US-China Strategic Competition in Cyberspace and Its Normative Challenges to Global Order

Submitted by: Syeda Duaa Zehra Naqvi

Enrollment No: 01-257221-012

A thesis submitted in fulfillment of the requirements for the award of the degree of Master of Science (International Relations)

Principal Supervisor

Professor Dr. Adam Saud

Department of Humanities and Social Sciences

Faculty of International Relations

BAHRIA UNIVERSITY ISLAMABAD

2024

THESIS APPROVAL SHEET

Topic: **US-China Strategic Competition in Cyberspace and Its Normative Challenges to Global Order**.

Name of Student: Syeda Duaa Zehra Naqvi

Enrollment No: 01-257221-012

Program: MS (International Relations)

____

Dr. Adam Saud

Thesis Supervisor

____

Name: Dr Saria Nawaz Abbasi

Internal Examiner

____

Name: Dr Bakare Najmideen Ayoola

External Examiner

________________________ _________________________

Program Coordinator Head of Department

Approval for Examination

Scholar's Name: Syeda Duaa zehra Naqvi Registration No. 01-257221-012

Program of Study: Master of Science (International Relations)

Thesis Title: US-China Strategic Competition in Cyberspace and its Normative Challenges to Global Order.

Principal Supervisor's Signature: ___________________

Date: 21-March -2024

Name: Professor Dr. Adam Saud

AUTHOR'S DECLARATION

I, Syeda Duaa Zehra Naqvi hereby state that my MS/MPhil thesis titled "US-China Strategic Competition in Cyberspace and its Normative Challenges to Global Order" is my own work and has not been submitted previously by me for taking any degree from this university Bahria University or anywhere else in the country/world.

At any time if my statement is found to be incorrect even after my Graduate the university has the right to withdraw/cancel my MS/MPhil degree.

Name of student: Syeda Duaa Zehra Naqvi

Date: 21-March-2024

PLAGIARISM UNDERTAKING

I, solemnly declare that research work presented in the thesis titled "US-China Strategic Competition in Cyberspace and its Normative Challenges to Global Order" is solely my research work with no significant contribution from any other person. Small contribution / help wherever taken has been duly acknowledged and that complete thesis has been written by me.

I understand the zero-tolerance policy of the HEC and Bahria University towards plagiarism. Therefore, I as an Author of the above titled thesis declare that no portion of my thesis has been plagiarized and any material used as reference is properly referred/ cited.

I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even after award of MS/MPhil degree, the university reserves the right to withdraw / revoke my MS/MPhil degree and that HEC and the University has the right to publish my name on the HEC / University website on which names of students are placed who submitted plagiarized thesis.

Scholar / Author's Sign: ______________________

Name of student: Syeda Duaa Zehra Naqvi

DEDICATION

I dedicate this research to my beloved father and mother. Their love and support encouraged me to complete my thesis in the required timeframe. They are the reason behind my success, and it was their prayers and efforts that brought me to this level. I also want to dedicate this work to Dr Adam Saud, (my honorable supervisor) for his great contribution and guidance.

ACKNOWLEDGEMENT

First and foremost, I humbly express my deepest gratitude to Allah Almighty, whose guidance and blessings have illuminated my path throughout this remarkable journey. To my beloved parents, whose boundless love, sacrifices, and belief have been the driving force behind my accomplishments. Your tireless support and endless encouragement have been the foundation upon which my achievements stand.

I am profoundly indebted to my exceptional supervisor Prof. Dr. Adam Saud, whose invaluable guidance, expertise, and mentorship have shaped my academic endeavors. Your unwavering commitment to my growth and development has propelled me towards excellence. I also want extend my heartfelt appreciation to the esteemed faculty of International Relations, whose profound knowledge, dedication, and passion for education have enriched my understanding of the world. Their commitment to academic excellence has been an endless source of inspiration.

Gratitude is also owed to the diligent and dedicated staff at the Department of Humanities and Social Sciences, whose unwavering support and administrative assistance have facilitated my academic journey and made it all the more fulfilling.

To my cherished friends Iqra Batool and Aksa Safdar, your camaraderie, laughter, and intellectual exchanges have made this journey extraordinary and have left an indelible mark on my heart.

Last but not least, I express gratitude to myself, for believing in my potential, resilience, and determination. It is through self-belief and perseverance that I have overcome obstacles and reached this significant milestone.

ABSTRACT

The study conducted to assess the role of cyberspace in the tensions which are central to the great power rivalry between China and the United States. The US and China have been in the strategic competition in the economic, military, and technological realms and cyberspace is one of the aspects of the strategic rivalry and it has implications beyond the domestic realm into the international rule-based order which was setup by the United States and the West after the World War 2. The objective of the study is to is to find out the implications of the cyberspace tensions on the rules-based order and try to assess the root causes of the warfare and what can be the way forward to deal with the issue on hand which is relatively new and the both the states are not willing to compromise on their stance when it comes to cyberspace as this domain is relatively significant in determining the next big solo super power. The research delves into the questions by reviewing the content specific to the cyberspace and US China strategic tensions and the research also includes testimonies of the experts on cybersecurity and great power politics. The study adopts a qualitative methodology, utilizing the constructivist theory as a framework for analysis. The findings involve that the competition between the United States and China in cyberspace is characterized by its multifaceted and ever-changing nature. Both countries are engaged in a constant pursuit of dominance over the cyberspace, utilizing a combination of legitimate and illegitimate strategies to achieve their goals. Both the United states and the Chinese are trying to outmaneuver each other in the cyberspace domain and this leads to the infringement on the rules-based order from the both sides.

Key words: US-China cyber competition, Global order, Technological superiority, Cyber capabilities, normative challenges, Cyber governance

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1) Background of the study:

Technological advancements, economic interests, security concerns, and geopolitical factors have all had an impact on how the U.S.A and China have competed strategically in cyberspace throughout time. As cyberspace emerged in the first decade of the 20th century, concerns regarding misuse of the cyberspace came on the surface. National security concerns, geopolitical conflicts, and technological rivalry have all played a complex role in the competition between hegemon United States of America, wants to maintain status quo, and China- as challenger- in cyberspace.[1] Both countries have participated in substantial cyber operations including as attempts to influence each other's political environments, cyber espionage, and intellectual property theft. China has long refuted the accusations claimed by the hegemon United States which claims a victim of cyber espionage, and has accused Beijing of state-sponsored cyber-attacks directed at vital infrastructure and sensitive data.[2]

The competition between these two major powers raises questions about the existing international norms and rules governing state behavior in cyberspace. Conflicts arise over issues such as attribution of cyber-attacks, defining appropriate conduct, and establishing systems for cooperation and dispute resolution. Different perspectives and objectives of the US and China in cyberspace

[1] ImreDobák, “Thoughts on the Evolution of National Security in Cyberspace,” *Security and Defence Quarterly* 33, no. 1 (March 1, 2021): 75–85, https://doi.org/10.35467/sdq/133154.

[2] Magnus Hjortdal, “China’s Use of Cyber Warfare: Espionage Meets Strategic Deterrence,” *Journal of Strategic Security* 4, no. 2 (2011): 1–24. https://www.jstor.org/stable/26463924

challenge the current normative framework- potentially undermining the principles of sovereignty, privacy, intellectual property rights, and the defense of critical infrastructure.[3]

However, as cyber espionage, hacking events, and intellectual property theft raised, worries about cyber-security started to surface. Chinese cyber activities targeting American businesses and government networks alarmed the US government and private sector organizations more and more.[4] A major source of interest and worry, in recent years, has been the US-China strategic rivalry in cyberspace. Cyber espionage actions linked to China attracted a lot of attention in the middle of the 2000s.

One of the earliest cases of state-sponsored espionage, alleged the China, was the 2003 Titan Rain cyber-attacks, which targeted US defense contractors and government institutions. Several notable organizations were affected by the cyber-attacks known as Titan Rain. Chinese hackers used a variety of techniques to breach targeted networks in the highly sophisticated "Titan Rain" operations. The hacks highlighted the ease with which sensitive material and information can be stolen by unauthorized parties and revealed vulnerabilities in US computer systems. [5]Chinese hackers used a variety of techniques to breach targeted networks in the highly sophisticated Titan Rain operations. The attacks highlighted the ease with which sensitive material and information may be theft by unauthorized parties and revealed weaknesses in US computer systems. The US government took strong action to improve computer system security in reaction to the Titan Rain disaster. Stronger cybersecurity procedures, cutting-edge threat detection tools, and thorough

[3] Robert D. O'Brien and ShiranShen, "The U.S., China, and Cybersecurity: The Ethical Underpinnings of a Controversial Geopolitical Issue," *Carnegie Council*, May 24, 2013, https://www.carnegiecouncil.org/media/article/the-u-s-china-and-cybersecurity-the-ethical-underpinnings-of-a-controversial-geopolitical-issue.

