to deterrence working. However, hypothetically, if a challenger was convinced that a defender possessed the capability to inflict considerable harm in retaliation for an attack they may be dissuaded despite their respective motivation. The behaviour of a nation-state, acting in accordance with its political interests, may be curtailed by the belief of a defender's possession of sizeable capabilities. Thus, a challenger may be compelled by a belief of capabilities into becoming a risk-averse loss minimiser as opposed to a risk-prone gain maximiser.

In recent years, there have been significant policy developments linking Sino-US promises to promote global cyber security. For instance, as previously mentioned the September 2015 meeting between President's Obama and Xi illustrated a desire to resolve the apparent conflict. Earlier in 2009, President Obama initiated an interagency cyber security review.[182] However, the assumption that both the US and China desire to avoid escalation and conflict because of their political interest could be misjudged. It is possible that China's lack of employment of cyber tactics resulting in categories 4 to 5 incidents in severity is due to their belief of unacceptable harm in retaliation. The logic of this conclusion is reasonable given the proven capabilities of US military power in other domains. In addition, though not as probable the same assumption could be made in reverse.

Although highly speculative, this line of questioning further illustrates the difficulty in determining the efficacy of deterrence. Scholars discussing the applicability of deterrence to cyberspace are limited due to the inherent difficulties in proving the success of a deterrence poster. The ambiguous nature of the psychological component of deterrence means that its effectiveness can never accurately be determined. Despite a challenger appearing to be dissuaded from an action by a threat made by a defender, it is

[181] Morgan, 2010.
[182] F. H. Cate, "Comments to the White House 60-Day Cybersecurity Review", *Center for Applied Cybersecurity Research*, 27 March 2009, accessed 5 March 2017, available from < https://obamawhitehouse.archives.gov/files/documents/cyber/Center%20for%20Applied%20Cybersecurity%20Research%20-%20Cybersecurity%20Comments.Cate.pdf>

virtually impossible to attain conclusive proof of the motivation behind the dissuasion. For this reason, it is important to consider the assumption of cyber weapons capabilities in the discussion on cyber deterrence and its functionality.

Broad Spectrum Deterrence

The cycle of interaction between the physical and cyber realms is fundamental. Cyberspace is not a separate entity. It is a platform for conducting an array of business with increased speed and convenience. Many variables can influence cyberspace. The interplay of different types of interaction laid down by Jarno Limnéll (i.e. cyber-cyber, cyber-physical…etc.) demonstrate it's ture nature. Yet the discussion around the applicability of deterrence to cyberspace often fails to incorporate this concept. Cyber deterrence is not cyber in its implementation and nor should it be.

Consider the key components for deterrence, threat communication, ability to retaliate and will to do so. Threat communication is rarely conducted solely in cyberspace. The rhetoric from a defender tends to cover broad mediums inlcuding policy and diplomatic back channels. Yet when discussing retaliation, scholars often fixate on proportional response as cyber equalling to cyber (ie. A cyber attack equals a cyber retaliation). Thomas Schelling's 1966 work *Arms and Influence*, outlines the concept of proportionality as being linked to objectives and scope of retaliation.[183] He states:

"There is an idiom in this interaction, a tendency to keep things in the same currency, to respond in the same language, to make the punishment fit the character of the crime… It helps an opponent in understanding one's motive, and provides him a basis for judging what to expect as the consequences of his own actions . . . the direct connection between action and response helps to eliminate the possibility of sheer coincidence and makes one appear the consequence of the other."[184]

However, there is a danger in assuming Schelling's notion of character was referring to domain. Proportionality is about objective. With this is mind, it is important to consider the target of the

[183] T. C. Schelling, *Arms and Influence,* New Haven, Yale University Press, 1966, 146–149.
[184] Ibid.

malicious incident. For instance, was the objective to steal state secrets (as was the case with the theft of the F-35) or damage a competitor's capability (such as Stuxnet)? Schelling was referring to the level of damage incurred not the method of incident.

The issue of proportional retaliation in cyberspace is an ongoing problem. The difficulty in assessing damage incurred influences the understanding of true cost and thus response. Regarding the less damaging levels of cyber incidents (usually encompassing information theft), it is easy to see how the attractive utility of cyberspace may influence the perception of its use in retaliation. When examining some of the literature on cyber deterrence it becomes apparent that its utility as a conduit for retaliation is believed to provide proportionality as well as speed and convenience. However, as previous addressed, cyber exploits take time to develop and as Buchannan aptly stated, retaliation in cyberspace has limited controls.[185] Considering the likely dissemination of cyber threats, a defender's usage of a malicious code in response to a challenger's actions could be used against it later. This in turn risks adversely affecting the stability of the cyber environment.

Considering these elements, it becomes apparent that cyber deterrence cannot and should not be conducted solely in cyberspace. The efficacy of deterrence in dissuading the utility of cyber incidents is not dependent on the affected domain. As advanced by Libicki and others, broad-spectrum deterrence is safer, practical and more likely to contribute to the success of deterrence in cyberspace.[186] It is also less ambiguous in threat communication and provides a more clearly defined retaliatory path.

Functioning Deterrence

It is probable that deterrence may be functioning at the more severe levels of cyber interaction between the US and China. The likelihood of both the US and China possessing considerable cyber capabilities contributes to this possibility. Even if China does not possess the ability to conduct a

[185] Buchanan, 2016.
[186] Libicki, 2009.

damaging cyber-attack there are other avenues for conducting conflict. As most of China's hard power military capabilities are well known, it could initiate a kinetic attack targeting US cyber infrastructure.[187] The theoretical foundations adopted for this thesis, used to help explain state behaviour, suggest that it is in China's interest to lessen the threat posed by the US. This does not suggest that China desires to surpass the US only that both neo-realism and balance of power theory would encourage this behaviour. Yet the absence of severe conflict suggests that a form of deterrence is functioning and that it most likely correlates with US-Sino political interests.

The assertion made in the 2012 Brookings publication on cyber security may also be contributing to the prevention of severe conflict. [188] It described how *spill over* of incidents in cyberspace was affecting the stability of relations.[189] The proliferation of low-level incidents correlates with China's political interest including cost evaluation. However, the absence of severe cyber incidents suggests that the evaluation of costs incurred in retaliation would be too devastating to undertake. The possibility of a cyber-incident spilling over into other domains due to level of damage sustained is highly probable. Given the considerable arsenal of the US, this spill over would act as a deterrent to any rational adversary.

Regarding political interest, Joseph Nye's 2016 publication stresses the issue of entanglement.[190] A situation whereby a challenger cannot detrimentally harm a defender as it would inevitably cause harm to itself. He states that despite political desire to lessen the threat posed to China by US military might, the integration of state-affairs and reliance on one another, deters the usage of malicious cyber tactics.[191]

The table below puts forward different levels of deterrence.

[187] J. T. Dreyer, "China's Power and Will: The PRC's Military Strength and Grand Strategy", *Orbis*, 2007, Vol. 51, Issue 4, pp. 651-664.
[188] K. Lieberthal et al. Brookings, 2012.
[189] Ibid.
[190] J. Nye, "Can China be Deterred in Cyber Space", *The Diplomat*, 3 February 2016, available from < http://thediplomat.com/2016/02/can-china-be-deterred-in-cyber-space/> (accessed 5 June 2016).
[191] Ibid.

Table 7 Scale of Incident vs Deterrence Posture

Severity	Explanation	Deterrence Posture
Category 1	Minimal damage	Realistically the utility of deterrence at this level of interaction is narrow.
Category 2	Targeted attack on critical infrastructure or military	Although limited in effectiveness, the pursuit of **norms** helps to mitigate the risk of escalation and clarify political interest.
Category 3	Dramatic effect on nation-states specific strategy	States should be mindful of conducting category 3 incidents to achive political goals as the risk of escalation is hightened. Again the importance of open dialogue is evident.
Category 4	Dramatic effect on a nation-state	Broad spectrum deterrence is necessary to disuade severe attacks.
Category 5	Escalated dramatic effect on a nation-state	Deterrence at these levels tends to corelate with both US and Chinese political inerest.

It displays the likelihood of the success of deterrence at distinct levels of severity. Regarding US-Sino relations, deterrence can function in cyberspace. However, it is far more likely to succeed when the cost of a challenger's actions is calculated to be severe.