[4] LyuJinghua, "What Are China's Cyber Capabilities and Intentions?," Carnegie Endowment for International Peace, April 1, 2019, https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734.

[5] "Connect the Dots on State-Sponsored Cyber Incidents - Titan Rain," Council on Foreign Relations, August 2005, https://www.cfr.org/cyber-operations/titan-rain.

employee training were all part of this effort to reduce cyber threats. Subsequent cyber-attacks against the US government and military continued in spite of preventative efforts. The Titan Rain incident made clear how important it is to continuously develop and modify cybersecurity defenses against changing threats.

Similar to this, Chinese hackers carried out Operation Aurora in 2009, stealing intellectual property from large American corporations.[6]These state-sponsored cyber-attacks targeted companies like Google, Adobe, Yahoo, Symantec, and others. The malware employed in the assaults makes references to a folder that MacAfee researchers discovered on one of the systems used by the attackers, which gives the attacks their name.[7]These events strengthened China's reputation in the US as a serious cyber threat.

Furthermore, the US Office of Personnel Management was hacked by Chinese hackers in 2015, which led to the loss of private information belonging to federal employees and applicants for security clearances. The scale of China's cyber espionage activities was questioned in light of these cyber -attacks, which further impacted US-China relations.

Moreover, an allegedly pilfered dataset from China is being sold by cybercriminals. Regarding the transaction, it is claimed that the entire data trove contains classified documents and personal identity information for nearly 500 million Chinese residents. China says that "U.S. cybercriminals" broke into a Wuhan earthquake monitoring system. According to Chinese official media, the programme was compromised to include a backdoor that might be used to steal seismic data. China

[6] James Mulvenon, “Pla Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability,” Beyond The Strait: (Strategic Studies Institute, US Army War College, 2009), https://www.jstor.org/stable/resrep11950.11.

[7] Fawad Ali, “Everything You Need to Know About Operation Aurora,” MUO, March 16, 2022, https://www.makeuseof.com/operation-aurora/.

stated, referring specifically to the National Security Agency's (NSA), that in the month June 2022, the US had obtained approximately ninety-seven billion pieces of global internet data and one hundred and twenty-four billion pieces of phone data. [8]

Cyberspace has seen an increase in strategic competition. In terms of offensive cyber operations, defensive countermeasures, and cybersecurity laws, both the US and China have expanded their investments. Due to concerns about national security, the US has restricted the export and import of some essential items, for example semi-conductors, to Chinese telecom companies. Additionally, China has tightened its internal cybersecurity laws, including by passing a contentious national cybersecurity law.[9]

Both nations, US and China, are technologically advance and strategically vying great powers in cyberspace. Cyberspace is the collective term for the network of interconnected computer systems and digital infrastructure that supports online interaction, data sharing, and other activities.[10] It has a substantial impact on the economic, political, and military spheres, making it a significant setting for international strategic struggle.

Both the US and China have participated in a range of cyber activities, including economic espionage, intelligence collection, and potentially disruptive or dangerous cyber operations. Although non-state actors may also participate in these activities, state-sponsored actors are frequently involved. The US and China's cyberspace strategic rivalry poses normative challenges

[8] "Significant Cyber Incidents | Strategic Technologies Program | CSIS," Center for Strategic and International Studies, accessed January 5, 2024, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

[9] Jon R. Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction | International Security | MIT Press," 7–47, accessed August 9, 2023, https://direct.mit.edu/isec/article/39/3/7/30310/The-Impact-of-China-on-Cybersecurity-Fiction-and.

[10] BojanAzap, "What Is Cyberspace?," *phoenixNAP IT Glossary* (blog), October 18, 2022, https://phoenixnap.com/glossary/what-is-cyberspace.

for the world order. Norms are collective expectations or standards of conduct that direct the activities of nations and other international players.[11]

The use of force, sovereignty, privacy, intellectual property rights, and the defense of vital infrastructure in cyberspace are all subject to norms. Due to the evolving nature of competition in cyberspace and the between the hegemon US and challenger China, the existing global order, which consists of international rules, norms, and institutions, may have trouble keeping up. Conflicts over the standards and guidelines that govern state behavior in cyberspace may result from these two great countries' differing perspectives and objectives.

Significant challenges to the global order are posed by issues including attribution of cyber-attacks, defining appropriate conduct in cyberspace, and building systems for cooperation and dispute resolution. The normative environment is also complicated by issues related to security and privacy, the control of emerging technologies, and the defense of key infrastructures.

1.2) Research gap/rationale

The work on advancement of technology and its integration into the economic, political and strategic domain has been illustrated by several researches. In the same way, researchers have pinned down many articles on the strategic competition between China and US alongside on-going trade war. In addition to this, a race to dominate the cyberspace has also begun between China and United States. There are, however, dire strategic implications of the US-China confrontation in the cyberspace which require deep and insightful research. The study prominently aims to focus on the strategic implications of US-China competition in cyberspace on global order and would work to fill this gap.

[11] "What Are Norms? - PHILO-Notes," March 21, 2023, https://philonotes.com/2023/03/what-are-norms.

1.2.1) Theoretical Gap

There are several researchers, who have worked on the topic of strategic competition between USA and China in cyberspace, but Thomas Elizabeth in an article used realism as theory to interpret the Chinese cyber capabilities and it poses normative challenges to the international order.[12]China's cyber capabilities are analyzed in the study, and the author uses a realism lens to understand China's cyber-related motivations and behaviors. He analyzes how China's pursuit of cyber power aligns with realist principles such as the pursuit of national interests, power projection, and the desire to reshape the international order to its advantage. Moreover, from a neo-realist perspective in particular, the power struggle may incorporate elements like technological prowess, control over global internet regulation, and ownership of essential infrastructure. In discussions of "US-China Strategic Competition in Cyberspace and Normative Challenges to Global Order," realist theory has frequently been utilized by academicians to explain events. But there haven't been conversations on constructivism, which provides understanding of how ideas, identities, and norms are formed in cyberspace. Therefore, the West—particularly the United States—is working hard to present china as violator of norms which formulate the global order in the realm of cyberspace.

1.2.2) Contextual Gap

The strategic rivalry between the US and China in cyberspace is a dynamic and complicated phenomenon with profound ramifications for both States as well as the broader international arena. This competition is characterized by a wide range of activities, including attempts to gain technological domination, information warfare, theft of intellectual property, and cyber espionage.

[12] Elizabeth Thomas, "US-China Relations in Cyberspace: The Benefits and Limits of a Realist Analysis," *E-International Relations* (blog), August 28, 2016, https://www.e-ir.info/2016/08/28/us-china-relations-in-cyberspace-the-benefits-and-limits-of-a-realist-analysis/.

The lack of a comprehensive global governance framework for cyberspace further complicates the competition between the Washington and Beijing in this domain. Guidelines and standards for responsible state conduct are still being developed, and the US and China continue to dispute on matters like state-sponsored cyber-attacks and how to strike a balance between privacy and security. It is crucial for both countries to find avenues for constructive dialogue and engagement to manage and mitigate the risks associated with this competition, while also identifying opportunities for cooperation in areas of common interest.

1.2.3) Methodological gap/analysis

The descriptive perspective of the strategic competition in cyberspace was the primary focus of earlier research projects. The study is qualitative in nature and Case Study is used as research strategy. Moreover, thematic analysis is used to analyze data.

1.3) Problem statement

The United States and China are in a strategic competition where both the states compete in various domains such as the economic, geopolitical, and technological realms. The intensifying strategic competition between the US and China in this domain is driven by their ambitions to lead in technological development. This has been also true in the realm of cyberspace and both the Chinese, and the United States are not following the normative rules which are helpful in running the affairs of states in the global context. Both states have been involved in cyberwarfare on each other and it has led to deviations from the international law and the normative rules of engagement have not been followed. So, it is imperative we study the impact of both China and the United states behavior in the realm of cyberspace to understand its implications on the world order when it comes to cyberspace.

1.4) Research questions

1. What is the vital importance of normativity as a factor in shaping the global order?
2. How are China and the U.S.A. competing strategically in cyberspace?
3. Why do China's and United Stated of America actions in cyberspace present normative challenges to the global order?

1.5) Objectives of the Study

- To analyzes the strategic implications of US-China competition and normative challenges to global order.

1.6) Research Hypothesis

The on-going strategic competition between US and China in cyberspace can be one of the factors which will reshape the normative world order as the both China and United States are not abiding by the rules when it comes to cyberspace.

1.7) Significance of the Study

The study is very significant because it helps in understanding the strategic relations between the United States and the Chinese when it comes to the cyberspace domain. There are various components of the strategic relations between the big powers, but the cyberspace domain is relatively new, and it needs to be explored to make sure that we identify the issues which includes privacy and sovereignty being challenged by the big powers. The rules in the international arena are not defined when it comes to cyberspace, and it leads to escalations between the US and China.