Chapter Summary

This chapter has attempted to address the questions laid out in the conclusion of the case study. It has set forth a series of statements addressing the applicability of deterrence to US-Sino cyber relations. In highlighting the limited utility of deterrent norms, it has also advocated for their continued development. The importance of sustained communication and the pursuit of endeavours such as the 2016 US-Sino cyber agreement, in preventing accidental escalation and conflict is paramount. To better, mitigate Jervis' risk of misperception both China and the US should pay careful attention to how they are viewed by one another. This correlates with both the Brookings (2012) and RAND (2016) publications, which stipulate the need to overcome cultural barriers and attain a more

in-depth level of understanding. Despite endeavours to bridge the gap (i.e. 2015 meeting between President Obama and President Xi) these cyber 'cultural barriers' still exist.

Although there are many different forms of deterrence (via denial or punishment…etc.) realistically the success or failure of the strategy revolves around the severity of the incident. There is minimal likelihood of a deterrence posture successfully preventing the proliferation of less damaging cyber incidents. US deterrence policy developed to curb China's behaviour in cyberspace lacks incentive. However, through continued negotiation and partnership the amount of attacks sustained by the US may decrease. As both China and the US begin to understand how both damage and number of incidents can contribute to the risk of escalation.

The interplay between the cyber domain and the physical domain is a key feature affecting the employment success of deterrent strategies. The implementation of broad-spectrum deterrence offers a more succinct approach to securing US cyber interests. The recommencement of negotiations between the US and China is a good example of the functionality of broad-spectrum deterrence. The path to the 2016 US-Sino cyber agreement was speculated to have been brought about through the threat of sanctions. Another interesting example of broad-spectrum deterrence is a US policy stipulating the usage of a kinetic military retaliation in the wake of a significant cyber incident.

Although it is likely that the more damaging cyber incidents are being successfully deterred. The problems posed by the unique characteristics of the cyber domain remain. The need to improve accurate cost assessment of malicious cyber incidents is important. As is the need to better, determine the efficacy of deterrence as a whole.

CHAPTER 6

CONCLUSION

Chapter Introduction

Regarding US-Sino relations, can deterrence function in cyber space and if so to what degree?

This dissertation has attempted to clarify the place of deterrence within the cyber domain. Set within the context of US-Sino relations it has explored different strands of deterrence theory in conjunction with the technical properties of cyberspace. It has investigated different levels of cyber incidents to establish the value of deterrence as a management tool as well as its applicability to cyberspace. In undertaking this project, the research has assessed the applicability of classical deterrence theory to cyberspace against the available data of cyber incidents perpetrated against the US with a high degree of attribution to China. As the stability of US-Sino relations has been affected by historic mistrust and confrontation the utility of deterrence, as a management tool is relevant.

The employment of a qualitative research method has proved an appropriate technique to study the changing dynamic of US-Sino relations cyberspace continues to evolve. The adoption of a US perspective helped to further focus the line of questioning explored in the dissertation.

Implications of the Research Findings

The research argues that though limited, deterrence can function in cyberspace. It reasons that at the lower levels of cyber incidents the utility of deterrent norms and mechanisms should not be employed for their deterrent prospects. The state of play with US-Sino relations indicates that there is currently little incentive for China to curb its malicious behaviour in cyberspace, the limitations of deterrent norms will not be overcome. However, the study suggests that the pursuit of deterrent norms through the sustained open lines of dialogue is beneficial in mitigating the risk of misunderstandings resulting in escalation. This implies that the pursuit of cyber agreements, between the US and China,

would be useful as a management tool for the relationship. The pursuit of deterrent norms would help lessen the risk of a misunderstanding that could lead to cyber escalation.

The research also indicates that beyond a specific threshold (the division between the costs of category 3 and 4 cyber incidents), deterrence is likely to hold. The thesis proposes that although somewhat counterintuitive, proof of significant cyber capabilities is also unnecessary for deterrence to function. This is primarily due to the known capabilities of both the US and China in other domains (such as their respective nuclear arsenals).

The unique characteristics of cyberspace which contribute to the proliferation of cyber incidents remain an obstacle. As previously explored in Chapter 4, many of those obstacles can be mitigated by the considerable resources of nation-states. For instance, the US has made significant advances in accurately determining clear attribution. However, the issues of attribution, based on the ability of actors to easily disguise themselves using false flag techniques or overloading information required to attribute such as needle in the haystack techniques remain problematic. The likelihood of mitigating these issues in the future relies on advancement within programing (such as gradual modifications of cyber technical protocols thereby improving the likelihood of identifying a source) and the ability to dedicate adequate resources.