The United States remains a hegemon and it defines the rules-based order. The Chinese are not accepting the rules imposed by the great power and the tensions have led to significant bans on the companies and technologies on either side in the recent times. So, the study becomes significant as understanding the nature of cyberspace politics will lead to better understanding the tensions and hence the world will be able to find the solutions to the cyberspace tensions between the US and China.

In addition, this research contributes to the academic knowledge by delving into the intricate interplay between technology, geopolitics, and normative frameworks. It specifically examines the multifaceted threats arising from the strategic competition between the US and China in cyberspace, with a special emphasis on the normative challenges confronting the global order. The study aims to bridge the existing gap in the literature on this subject matter.

CHAPTER 2

LITERATURE REVIEW/ THEORETICAL FRAMEWORK

2.1) Literature Review

The ongoing competition in cyberspace between two prominent great power, the US and China, is of great significance to researchers for a number of prominent reasons. First and foremost, cyberspace is becoming vital area of contention due to economic growth, technical innovation, and national security. Since both, Washington and Beijing, are significant actors in the world stage, their online behavior has far-reaching effects on both the international community and each other. Both countries want to become world leaders in emerging technologies and acquire a competitive advantage in fields like artificial intelligence, 5G, and quantum computing. They also want to influence digital governance and set global standards. Studying this competition is crucial due to concerns about cyber security threats, economic espionage, and protecting sensitive data. It is essential to comprehend the dynamics of their interactions in cyberspace in order to create international standards, diplomatic approaches, and cyber-security measures that effectively manage and prevent possible disputes.

This section broadly covers the literature review. Moreover, the section of literature review is further divided into the following categories based on the common themes i.e. US-China Strategic Competition in Cyberspace, Risks and Opportunities in Cyberspace Competition for US and China, Future of US-China Strategic Competition and World Order.

2.1.1) US-China Strategic Competition in Cyberspace

Research article on US-China Confrontation in Cyber Security conducted by Sergii Fedoniuk, discusses the on-going activities of major competitors the prominent and new emerging field of cyber-security. Furthermore, it elucidated the principal patterns of the rivalry and investigated the goals and strategies of cyber influence between these two states. The author identified the United States of America as the undisputed world leader in cyber-security and also foresees Beijing as potential competitor to close the gap[13]. With the advent of the cyber technology, both states are at crossroads and alleged each other of espionage and cyber-attacks for economic and strategic purposes. On the other hand, China accuses United States of using and exploiting the cyber domain to extend the world hegemony. Overall, this research revealed that the topic of cyber-security in US-China relations is growing important with regard to the security plans of the two powerful leaders of contemporary global politics. At the level of relationships with strategic competitors, cyber threats are being used as a vehicle for communication and influence.

KVV Sanchez noted in their research that China and the US both openly acknowledge cyberspace as a theatre of war. The competition is centered on several technological fields, including as military technology, artificial intelligence, and cyber-espionage. This study's major goal was to illustrate how big powers use the US-China competition to their advantage in order to further their political goals.[14] Discourse analysis, a survey of the literature, and pertinent data has been used primarily in the research process. According to the research findings, both governments are swiftly exploiting the cyberspace as a novel platform for competing activities in fields like trade, technology and military

[13] СергійФедонюк and СергійМагдисюк, "US-China Confrontation in Cyber Security," *Історико-ПолітичніПроблемиСучасногоСвіту*, no. 45 (June 27, 2022): 113–27, https://doi.org/10.31861/mhpi2022.45.113-127.

[14] Karina Veronica Val Sanchez and NezirAkyesilmen, "Competition for High Politics in Cyberspace: Technological Conflicts between China and the USA," *Polish Political Science Yearbook* 50 (2021): 43.

applications, which is consistent with prior literature and general public opinion worldwide. The key areas of contention between these two major competitors over the past ten years have been cyber espionage, the militarization of cyberspace, and AI.

According to GP Manson's research, China has grabbed attention from throughout the world because of its bold and frequently highly sophisticated use of cyber capabilities against both foreign and domestic targets.[15]. Chinese cyber activities increasingly target American businesses or government networks. The use of cyber warfare, which has recently become an essential operational arena, will have a major influence on how future confrontations between the hegemon Washington and Beijing turn out. This study analyses relative cyber capabilities that each nation currently possesses and proposes policy recommendations for strengthening American Cyber war-fighting prowess.

The study, conducted by Spade and Jayson, examines China's evolving cyberspace policies. It examines China's goals, which include defending its own cyber interests, strengthening its military, economic, and geopolitical power. The writers look at China's strategy and how it uses cyber tools and techniques to accomplish its objectives. The research paper also explores the precise strategies and methods used by China in the cyberspace. It looks at how China uses advanced persistent threats (APTs), cyber espionage, hacking, and other cyber capabilities. The authors examine the effects these strategies have on the entities they are targeting as well as how they fit with China's strategic goals[16]. The developments of Chinese technology in the field of cyberspace are also discussed in the study. It looks at China's spending in R&D, its emphasis on cutting-edge technologies like artificial intelligence and quantum computing, and how these affect its cyber capabilities. The authors also

[15] George Patterson Manson, "Cyberwar: The United States and China Prepare For the Next Generation of Conflict," *Comparative Strategy* 30, no. 2 (May 3, 2011): 121–33, https://doi.org/10.1080/01495933.2011.561730.
[16] COLONEL JAYSON M. SPADE, "China's Cyber Power and America's National Security" (Defense Technical Information Center, March 24, 2011), https://apps.dtic.mil/sti/citations/ADA552990.

evaluate how China's technological development may affect the dynamics of global cyber power. The writers go over the effects China's cyber strength will have on international relations and world security. They look at how China fits into the global cyberspaces, how it interacts with other governments, and the threats it poses to long-standing cyberspace norms and regulations. The influence of China's cyber strength on global security dynamics and the possibility for conflict escalation are discussed in the study.

Richard A. Clarke and Robert K. Knake's Book Cyber War: The Next Threat to National Security and What to do about it focuses on the threat posed by cyber warfare and how it might affect national security. The book discusses the growing importance of cyber-attacks and looks at the risks that government, businesses, and people face today. The authors also emphasize the growing danger of cyber warfare and how bad actors might use information system flaws to launch devastating strikes on military targets, key infrastructure, and government networks. They talk about how such attacks might have negative effects like disrupting vital services, causing economic instability, and compromising private information. The authors emphasize how bad actors might use information system flaws to launch devastating attacks on vital infrastructure, military assets, and governmental networks while also highlighting the growing threat posed by cyber warfare[17]. They talk about the possible effects of these attacks, such as the interruption of vital services, the instability of the economy, and the compromise of private data. “Cyber War" also explores the difficulties in attribution in cyberspace and defending against cyber-attacks. The writers offer light on the complex makeup of cyber battles and the significance of intelligence collection, analysis, and preventative defense tactics.

[17] George Michael, “A Review of: ‘Richard A. Clarke and Robert K. Knake. Cyber War: The Next Threat to National Security and What To Do About It.,’” *Terrorism and Political Violence* 23, no. 1 (December 7, 2010): 124–26, https://doi.org/10.1080/09546553.2011.533082.

The theme of the Cyberspace 'Great Game’, written by G Viral, revolves around the intense competition among major global powers to shape and control the norms and rules governing the cyberspace domain. The principal players in this game are the Five Eyes alliance and the Sino-Russian bloc, which consists of China and Russia. In an effort to establish their preferred rules in cyberspace and demonstrate their influence, both sides are fighting for dominance. Historically, the Five Eyes alliance has placed a strong emphasis on privacy of the individuals and protection of norms such as protection of freedom of speech and expression in its support of an open and democratic internet. The Sino-Russian bloc, in contrast, advocates a more state-centric strategy that places a higher priority on sovereignty, control, and censorship in cyberspace.[18] These two groups are attempting to gain support and influence from other nations and regions as their rivalry heats up in an effort to change the course of history worldwide and mould the future of cyberspace. The outcome of this great game will have far-reaching implications; not only for the countries involved but also for individuals, businesses, and governments worldwide as the rules and norms that emerge will shape the nature of our increasingly interconnected digital world.