Moreover, the study has concluded that a deterrent strategy not be implemented solely in cyberspace to better insure the prospect of its success. The employment of broad spectrum deterrent methods, involving both digital and physical measures, increases the chance of the deterrence working. The adoption of what Cirenza refers to as hybrid deterrence is also natural and evident in other areas where a deterrence posture has been employed.[192]

Conversely, the thesis has also found that given the threat to the cyber environment and the inability to control malicious code once employed, a retaliatory strike should not be conducted in the cyber domain. This assertion has significant implications for the development of cyber policy. It potentially

[192] Cirenza, 2016.

changes the cost of nation-state cyber engagement and could lessen the offence advantage offered by the utility of cyberspace.

Limitations of the Research

In undertaking this research project, several limitations became apparent. The restriction of the course requirements, including completion time and word count, heavily affected the depth of material covered as well as complexity of the findings presented. It is evident that the questions cantering on the applicability of deterrence to the cyber domain are extensive.

Due to the reach of the research project and the limitation of the word count, some areas have had to be covered in less detail. For instance, some of the five requirements set forth by Morgan to enable the success of cyber deterrence have not been adequately presented.[193] The ability to immediately respond to and detect a cyber-attack does not currently exist due to the unique characteristics of the cyber domain. Thus, the prospect of detection and attribution has been narrowly explored; as has the need to improve methods of clear cost evaluation in the wake of cyber incidents, particularly regarding the prevalence of information theft.

Next Steps

The applicability of deterrence theory to cyberspace requires further analysis. Given the confrontational nature of US-Sino relations, clear lines of dialogue and a far greater level of bilateral understanding is needed. Previous publications attempting to address the necessary concessions to reach enforceable agreements on cyber behaviour should also seek to develop a greater understanding of the technical advantage offered by the cyber domain. The research should endeavour to encompass an appropriate amount of technical information to more accurately assess the applicability of certain strategies to the domain.

The information presented in this thesis has raised three areas for further examination by the academic community. Firstly, as the findings have indicated the danger of cyber retaliation in the wake of a

[193] Morgan, 2010

cyber-attack, research investigating how best to evaluate cost and equate a cyber-attack to a kinetic response is necessary. Secondly, as is evident from the lack of understanding regarding cyber – physical interaction, a more comprehensive knowledge of the interplay is needed. Finally, that given the ambiguity of the success of a deterrent measure as the motivation in dissuading a challenger from attacking, it is recommended that methods to test the efficacy of deterrence in cyberspace should be further explored.

The arguments put forward in this dissertation provide a perspective on the functionality of cyber deterrence and its utility to better manage the turbulent relationship between the US and China. In an age of increasing reliance on the proper functioning of the cyber domain the stability of the digital environment is an important question for scholars and strategists alike. Through constant evolution of the cyber domain great power nations, such as the US and China, will continue to shape the usage of cyberspace in the international political sphere. Of increasing importance is the applicability of deterrence to the cyber domain as both a management tool and a method to avoid severe conflict. This dissertation has contributed to the current discourse by helping to shape the conversation on cyber deterrence and its utility to US-Sino relations. However, the future of US-Sino cyber relations remains topical as both an area of interest and concern and will undoubtedly be explored further.

REFERENCES

AFP, "Latest China Military Hardware Displayed at Airshow", *Asia One News*, Singapore Press, 13 November 2012, available from < http://news.asiaone.com/News/AsiaOne%2BNews/Asia/Story/A1Story20121113-383169.html>, (accessed 28 June 2016).

Betz, D. J. & Stevens, T., *Cyberspace and the State: Toward a Strategy for Cyber-Power*, Routledge, London, 2011.

Blanchard, B., "U.S. Sees Progress in Latest Cyber Talks with China, *Rueters*, Business Day, 14 June 2016, available from Reuters < http://www.reuters.com/article/us-china-usa-cyber-idUSKCN0Z00DN> (accessed 15 June 2016).

Buchanan, B., 'The Life Cycles of Cyber Threats', *Survival: Global Politics and Strategy*, February- March 2016, Vol. 58.

Cate, F. H., "Comments to the White House 60-Day Cybersecurity Review", *Center for Applied Cybersecurity Research*, 27 March 2009, accessed 5 March 2017, available from < https://obamawhitehouse.archives.gov/files/documents/cyber/Center%20for%20Applied%20Cybersecurity%20Research%20-%20Cybersecurity%20Comments.Cate.pdf>

Chang, A., *Warring State: China's Cybersecurity Strategy,* Washingtong, D.C.: Center for a New American Security, December 2015, pp. 7, 10. Available < https://s3.amazonaws.com/files.cnas.org/documents/CNAS_WarringState_Chang_report_010615.pdf> (accessed on August 24, 2016).

Cirenza, P., "The Flawed Analogy Between Nuclear and Cyber Deterrence", *Bulletin of the Atomic Scientists*, 22 February 2016, , available from < http://thebulletin.org/flawed-analogy-between-nuclear-and-cyber-deterrence9179> (Accessed 27 July 2016).

Clark, R. A. & Knake, R., *Cyber War: The Next Threat to National Security and What to do About it*, New York, Harer Collins, 2010.

Clausewitz, C. Von, 1832, 1980.

Co-Chairs Commissioner P. Brookes & Senator B. Dorgan, "Hearing on Chinese Intelligence Services and Espionage Operations", *U.S.-China Economic and Security Review Commission*, Washington, D.C.: 9 June 2016, available from < http://www.uscc.gov/Hearings/hearing-chinese-intelligence-services-and-espionage-operations> (accessed 16 June 2016).

Creswell, J. W., *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*, (2nd ed.). Thousand Oaks, SA: Sage, 2007.

Demchak, C., *'Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security'*, University of Georgia Press, Athens, 2011.

Der Derian, J., "Cyber Deterrence", *Wired Magazine*, 2.09, September 1994, available from <https://www.wired.com/1994/09/cyber-deter/> (accessed 28 February 2016).

Donilon, T., "The United States and the Asia-Pacific in 2013", *Asia Society*, Washington, D.C.: White House, March 2013.

Dreyer, J. T., "China's Power and Will: The PRC's Military Strength and Grand Strategy", *Orbis*, 2007, Vol. 51, Issue 4.

Ducheine, Osinga & Soeters (Eds.), *Cyber Warfare: Critical Perspectives*, T.M.C. Asser Press, The Hague, The Netherlands, 2012.

Feakin, T., "Enter the Cyber Dragon – Understanding Chinese Intelligence Agencies' Cyber Capabilities", *Australian Strategic Policy Institute*, June 2013, Issue 50, accessed 2 March 2017, available from <https://www.aspi.org.au/publications/special-report-enter-the-cyber-dragon-understanding-chinese-intelligence-agencies-cyber-capabilities/10_42_31_AM_SR50_chinese_cyber.pdf>

Fearon, J. D., "Selection Effects and Deterrence," *International Interactions*, Taylor & Francis, Vol. 28, 2002.

Fortino, G. & Trunfio, P. (Eds.), *Internet of Things Based on Smart Objects: Technology, Middleware and Applications*, Springer International Publishing Switzerland, Italy, 2014.

Freedman, L. "Britain: The First Ex-Nuclear Power", *International Security*, Vol.6, No. 2, Fall, 1981.

Freedman, L., "General Deterrence and the Balance of Power", *Review of International Studies*, Vol. 15, No. 2, Special Issue on the Balance of Power, April 1989.

Freedman, L., *The Evolution of Nuclear Strategy*, New York, St. Martin's Press. 1981.

Gady, F-S., "New Snowden Documents Reveal Chinese Behind F-35 Hack", *The Diplomate*, 27 January 2015, available < http://thediplomat.com/2015/01/new-snowden-documents-reveal-chinese-behind-f-35-hack/> (accessed 24 February 2016).

Gasser, M., 'What is Computer Security' in *Building a Secure Computing System*, Van Norstrand Reinhold, New York, 1988.

Gertz, B., "China Hacked f-22, F-35 Stealth Jet Secrets", *The Washington Free Beacon*, 24 March 2016, available < http://freebeacon.com/national-security/china-hacked-f22-f35-jet-secrets/>, (accessed 28 June 2016).

Gjelten, T., "First Strike: US Cyber Warriors Seize the Offensive", *World Affairs*, January – February 2013, Vol. 175 Issue 5.

Goodman, W., "Cyber Deterrence: Tougher in Theory than in Practice", *Strategic Quarterly*, Fall, 2010.

Graham, B., "Hackers Attack Via Chines Wed Sites", *The Washington Post*, Washington, D.C., 25 August 2005.

Harknett, R. J., "Information Warfare and Deterrence", *Parameters*, Autumn 1996.