As a result of the region's increased exposure to cyber threats, the main argument of RANDY PESTANA’s works Cyber-security: The Next Frontier of U.S.-China Competition in the Americas examines growing need for international collaboration to strengthen cybersecurity defenses in Latin America and the Caribbean (LAC). The United States is presenting itself as a preferred cyber partner in an order to counter China's growing dominance in the area. The lack of resources, inadequate legislation, and ageing digital infrastructure in LAC nations has fostered an environment conducive to cybercrime. The majority of LAC countries do not have adequate

[18] Nikola Pijović, “The Cyberspace ‘Great Game’. The Five Eyes, the Sino-Russian Bloc and the Growing Competition to Shape Global Cyberspace Norms,” in *2021 13th International Conference on Cyber Conflict (CyCon)*, 2021, 215–31, https://doi.org/10.23919/CyCon51939.2021.9468296.

cybersecurity policies in place, and the existing legislation against cybercrime is inadequate. China has made large investments in the region's ICT infrastructure, raising questions about data security and the potential for user data to be controlled by the Chinese government. In US National Cyber security Strategy, the United States has emphasized the need to support partner countries against cyber-attacks because it has a vested interest in defending LAC nations against agreements with China that take advantage of them.[19] LAC nations can take advantage of current global initiatives and work with world leaders to improve their cyber security capabilities. The United States of America must play a significant role in aiding the region by sharing knowledge, extending legal and regulatory support, and investing in cyber security education and training. The article emphasizes how regional stability, economic development, and digital resilience may all be enhanced through international cooperation and support.

Francis C. Domingo explains the reasoning behind the development of cyber warfare capabilities by powerful states in his paper Conquering a new domain: Explaining great power competition in cyberspace. In order to compete for military supremacy in the global system, it is believed that powerful nations seek to improve their cyber capabilities, even though cyberspace appears to have limited strategic utility. Since it offers the most plausible explanation for governments' competitive behavior in cyberspace, it is best to analyze this argument within a neorealist framework. Three prominent conclusions may be drawn from the study: first, powerful governments will continue to dominate cyberspace; second, given the uncertainty surrounding current cyber capabilities, cyber-

[19] Randy Pestana, “Cybersecurity: The Next Frontier of U.S.-China Competition in the Americas,” *Americas Quarterly* (blog), July 25, 2023, https://www.americasquarterly.org/article/cybersecurity-the-next-frontier-of-u-s-china-competition-in-the-americas/.

attacks may escalate to kinetic strikes; and third, there will undoubtedly be a proliferation of capabilities for combat in cyberspace.[20]

2.1.2) Risks and Opportunities in Cyberspace Competition for US and China

The study Chinese Concepts and Opportunities in Information Warfare: China - US Rivalry in Cyberspace by Katkova E.Y. and Yunyushkina A.S. mainly concentrated on the increasing threats to information security and the geopolitical struggle in cyberspace between China and the United States of America, two of the major actors in contemporary world politics. S. Mori, the author, provided evidence of China's aggressive development of offensive cyber capabilities throughout the previous ten years. With the newest technology and a modern army ready for combat, China is becoming a more formidable force in the world. But China is falling behind the United States in terms of technological capabilities. And it is also lagging behind in the area of cyberspace. Nowadays, there is a strategic component to the cyber race. Both titans are investing a great deal in the development of cybersecurity. The methods China and the United States use to wage informational wars and protect themselves against various threats and difficulties they face online are also contrasted and compared by the author. The author has, for the most part, concluded that China plans to actively push information technology forward and enhance its strategic potential in the cyber domain in the foreseeable future. This will eventually lead to more competitive ties between major nations in crypto space.

The theme of the research study Cyber Espionage and the Future of Sino-American Relations by Wortzel, Larry revolves around the exploration of cyber espionage activities between Washington and the Beijing and its consequential effects on the bilateral relationship. The paper analyzes the

[20] Francis C. Domingo, "Conquering a New Domain: Explaining Great Power Competition in Cyberspace," *Comparative Strategy* 35, no. 2 (March 14, 2016): 154–68, https://doi.org/10.1080/01495933.2016.1176467.

motivations, methods, and consequences of cyber espionage, highlighting the challenges it poses to Sino-American relations and discussing potential future developments. Additionally, the impact of cyber espionage on China-US bilateral ties is covered in this paper. It examines how the discovery and exposure of cyber espionage activities have strained diplomatic ties, eroded trust, and heightened tensions between the two nations. The author analyzes the implications for cooperation, trade, and security cooperation. The study also discusses prospective changes in Sino-American cyber espionage in the future and how they might affect bilateral ties.[21] It takes into account scenarios like heightened cooperation, intensifying conflicts, or the creation of standards and agreements to reduce cyber espionage activities. The author talks about the difficulties and possibilities for controlling cyber dangers and creating positive relationships.

The article determining the Future of the Internet: The U.S.-China Divergence by Johanna Costigan explores the differences between the Chinese and American digital policy frameworks. The article highlights how both nations' approaches to the Internet are shaped by their respective guiding views.[22] The US prioritizes individual independence and freedom of expression, whereas China focuses on collective discipline and government oversight. The US advocates for a vague concept of digital liberty, in line with its political ethos, while China closely regulates its internet through bodies like the Cyberspace Administration. The Chinese government aims to uphold a distinct Chinese internet and propagate the concept of "internet sovereignty" as a global standard, contrasting with the Western idea of an unrestricted and accessible internet. The article brings attention to

[21] Larry M. Wortzel, "China's Approach to Cyber Operations: Implications for the United States," *U.S.-China Economic and Security Review Commission. H*, March 10, 2010, 4–5.
[22] Johanna Costigan, "Determining the Future of the Internet: The U.S.-China Divergence," Asia Society, January 2023, https://asiasociety.org/policy-institute/determining-future-internet-us-china-divergence.

growing tensions between the US and China concerning internet governance and the widening disparity in their principles.

Greg Austin's book China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain offer a thorough examination of China's involvement in cyber security. The book delves into the complex dynamics of Chinese cyber operations, encompassing political aspects in the digital sphere, strategic concerns, and espionage. Austin's study is noteworthy for its strength in highlighting the political ramifications of China's cyber operation particularly about the geopolitical aspects of the digital sphere by delving into the relationship between politics and cybersecurity. This is especially pertinent now that cyberspace is playing a bigger role in determining the balance of power in the world. In conclusion, Greg Austin's book "China and Cybersecurity" predicts the Chinese offensive role in cyberspace that can shackle the US-China strategic relations particularly in cyberspace.[23]

The book The Dawn of Code War: America's Battle against Russia, China, and the Rising Global Cyber Threat authored by Edwin E. Urie offers an engaging examination of the current issues surrounding cyber threats on a worldwide basis. Carlin expertly simplifies the ongoing cyber war and explains how cyber activities are impacting the relationships among the great powers. "The Code War" is still a useful tool for comprehending the larger context of worldwide cyber threats and the difficulties the United States has in this changing environment, notwithstanding the claims of some detractors that the rapid pace of cyber advancements may make some details out of date. In

[23] Greg Austin, “China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain, Edited by Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron,” *The China Journal* 75 (January 2016): 161–63, https://doi.org/10.1086/684056.

conclusion, John P. Carlin'sbook “The Code War” states summarize the modern cyber threats which are being posed and confronted by states.[24]

In this article, the innovation imperative: technology and US–China rivalry in the twenty-first century Andrew B. Kennedy, Darren J. Lim asserts that technology is a key factor in power shifts, but there is currently no framework in the area to comprehend how innovation and technology lead to rivalry between established and emerging states. This study fills that vacuum with an empirical focus on modern US-China relations. The author delineates the "innovation imperative" that is pushing emerging nations to strive for technical modernity. Moreover, it underscores the prominent two ways that can jeopardize the strategic objectives of the leading state- which is predominantly US. First, there are negative security externalities that seriously undermine the security environment of the dominating state: US. Second, negative order externalities pose a danger to the dominant state's supported international order- liberal international order.[25] The author goes on to describe how the dominating state reacts to the adverse externalities brought about by the rising and dominant states, Furthermore, the author surpasses the conventional emphasis on military conflict during shifts in power and provides novel perspectives on the ongoing dynamics within the relations between the United States and China.

The article, China’s Growing Cyber War Capacities written by Mattia, explains the term’s usage in brief and goes into detail about three main issues pertaining to Cyber war: the benefit of offensive tactics, the issue of attribution, and the issue of deterrence. The two sorts of assaults that will be discussed next are military and non-military, with a special emphasis on cyber espionage as opposed

[24] Edwin Urie, “Dawn of the Code War: America’s Battle Against Russia, China, and the Rising Global Cyber Threat. By John P. Carlin, with Garrett M. Graff. New York: Hatchett Book Group, 2018.,” *Journal of Strategic Security* 12, no. 3 (October 1, 2019), https://doi.org/10.5038/1944-0472.12.3.1766.

[25] Andrew B. Kennedy and Darren J. Lim, “The Innovation Imperative: Technology and US–China Rivalry in the Twenty-First Century,” *International Affairs* 94, no. 3 (May 1, 2018): 553–72, https://doi.org/10.1093/ia/iiy044.

to the numerous other cyber-attacks that can be carried out by both governments and non-state actors. Second and most important section of the article mainly examines China's cyber foreign policy while also summarizing and assessing the country's military's cyber capabilities. In addition, it examines China's non-military cyber-foreign policy endeavors, specifically cyber espionage, and raises the question of how such capacities can be applied in a hypothetical war with the United States. In evaluating China's cyber capabilities in light of recent claims, this article examines assessments and a few of the more notable instances of what are known as Sino cyber intrusions.[26]

In the article, People's War in Cyberspace: Using China's Civilian Economy in the Information Domain, kieran Richard green states that People's China is considered to be the main threat to US national security's objectives in cyberspace. These dangers occur everywhere. The spectrum of conflict, which includes low-level criminal activity, network intrusions, and cyber-attacks with the capacity to seriously harm physical infrastructure, has been discussed in the paper. Most strategic evaluations of China's cyber capabilities to far have concentrated on the People's Liberation Army (PLA), whose official mission is to conduct offensive operations in cyberspace, plays this role. China, however, does not use its cyber capabilities alone. Instead, it views cyberspace as a component of the Information. Chinese ideology states that managing the information environment requires utilizing network, electromagnetic assets for propaganda and intelligence in the military and civilian domains that are working in collaboration with other gradients of national power to accomplish strategic goals. Thus, during the previous 20 years, China has implemented a programme of enhancing its capabilities in information warfare (IW) by utilizing the civilian sector (commercial entities, academics, and institutions of civilian government). In conclusion, this study evaluates

[26] MattiaNelles, “China’s Growing Cyber War Capacities,” *E-International Relations* (blog), July 29, 2012, https://www.e-ir.info/2012/07/29/chinas-growing-cyber-war-capacities/.

China's cyber auxiliary capabilities and offers a comprehensive overview of how China employs the civilian economy in each of the four information domain domains as a "strategic reserve."[27]

2.1.3) Future of US-China Strategic Competition and World Order

In the research article, Sangbae Kim states that what kind of underlying structural factors are contributing into the US-China strategic competition in cyberspace. Moreover, this article revolves around the foreign policy dynamics and effective role of norms in making and shaping the competition. The report examines the structural features of the cybersecurity competition between China and the US. It examines issues such as the development of technology, economic interconnectedness, military prowess, and the allocation of power in the global order.[28]The authors investigate how the dynamics of cybersecurity competition are impacted by these fundamental elements. In the area of cybersecurity, the research paper analyses the foreign policy plans and initiatives of both the United States and China. It examines how their respective national security concerns, foreign policy objectives, and regional interests influence their approach to cybersecurity, including their offensive and defensive capabilities, interactions with other actors on the international stage, and cooperation with other actors. The authors also talk about how norms have influenced China's and the United States' competition in cybersecurity. They look at how international standards have developed and emerged in cyberspace, including those pertaining to state conduct, responsible behavior, and the deployment of offensive cyber capabilities. The analysis in the study looks at how both countries' adherence to or disregard for these standards impacts the competitive dynamics.

[27] Kieran Green, “People’s War in Cyberspace: Using China’s Civilian Economy in the Information Domain,” *Military Cyber Affairs* 2, no. 1 (December 20, 2016), https://doi.org/10.5038/2378-0789.2.1.1022.
[28] Sangbae Kim, “US-China Competition in Cyberspace: A Perspective of Emerging Power Politics and Platform Competition,” *The East Asia Institute*, January 2019, http://www.sangkim.net/us-china-c-in-c.pdf.

The primary idea of Ghost Fleet: A Novel of the Next World War book by P.W. Singer and August Cole is the fictional use of cutting-edge military technology in a future world war. In the book, the effects of technical development, geopolitical unrest, and the changing character of combat are all examined. With a focus on the role of cutting-edge technology like artificial intelligence, unmanned vehicles, cyber warfare, and space-based systems, "Ghost Fleet" portrays a speculative view of future warfare.[29] The book looks at how new technologies might alter and how war and military operations are conducted. The complicated geopolitical interactions between the United States, China, and Russia are examined in the book. It explores the rising conflicts and rivalries over power, wealth, and controls that eventually resulting in a major war. The movie "Ghost Fleet" which was produced by keeping this book in the mind explicitly examines the advantages and risks of using cutting-edge military technology.

In this article, The Origin of Security Dilemma between China and US in Cyber Space, Li Senlin states that global phenomena are constantly emerging as a result of the significant changes in the post-Cold War global setting. As the cyberspace emerged, it became one of the five power spaces—along with the land, sea, air, and outer spaces—and inevitably turned into a battlefield for states. Nonetheless, the characteristics of virtual cyberspace differ from those of other entities. Thus, this research begins with outlining the current cyber security scenario that China and the US are facing; it verifies the type of cyber security difficulty that China and the US are confronting; and lastly identifies the factors that are driving these issues. In addition, the research makes recommendations for resolving the cyber security conundrum, such as the necessity of group security measures, enhanced network equipment performance and production, and greater openness in cyberspace.

[29] Connie Frizzell, "Ghost Fleet: A Novel of the Next World War, by P. W. Singer and August Cole," *Naval War College Review* 69: No. 3, (2016), https://digital commons.usnwc.edu/cgi/viewcontent.cgi?article=1172&context=nwc-review.

Enhancing cross-cultural communication and collaboration can help advance understanding between people and keep the internet from turning into an area of war.[30]

The paper US-China Technology Competition: Impacting a Rules-Based Order investigate the potential effects of the current international regulatory framework on the technological rivalry between the United States and China. The study is probably going to look at how technological developments, especially in fields like artificial intelligence, cybersecurity, telecommunications, and emerging technologies, have played a significant role in determining the dynamics of the US-China relationship.[31] The primary objective of the article is to evaluate the effects of the US-China technology competition on the current rules-based order including espionage activities and surveillance acts. Examining potential alterations in global power dynamics, the formation of new laws and regulations, and the possibility for the fragmentation or bifurcation of the global technological environment are a few examples of how this might be done.

Kai-Fu Lee, the author of AI Superpowers: China, Silicon Valley, and the New World Order, proposes an analysis of the dynamic nature of the US-China relationship in the age of artificial intelligence (AI) and how this will shape the future global order.[32] Lee provides an optimistic evaluation of China's potential in the AI race, emphasizing its abundant data resources and government policies that support its rise as an AI powerhouse, potentially surpassing the United States in terms of AI capabilities. Going beyond the rivalry between the two countries, Lee

[30] Li Senlin, "The Origin of Security Dilemma between China and US in Cyber Space," 2018, 995–99.https://webofproceedings.org/proceedings_series/ESSP/EREMS%202018/EREMS18211.pdf

[31] Hilary McGeachy, "US-CHINA TECHNOLOGY COMPETITION: IMPACTING A RULES-BASED ORDER," *UNITED STATES STUDIES CENTRE*, May 2019, https://publicsectornetwork.com/wp-content/uploads/2020/01/US-China-technology-competition-impacting-a-rules-based-order.pdf.

[32] Kai-Fu Lee, "Book Review: AI Superpowers - China, Silicon Valley, and the New World Order," Thinking Ahead Institute, September 25, 2018, https://www.thinkingaheadinstitute.org/research-papers/book-review-ai-superpowers-china-silicon-valley-and-the-new-world-order/.

underscores the broader societal implications of AI. He anticipates that the dominance of the United States and China in AI will exacerbate global inequality, consolidating power between these two nations. Additionally, he expresses concerns about the significant loss of jobs and the impact on individuals who not only face the loss of their livelihoods but also a sense of personal identity and purpose. Lee proposes that addressing these challenges necessitates more than simply implementing a universal basic income.

In the article, An Analysis of Cyberspace Rule-Making in China-U.S. Relations, Zhao GENG elaborates that China and the United States, two rising and established powers, respectively, have a significant influence on the growth of cyberspace. Using strong standards to impose behavioral restrictions on all international actors is the cornerstone of internet administration. As a result, developing cyberspace rules within mutually agreeable frameworks is vital for both China and the United States because it significantly impacts the US-China strategic relationship. Furthermore, the concepts of "a new type of major power relations" and "a community with a shared future for mankind" offer a theoretical framework for the development of regulations governing cyberspace. Negotiating narrow issues—what is sometimes referred to as a low-level path—can help to encourage the creation of norms in the short run. Over time, the enforcement of cyberspace norms will be facilitated by both formal mechanisms of mutual recognition, which may be viewed as a high-level path, and informal mechanisms, which can be thought of as a middle-level road. Additionally, "Track Two Diplomacy" and "Track 1.5 Diplomacy" are advantageous to the process of negotiating cyberspace regulations.[33]

[33] Zhao Geng, “An Analysis of Cyberspace Rule-Making in China-U.S. Relations,” *International Relations and Diplomacy* 6, no. 1 (January 28, 2018), https://doi.org/10.17265/2328-2134/2018.01.002.