Harold, S. W., Libicki, M. C. & Cevallos, A. S., "Getting to Yes with China in Cyberspace", Santa Monica, C.A.: RAND Corporation, 2016.

Harvey, F. P., *The Future's Back: Nuclear Rivalry, Deterrence Theory, and Crisis Stability After the Cold War*, McGill-Queen's Press, 1997.

Huth, P. & Russett, B., "Testing Deterrence Theory: Rigor Makes a Difference." *World Politics*, Vol. 43,1990.

Ikenberry, G. J., Mastanduno, M. & Wohlforth, W. C., "Unipolarity, State Behaviour, and Systemic Consequence", *World Politics*, 61, No. 1, January 2009.

Jervis, R., "Deterrence Theory Reconsidered", *World Politics*, 39, 1979.

Jervis, R., *Review Article, Deterrence Theory Revisited*, Cambridge University Press, 1979.

Johnson, R. F., "Experts: The US has Fallen Dangerously Behind Russia in Cyber Warfare Capabilities", *The Washington Free Beacon*, 27 July 2016 available < http://www.businessinsider.com/us-behind-russia-cyber-warfare-2016-7?IR=T>, (accessed 31 July 2016).

Kahn, H., *The Nature and Feasibility of War and Deterrence*, RAND Corporation, 20 January 1960.

Kassab, H. S., 'In Search of Cyber Stability: International Relations, Mutually Assured Destruction and the Age of Cyber Wargare', pp.59-76, J-F. Kremer & B. Müller (ed.) in *Cyberspace and International Relations: Theory, Prospects and Challenges*, Geneva, Switzerland, 2014.

Kaufmann, W., *The Requirements for Deterrence*, Centre for International Studies, Princeton University, 1954.

Kderner, B. I., "Inside the Cyberattack That Shocked the US Government", *Wired Magazine*, International Frontiers, Security, 23 October 2016, available from Wired <https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/>, (accessed 16 June 2016).

Kelo, L., "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft", *International Security*, Vol. 38, No. 2, Fall 2013.

Kovacich, G. L., *The Information Systems Security Officer's Guide: Establishing and Managing a Cyber Security Program*, Butterworth-Heinemann, 3rd Edition, 2016.

Kugler, R., "Deterrence of Cyber Attacks", in F. D. Kramer, S. H. Starr & K. Wents (eds.), *Cyberpower and National Security*, Washington, D.C., 2009.

Kuusisto, T. & Kuusisto, R., 'Cyber World as a Social System', in M. Lehto & P. Neittaanäki (ed.), *Cyber Security: Analytics, Technology and Automation*, Springer, 2015.

Lagorio, C., "State Department Computers Hakced", *CBSNEWS*, 11 July 2006, available from CBSNEWS < http://www.cbsnews.com/news/state-department-computers-hacked/> (accessed 15 June 2016).

Lamont, C., *Research Methods in International Relations*, Sage Publishing, London, 2015.

Langer, R., "Stuxnet: Dissecting a Cyberwarfare Weapon", *IEEE Security & Privacy*, Vol. 9, Issue 3, May-June 2011.

Larson, D. W., *Anatomy of Mistrust: U.S.-Soviet Relations During the Cold War*, Ithaca and London, Cornell University Press, 2000.

Lebow, R. N. & Stein, J. G., "Rational Deterrence Theory: I Think, Therefore I Deter", *World Politics*, Cambridge University Press, 1989.

Lebow, R.N., & Stein, J. G., *We All Lost the Cold War*¸ Princeton University Press, 1994.

Lewis, J. A., *Computer Espionage, Titan Rian and China*, Centre for Strategic and International Studies – Technology and Public Policy Program, December, 2005.

Lewis, J. A., *Cyber War and Competition in the China-U.S. Relationship*, Centre for Strategic and International Studies, Remarks delivered at the China Institutes of Contemporary International Relations, May 2010.

Libicki, M., "Cyberdeterrence and Cyber War", *RAND Corporation* Project Air Force, 2009.

Lieberthal, K. & Singer, P. W., *Cybersecurity and U.S.-China Relations*, John L. Thornton China Centre at Brookings, February 2012.

Lieberthal, K. & Wang Jisi, *Addressing U.S.-China Strategic Distrust*, "John L. Thornton China Center Monograph Series", Brookings Institute, Vol. 4, March 2012.