The research paper, Why International Order in Cyberspace Is Not Inevitable published by Brian M. Mazanec, discusses establishment of standards, conventions, and guidelines for cyberspace will unavoidably involve major countries working together. Based on the premise that “great powers will have no choice but to cooperate and soften the hard impacts of multi-polarity and oligopolistic competition. They contend that such a result is unavoidable. The history of norm evolution for other emerging-technology weapons suggests that while it is true that more competition may produce incentives for collaboration on restricting norms, such an outcome seems implausible. According to Forsyth and Pope, governments would eventually succumb to restricting standards because cyber warfare presents such a wide range of difficulties. Conversely, norm evolution theory for warfare involving developing technologies leads one to believe that limiting norms for cyber warfare will be difficult, if not impossible. The history of norm evolution for other emerging-technology weapons suggests that while it is true that more competition may produce incentives for collaboration on restricting norms, such an outcome seems implausible.[34]

Written by Christian Ruhl, Duncan Hollis, Wyatt Hoffman, and Tim Maurer, the research paper in consideration, Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads, explores the complex relationship between geopolitics and cyberspace, with a particular emphasis on the evaluation of international cybersecurity norm procedures. The writers adeptly traverse the intricate domains of cyberspace and geopolitics, providing an all-encompassing examination of worldwide cybersecurity normative procedures. They investigate how state and non-state actors shape norms in the cyberspace and how those norms have evolved over time. Finally, the review highlights the article’s major insights and highlights how it advances knowledge of

[34] Brian M Mazanec, “Why International Order in Cyberspace Is Not Inevitable,” *Strategic Studies Quarterly*, 2015, 78–95. https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-09_Issue-2/mazanec.pdf

international cybersecurity standard procedures. Today, a number of organizations claim to be able to identify or operationalize different normative standards of behavior for states and/or other stakeholders in cyberspace. These organizations include the United Nations (UN) groups, the Open-Ended Working Group (OEWG) and the Group of Governmental Experts (GGE), expert commissions, industry coalitions, and multi-stakeholder collectives, such as the Paris Call for Trust and Security in Cyberspace and the Tech Accord.[35]

The chapter, Beyond Quasi-Norms: The Challenges and Potential of Engaging with Norms in Cyberspace by Toni Erskine and Madeline Carr, challenges the traditional notion of "quasi-norms" by examining the changing geography of norms in cyberspace. By providing a novel viewpoint on online norms, they add to the scholarly discourse and may even refute or build upon preexisting ideas. The chapter's distinctive contribution to the subject is assessed, emphasizing how it might influence conversations about policy and future study. The swift expansion of cyberspace has given rise to new protocols that deal with managing the global domain name system, negotiating content restrictions, managing personal networks, social media communication, coordinating online financial transaction protocols, anticipating, thwarting, and responding to cyber-attacks. The conflicts and contradictions between different value systems associated with globalized practices create an additional challenge in establishing norms in cyberspace. This challenge is further complicated by the ever-changing and unique nature of these evolving practices. For instance, conflicting views of the link between anonymity, openness, and privacy lead to tensions over varying notions of "security" in cyberspace. The review concludes by summarizing the major conclusions

[35] Christian Ruhl Maurer Duncan Hollis, Wyatt Hoffman, Tim, “Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads,” Carnegie Endowment for International Peace, February 26, 2020, https://carnegieendowment.org/2020/02/26/cyberspace-and-geopolitics-assessing-global-cybersecurity-norm-processes-at-crossroads-pub-81110.

and takeaways from the chapter, highlighting its significance for the larger conversation about internet norms.[36]

In an article, Power and diplomacy in the post-liberal cyberspace, André Barrinha, Thomas Renard states that there is a growing consensus that we have moved—or are moving—from an international liberal order to a new reality. It is debatable if the only differences in that reality are related to power dynamics or if institutions and ideals also have a role. In order to investigate how the post-liberal transition relates to cyberspace, this study draws on the expanding corpus of literature on post-liberalism. It examines the changing nature of power relations in cyberspace and the challenges faced by institutions, norms, and values. The development of cyber diplomacy as a result and reaction to the post-liberal shift is then examined in the study. Given that the liberal order gave rise to cyberspace, it will be claimed that cyber-diplomacy is a post liberal world order practice. The primary topics of discussion revolve around what it implies for the future of cyberspace, how it shapes a new order, and how it bridges political divides.[37]

In his article A Chinese Perspective on Ensuring Stability in the Digital World, Zhou Hongren explores the rise of two novel domains in global studies: international cyber management and the maintenance of strategic cyber equilibrium. The author identifies three broad degrees of stability in the digital realm: stable, delicately balanced, and unpredictable. Employing a cyclical approach, the article thoroughly investigates the progression of the digital landscape across these stages to deepen comprehension of cyber organization and facilitate well-informed decision-making. Within these

[36] Toni Erskine and Madeline Carr, "Beyond 'Quasi-Norms': The Challenges and Potential of Engaging with Norms in Cyberspace," 2016, 1–22.https://discovery.ucl.ac.uk/id/eprint/10054298/1/Beyond%20Quasi-Norms%20in%20Cyberspace_Preprint.pdf

[37] André Barrinha and Thomas Renard, "Power and Diplomacy in the Post-Liberal Cyberspace," *International Affairs* 96, no. 3 (May 1, 2020): 749–66, https://doi.org/10.1093/ia/iiz274.

frameworks, pivotal guidelines such as international standards, legislation, and regulations have been devised to serve as indispensable principles governing the behavior of individual nations in the digital sphere. The paper underscores that international cyber management is primarily concerned with overseeing the process of digital transformation and establishing robust institutions to prevent instability. Ensuring effective management of the strategic stability of the transformation cycle necessitates the establishment of resilient institutions, which in turn reinforce global cyber management. The international framework for cyber management must address three tiers of concern: safeguarding national cyber security, including the protection of critical infrastructure; promoting cyber arms control and crisis management among dominant cyber powers; and fortifying international norms and legislation. [38]

In an article, China and International Law in Cyberspace, Kimberly Hsu states that the Chinese government has expressed its commitment to cooperating with the "global community" in order to foster a tranquil, secure, accessible, and collaborative digital realm. Similarly, the official aim of the US government is to collaborate internationally to promote an accessible, interconnected, secure, and dependable cyberspace. While there are notable resemblances in the publicly stated intentions of both China and the US regarding international laws and internet norms, there are also significant disparities. It is worth mentioning that China participated in a 2013 UN report confirming the application of international laws to the digital realm. In 2014, the same UN organization will assemble to deliberate complex and contentious ideas such as state accountability and the use of force in the digital realm. Despite differing viewpoints on digital realm policies, a recent development within the United Nations emphasizes some fundamental points of concurrence. The

[38] Hongren Zhou, “Strategic Stability in Cyberspace: A Chinese View,” *China Quarterly of International Strategic Studies* 05, no. 01 (January 2019): 81–95, https://doi.org/10.1142/S2377740019500088.

UN Group of Government Experts (GGE) comprises national experts from fifteen countries, including China and the US, who have been chosen by the Secretary General to evaluate existing and potential risks in the cyber domain and suggest cooperative measures to address them.[39]

In an article, China's New Cybersecurity Law and U.S-China Cyber security, written by Liudmyla Balke states that concern over cybersecurity and misuse of cyberspace has grown both domestically and internationally. China and the United States have launched a number of cybersecurity plans in response to this problem. Regretfully, those tactics failed to get much traction. These two superpowers require a more workable, long-lasting plan. The economy of both China and the United States are harmed by security surveillance and cyber-warfare, which also jeopardizes the security of their IP networks. The online community draws attention to the fact that some national government policies may have a negative impact on a foreign country or its people. Because national government lacks sovereignty over another and the former's regulations will not apply to the latter's behavior. This highlights a serious weakness in international law and restricts what the United States or any other country can do in reaction to an aggressive strike by another country, like China, or vice versa. As a result, the article explores that China is unable to cut itself off from the outside world as it would want. A new approach would provide the US with a chance to enhance and concentrate on cybersecurity defenses, which would aid in the battle against cybercrimes and stop undesired cyber-attacks.[40]

[39] Kimberly Hsu, “China and International Law in Cyberspace,” *U.S.-China Economic and Security Review Commission Staff Repor,* May 6, 2014, 1–10.https://www.uscc.gov/sites/default/files/Research/China%20International%20Law%20in%20Cyberspace.pdf

[40] LiudmylaBalke, “China’s New Cybersecurity Law and U.S-China Cybersecurity Issues,” *Santa Clara Law Review* 58, no. 1 (June 4, 2018): 137. https://digitalcommons.law.scu.edu/lawreview/vol58/iss1/4/

The article, International Order Transition and US-China Strategic Competition in the Indo-Pacific written by Alum Kai and H. Feng revolves around the concept of evolving international order that rests upon the power, institutions and norms. According to the author, if two pillars of these three are challenged by any state, particularly China, the liberal order will see transition phase. Moreover, the author concludes that power shift is merely not a significant indicator of order change, but there should be constant threat to norms and institutions that maintain the liberal order, if China wants to change the liberal order in its favor. [41]

In an article, Technology, power, and uncontrolled great power strategic competition between China and the United States, the author Xiangning states that great power competition, once again, has become a salient feature of the global politics where China and US are at loggerheads. Activities of China as well as US are backlash to the liberal order in cyberspace. According to the author, the rules-based post-war international order is in decline and on the verge of internal breakdown, which is indicative of the rising global chaos. The author concludes that the United States has failed both economically and psychologically, to assume the responsibilities of global leadership.[42]

2.2) Theoretical framework

A complex interaction of geopolitical, economic, and technological elements characterizes the US-China strategic conflict in cyberspace. Both countries understand how crucial cyberspace is to economic growth, technical innovation, and national security. Sensitive information protection, economic espionage, and cybersecurity threats are the main causes of the competition. Regarding

[41] Kai He and HuiyunFeng, "International Order Transition and US-China Strategic Competition in the Indo Pacific," *The Pacific Review* 36, no. 2 (March 4, 2023): 234–60, https://doi.org/10.1080/09512748.2022.2160789.

[42] Xiangning Wu, "Technology, Power, and Uncontrolled Great Power Strategic Competition between China and the United States," *China International Strategy Review* 2, no. 1 (June 1, 2020): 99–119, https://doi.org/10.1007/s42533-020-00040-0.

cyber-attacks and intellectual property theft, the two nations have been exchanging allegations nonstop. As pioneers in cutting-edge technologies like 5G and artificial intelligence, the competition also involves influencing global norms and the digital sphere. Using the lens of social constructivism theory, the thesis "US-China Strategic Competition in Cyberspace: Normative Challenges to Global Order" sheds light on the normative aspects of the rivalry.

As a theoretical framework, social constructivism highlights how ideas, conventions, and common understandings shape international interactions. According to this theory, the norms and values surrounding cybersecurity, information sharing, and digital governance are socially constructed and open to interpretation in the context of the US-China cyberspace conflict.

2.2.1) Social Constructionism

A theoretical viewpoint, in sociology and other social sciences such as International Relations, called social constructionism basically emphasizes the part that social interaction and language play in the construction and upkeep of social reality. The social constructionism idea was first presented by Thomas Luckmann and Peter L. Berger in their book ‘’The Social Construction of Reality’’ in 1966.[43]

The idea is that people and cultures develop knowledge, meanings, and understandings of the world via interactions and shared interpretations rather than having these things naturally or objectively. Social constructionism mainly holds that reality is actively created through social processes rather than being merely discovered or determined by individuals. It implies that a variety of social elements, such as cultural norms, language, historical background, and power dynamics, have an

[43] Nickerson Charlotte, “Social Construction of Reality,” April 20, 2023, https://simplysociology.com/social-construction-of-reality.html.

impact on how we perceive the world. These elements influence our perceptions, assumptions, and interpretations, which eventually helps to build societal norms and common understandings.

2.2.2) Basic Principles of the Social Constructionism

Social constructionism in international relations is centered on the core principle that reality is not fixed or predetermined, but rather a result of human interaction, language, discourses, and shared meanings.[44] This perspective highlights the significant influence of ideas and discourses in shaping global politics, as actors use these tools to establish or challenge existing beliefs and norms.[45]

Norms and social practices play a central role in guiding the behavior of both state and non-state actors, evolving over time through interactions and socialization. Identity, in its various forms, profoundly impacts how actors perceive and respond to the world, influencing their interests and actions in international relations.

While social constructionism acknowledges the importance of structures and systems, it places emphasis on agency, emphasizing that actors have the ability to actively shape and modify these social constructs. This approach adopts an interpretive framework, recognizing the critical role of context, interpretation, and meaning-making in understanding international relations and the dynamic interplay of subjective factors in shaping the global political landscape.

[44] W. Detel, "Social Constructivism - an Overview | Science Direct Topics," International Encyclopedia of the Social & Behavioral Sciences, 2001, https://www.sciencedirect.com/science/article/abs/pii/B008043076701086X.

[45] Frank Fischer, "Constructing Policy Theory: Ideas, Language, and Discourse," in *Reframing Public Policy: Discursive Politics and Deliberative Practices*, ed. Frank Fischer (Oxford University Press, 2003), 0, https://doi.org/10.1093/019924264X.003.0002.

2.2.3) Theory Interpretation

It has already been discussed above that the study would reflect on the pinpoints and principles of constructivism and social constructionism. Constructivism refers to the idea that humans construct their own knowledge and reality. People who hold the social constructionist view, in contrast, contend that reality and knowledge are created via discourse. Constructivists concentrate on what goes on within each person's head or brain, whereas social constructionists concentrate on what goes on as people come together to form reality.

According to Guterman (2006), there are two viewpoints: Although both social constructionism and constructivism support a subjective view of knowledge, the latter places knowledge in the realm of social exchange while the former emphasizes individual’s biological and cognitive processes.

1. Vital Importance of Normality in Global Order

Norms have a significant impact on state behavior and interactions, which helps to shape global order, according to constructivism. A foundation for determining what is deemed acceptable or unacceptable in the international system is provided by norms, which are common ideas and values that direct state behavior. Though constructivism emphasizes the significance of ideas, identities, and social processes, realist approaches place more emphasis on material power. As a type of social currency in the context of international order, norms promote collaboration, lessen conflict, and give states a foundation for mutual understanding. States are social actors impacted by normative concerns in addition to being motivated by material interests, according to constructivist theory. States help to create a global order through mutual expectations, cooperative interactions, and the establishment of common laws and institutions as they adopt and uphold particular standards. Cyberspace norms are socially formed through continual processes of state-to-state negotiation, shared understanding, and dialogue rather than being predetermined. These principles form the foundation of a cooperative and stable international system, covering topics like cyber sovereignty, non-interference, and responsible state behavior in cyberspace. As a result, norms act as a social glue to hold states together and modify the changing makeup of the international system.

2. US-CHINA Strategic Competition in Cyberspace

Social constructivism illustrates how social constructions shape public discourse and governmental decisions regarding cyber activities –by taking the US-China strategic competition in cyberspace into consideration. Within this framework, the way cyber incidents are framed and cyber-attacks are attributed can be understood as socially constructed narratives that influence the strategic rivalry between China and the United States. Furthermore, the language employed in international forums and diplomatic communications reflects how the US-China cyber conflict is socially framed. Phrases like "information warfare," "cyber espionage," and "cybersecurity threat" are loaded with connotations that shape the problem. The concept of social constructivism challenges researchers to analyze the terminology used in debates about US-China cyber activity critically, as it shapes public perception, policy choices, and the general dynamics of the strategic competition in cyberspace.

3. China’s and United Stated of America actions in cyberspace present normative challenges to the global order

The claim that "Chinese espionage activities in cyberspace threaten global order" raises interesting questions about how common assumptions and conventions influence how people perceive and react to these kinds of operations, particularly from the perspective of social constructivism. The constructivist lens highlights how the idea that Chinese espionage poses a threat to the international order is socially produced through interactions, discourses, and interpretations within the international community rather than being an inherent or objective fact. The categorization of these actions as dangerous reflects the standards that are now in place about governmental conduct, cybersecurity, and sovereignty. As such, how common understandings and norms governing state behavior in cyberspace shape the reaction to Chinese espionage as well as US espionage activities in cyberspace domain. Social constructivism invites an investigation of the ways in which participants in the international system—China and other states among them—negotiate, challenge, or acquiesce to these standards, eventually shaping the perception of danger and its consequences for the larger international order in the cyberspace.

Social constructionism can be used to analyze the US-China strategic rivalry in cyberspace and how it poses normative challenges to global order. According to social constructionism, social interactions and processes impact how we perceive social norms, regulations, and threats in cyberspace. Both states actively create and interpret cyberspace in the context of the strategic rivalry between the US and China in order to forward their goals and narratives. The creation of threat perceptions is one facet of social constructionism in this battle. Each nation uses instances of cyber espionage, intellectual property theft, or disruptive cyber-attacks to paint the other as a potential threat in cyberspace. These actions are used to support their own cybersecuritypractices, defensive plans, and expenditures on cyber capabilities. Both countries- US and China- attempt to obtain legitimacy and support for their own positions by portraying the other as a danger to global order.