Limnéll, J., "The Cyber Arms Race is Accelerating – What are the Consequences?" *Journal of Cyber Policy*, 1:1, 8 May 2016.

Lyngaas, S., "Pentagon Fret's Over China's Cyber Capabilities", *FCW The Business of Federal Technology*, 8 May 2015, available from < https://fcw.com/articles/2015/05/08/china-cyber-report.aspx>, (accessed on 25 August 2016).

Maj, L. H. W., "The Challenges of Cyber Deterrence", *Pointer, Journal of the Singapore Armed Forces*, Vol. 41, No. 1, 2015.

Majumdar, D., "America's F-35 Joint Strike Fighter vs. China's J-31, F-15SA and Russia's Su-35: Who Wins?", *The National Interest*, 20 September 2016, available from < http://nationalinterest.org/blog/the-buzz/americas-f-35-joint-strike-fighter-vs-chinas-j-31-f-15sa-17767>, (accessed 25 September 2016).

Mallery, J. C., published in summary form in Demchak, "Resilience, Disruption, and a 'Cyber Westphalia': Options for National Security in a Cybered Conflict World." 2011.

Mandiant Report 2013 "APT1, Exposing One of China's Cyber Espionage Units', *Mandiant* 18 February 2013, <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf> (accessed 2 March 2017).

Metz, C., "US to China: We Hacked Your Internet Gear We Told You Not to Hack", *Wired Magazine,* 31 December 2013, available from < https://www.wired.com/2013/12/nsa-cisco-huawei-china/>, (accessed on 3 March 2016).

Montalbano, E., "Virus Hits Part of U.S. Commerce", *Dark Reading,* Information Week IT Network, 3 March 2012, available from < http://www.darkreading.com/risk-management/virus-hits-part-of-us-commerce-dept/d/d-id/1102648>, (accessed 16 June 2016).

Moore, M., "China's Global Cyber-Espionage Network GhostNet Penetrates 103 Countries", *The Telegraph,* 29 March 2009, available from The Telegraph < http://www.telegraph.co.uk/news/worldnews/asia/china/5071124/Chinas-global-cyber-espionage-network-GhostNet-penetrates-103-countries.html> (accessed 20 June 2016).

Morgan, P., "Applicability of Traditional Deterrence Concepts and Theory to The Cyber Realm", *Proceedings of a Workshop of Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy*, University of California, Irvine, 2010.

Morgan, P., "Applicability of Traditional Deterrence Concepts and Theory to The Cyber Realm", *Proceedings of a Workshop of Deterring Cyber Attacks: Informing Strategies and Developing Options for US Policy*, University of California, Irvine, 2010.

Morgan, P., *Deterrence Now*, Cambridge University Press, 2016.

Morgenthau, H. J., *The Balance of Power,* "Essential Readings in World Politics", editors K. A. Mingst & J. L Snyder, 5th edition, W.W. Norton & Company, Inc. London, 2014.

Mueller, P., & Yadegari B., *The Stuxnet Worm*, University of Arizona, Department of Computer Science, 2012, available < http://www.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf>, (accessed 20 January 2016).

Murdock, J., "Shadow Warfare: The Cyber Relationship Between China and the US at 'Breaking Point'", V3, London, 25 August 2015, available from < http://www.v3.co.uk/v3-uk/feature/2423655/shadow-warfare-the-cyber-relationship-between-china-and-the-us-at-breaking-point>, (accessed 24 May 2016).

Nye, J., "Can China be Deterred in Cyber Space", *The Diplomat*, 3 February 2016, available from < http://thediplomat.com/2016/02/can-china-be-deterred-in-cyber-space/> (accessed 5 June 2016).

Nye, J., *Diffusion and* "Cyberpower", In J. Nye (Eds.), *The Future of Power* (pp.113-151). New York: Public Affairs. 2011.

O'Gorman, G. & McDonald, G., *The Elderwood Project*, Symantec Security Response, Mountain View, California, 2012.

Oh, J., "Cyber Cooperation in Northeast Asia: An Interview with James Lewis", *National Bureau of Asian Research*, Policy Q&A, March 17, 2015.

Pan, C., *A Conceptual Corrective to the "Power Shift" Narrative*, Deakin University, 2013.

Presidential Policy Directive/ PPD-41, "Presidential Policy Directive – United States Cyber Incident Coordination", 26 July 2016, accessed on 1 March 2017, available from < https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>

Rainie, L., Anderson J. & Connolly, J., "Cyber Attack Likely to Increase", *PewResearch Center:* Internet, Science & Tech, 29 October 2014, available at< http://www.pewinternet.org/2014/10/29/cyber-attacks-likely-to-increase/> (accessed 2 February 2016).

Rid, T., Cyber War Will Not Take Place, *Journal of Strategic Studies*, 35:1, 2012.

Schelling, T. C., *Arms and Influence,* New Haven, Yale University Press, 1966.

Shih, G., "China, U.S. Hold Talks to Bridge Cybersecurity Differences", *The Bid Story*, 14 June 2016, available from <http://bigstory.ap.org/article/a493922899424ecf988f5a917cd63458/china-us-meet-cybersecurity-talks-beijing> (accessed 15 June 2016).

Shih, G., *China, US Holds Talks to Bridge Cybersecurity Differences*, "The Daily Star", 14 June 2016, available from < http://www.dailystar.com.lb/News/World/2016/Jun-14/356847-china-us-hold-talks-to-bridge-cybersecurity-differences.ashx>, (accessed 15 June 2016).

Siers, R., Silber, M. D & Garrie, D. B., "Cyberwarfare: Understanding the Law, Policy and Technology", (ed. 2015-2016), LegalWorks.

Simonite, T., "Stuxnet Tricks Copied by Computer Criminals", *MIT Technology Review*, 19 September 2012, available < https://www.technologyreview.com/s/429173/stuxnet-tricks-copied-by-computer-criminals/>, (accessed 20 January 2016).

Sims, J., "'Heartbleed' Canada Revenue Hacker Gets a Break", *Toronto Sun*, 20 July 2016, available < http://www.torontosun.com/2016/07/20/heartbleed-canada-revenue-agency-hacker-gets-a-break>, (accessed 31 July 2016).

Smith, I. C., & West, N., *Historical Dictionary of Chinese Intelligence*, Scarecrow Press, Toronto, 2012.

The Wassenaar Arrangement: On Export Controls for Conventional Arms Dual-Usage Goods and Technologies, 2016, viewed 5 April 2016, <http://www.wassenaar.org/>.

Thomas, P., "Chinese Hack Into US Chamber of Commerce, Authorities Say", *ABC NEWS*, 21 December 2011, available from <http://abcnews.go.com/International/chinese-hack-us-chamber-commerce-authorities/story?id=15207642>, (accessed 16 June 2016).

Thornburgh, N., "Inside the Chinese Hack Attack", *Time Magazine*, New York, 25 August 2005.

US Department of Defense, *Joint Publication 3.0, Joint Operations*, Washington, DC, 2011, viewed 12 March 2016 <www.dtic.mil/doctrine/new_pubs/jointpub_operations.htm>.

Valeriano, B. & Maness, R. C., *Cyber War Versus Cyber Realities*, Oxford University Press, 2015.

Waltz, K. N., *Theory of International Politics*, 1ST Edition, Addison-Wesley Publication & Co. 1979.

Warren, S., Libicki, M. C. & Cevallos, A. S., *Getting to Yes with China in Cyberspace*, RAND Corporation, 2016.

Weisgerber, M., "China's Copycat Jet Raise Questions About the F-35", *Defense One*, 23 September 2015, available from Defense One < http://www.defenseone.com/threats/2015/09/more-questions-f-35-after-new-specs-chinas-copycat/121859/>, (accessed 28 June 2016).

Xuetong, Y., *The Instability of China-US Relations*, "The Chinese Journal of International Politics", Oxford Journals, Vol. 3, 13 August 2010.

Yan, X., “The Instability of China- US Relations”, *The Chinese Journal of International Politics*, Oxford University, Vol. 3, No. 3, 13 August 2010.

Yufan, H., & Zhihai, Z., “China’s Decision to Enter the Korean War: History Revisited”, *The China Quarterly*, 121, February 2009.

Zagare F., & Kilgour, D. M., *Perfect Deterrence*, Cambridge University Press, 2000.

Zetter, K., “Google Hack Attack was Ultra Sophisticated, New Details Show”, *Wired Magazine*, 14 January 2010, available from <https://www.wired.com/2010/01/operation-aurora/>, (accessed 25 July 2016).

Zetter, K., “Everything we Know About Ukraine’s Power Plant Hack”, *Wire Magazine*, 20 January 2016, accessed 2 March 2017, available from < https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/>