According to social constructionism, the perception and use of power in the strategic rivalry between the US and China are socially constructed. Although it is not tangible, power is created through discourses, acts, and interactions between the two nations. Through the structuring of actions, language, and symbolic representations by both the US and China, power relations in cyberspace are negotiated and built. For instance, the classification of specific cyber operations as "cyber espionage" or "cyber warfare" affects the perception of the rivalry and alters the power dynamics. The concept of social constructionism emphasizes that norms and regulations are socially produced and dynamic rather than absolute or universal. The development of what constitutes a normative order, rules controlling state conduct, and standards surrounding acceptable behavior are all socially negotiated and challenged in the setting of cyberspace. Discursive methods are employed by the United States and China to exert influence and challenge norms in the governance of cyberspace. These methods have a profound impact on shaping perceptions and constructing the global structure of cyberspace. From a social constructionist viewpoint, language is viewed as a transformative power that molds reality and beliefs. In the strategic conflict between the United States and China, both nations utilize discursive methods to create their own narratives, justify their actions, and weaken their opponents. They employ a variety of rhetorical strategies, such as presenting cyber operations as threats to national security or acts of self-defense, in order to achieve their desired results and gain support from domestic and international audiences. These methods significantly affect how cyberspace is perceived and contribute to the rise of challenges to the international order. Various means of communication, including formal and informal writings, speeches by leaders, traditional and innovative social media, and mainstream media, are used to transmit and shape this constructed reality.

The utilization of the theory of social constructionism to analyze the strategic cyberspace conflict between the United States and China illuminates the influence that power, norms, and online realities have on this clash. It emphasizes the significance of communication, individual agency, and social interactions in shaping power dynamics, influencing perceptions, and challenging the current framework. Acquiring a comprehensive comprehension of these social processes can offer valuable insights into the complexities and obstacles posed by this rivalry, and aid in the development of sophisticated strategies to address the global ramifications it entails.

To sum-up, the US-China strategic competition in cyberspace revolves around the construction of norms, particularly in the areas of disinformation and social engineering. Both countries are actively shaping the cyberspace to suit their interests. China practices cyber sovereignty, exerting state control over the internet and manipulating search results and websites accessed by its citizens. Similarly, the US engages in monitoring and surveillance, as evidenced by programs like Prism. Through artificial intelligence and software, individuals are influenced and constructed, leading to social engineering on a larger scale, ultimately impacting decision-makers and states. This constructivism in cyberspace transcends material considerations and directly influences global order, posing a challenge for each nation's approach to this competition.

CHAPTER 3

RESEARCH METHODOLOGY

This research is focused to analyze the competition in cyberspace, particularly between US and China, and how the activities and will to thrill in the cyber domain, with both legitimate as well as illegitimate ways, are posing normative challenges to the established global order. This chapter is aimed to address the choice of research methodology in order to collect the data and findings.

Furthermore, this chapter highlights the specific research designs and philosophical underpinnings of the research. Research Methodology can be defined as the general and careful study to investigate in the field of knowledge to establish a fact. Methods can be of three types: exploratory, explanatory, and descriptive. The research methodology used is explanatory and analytical. Different data collection methods, both primary and secondary, include interviews, surveys, and other investigative techniques that include current and historical information are used in this research study.

3.1) Research Ontology

The ontology of the research is often referred to understanding the being.[46] Questions like what is used. In ontological research reality and existence is investigated. There are multiple definitions for ontology. According to Oxford Dictionaries, it is the branch of philosophy which deals with the nature of existence. [47]Simply put, it is the study of existence and reality.

[46] Abdelhamid Ahmed, "Ontological, Epistemological and Methodological Assumptions: Qualitative Versus Quantitative," 2008, https://files.eric.ed.gov/fulltext/ED504903.pdf.

[47] Kristel Marie Pujanes, "Philosophy 101: The Six Branches of Philosophy," *The Quarter-Life Experiment* (blog), April 8, 2020, https://thebadbread.com/2020/04/08/philosophy-101-the-six-branches-of-philosophy/.

Its assumptions can take two stances: objectivism and constructionism. The assumptions of objectivism perpetuate that reality's existence is independent of our principles and should be observed directly and with accuracy. In objectivism, science is the key to understand reality and being. On the other hand, constructionism states that reality is subjective in nature.[48] There is no shared social reality and although external reality does exist, it is only known through human minds and meanings that are constructed. To understand reality, approximate observation is required, and the phenomena are constructed by social actors and are dynamic rather than static.

This study too is based on constructionism, as the military buildup, offensive defensive doctrines and ideological differences are made up by the policy makers of their respective countries and the concepts such as anarchy, security maximization are constructed. These policy makers are human beings, and their workings and decisions are based on perception, personal interests, and their understanding of the situation. The situation or events caused cannot be identified using objectivism. They are all social constructions invented by the human mind.

By applying constructionism as ontology, this study is aimed to analyze how social constructions and shared meanings influence and how the issue is understood and constructed, particularly in relation to the competition between Washington and Beijing in cyberspace and moral challenges to global order. According to constructionism, language, discourse, and collective interpretations are the different means through which society constructs reality. This research study examines the terminologies used by important players, decision-makers, and the media in relation to the cyberspace strategic competition between the US and China. Determine the essential phrases, analogies, and stories that help to explain the significance of cyber-activity and how it affects world

[48] Lowell Yarusso, "Constructivism vs. Objectivism," *Performance + Instruction* 31, no. 4 (1992): 7–9, https://doi.org/10.1002/pfi.4170310404.

order. Additionally, this study examines how the public's view of cyber-threats is shaped by the media, official reporting, and international organizations. According to constructionism, these perceptions are socially produced interpretations rather than actual realities.

3.2) Research Epistemology

Research epistemology refers to the branch of philosophy that explores the nature, methods, and scope of knowledge and how it is acquired in the context of research.[49] It deals with questions such as how knowledge is generated, what counts as valid evidence, and what criteria are used to evaluate the truth or validity of claims made in research.

Epistemology, in general, is concerned with understanding the nature of knowledge and how it is justified. In the context of research, epistemology examines the underlying assumptions, theories, and methodologies that shape the process of inquiry and the production of knowledge. Its assumptions can take two stances: Positivism and Interpretivism.

Interpretivism/Constructivism: These epistemologies emphasize the subjective and contextual nature of knowledge. They argue that individuals construct their own understanding of the world based on their experiences and social interactions. Interpretivism focuses on understanding and interpreting the meanings behind human actions and behaviors, often using qualitative research methods. [50]

[49] Matthias Steup and Ram Neta, "Epistemology," in *The Stanford Encyclopedia of Philosophy*, ed. Edward N. Zalta and Uri Nodelman, Spring 2024 (Metaphysics Research Lab, Stanford University, 2024), https://plato.stanford.edu/archives/spr2024/entries/epistemology/.

[50] HusamHelmiAlharahsheh and Abraham Pius, "A Review of Key Paradigms: Positivism VS Interpretivism," *Global Academic Journal of Humanities and Social Sciences*, Global Academic Journal of Humanities and Social Sciences, June 30, 2020, 39–43.

The epistemology used for the study is based on Interpretivism. Since Interpretivism is subjective in nature, it helps in understanding the interaction between the social world and the researcher. The researcher has understood the beliefs of the scholar and people by utilizing different internal and external files under a topic. This study is also based on the assumptions that reality and knowledge exist in this world and this reality is merely constructed by the human minds. Only the interpretation and understanding of the social world can help in gaining knowledge and experience of reality.

The application of Interpretivism as an epistemology to the study of "US-China Strategic Competition in Cyberspace and Normative Challenges for Global Order" entails taking a viewpoint that prioritizes the significance of comprehending the meanings that individuals and groups assign to their experiences, as well as the subjective interpretation of social phenomena. Interpretivism, which emphasizes the investigation of meanings, values, and viewpoints, is frequently linked to qualitative research techniques. By using Interpretivism as epistemology, this study is aimed to explore how different actors, particularly US and Chinese stakeholders, interpret and frame issues related to the cyberspace competition, norms and global order.

3.3) Research Approach

The research approach outlines the designs used for the study. Inductive and deductive approaches are the two focal approaches used to discover the truth. The inductive approach is about the development of the theory and that is achieved through observation.[51] For the use of this approach qualitative data is used. On the other hand, the deductive approach deduces conclusions based on pre-defined theory.

[51] David R Thomas, “A General Inductive Approach for Qualitative Data Analysis,” School of Population Health, University of Auckland, 2003, 2–9.

Deductive Approach: Starting from a basic theory or hypothesis, the deductive approach applies logical reasoning to produce particular predictions or hypotheses that may be verified by empirical observation.[52] It follows a top-down approach, moving from general to specific. The process typically involves the following steps:

- Start with a theory or existing body of knowledge
- Formulation of a hypothesis or prediction based on the theory
- Designing a research plan or study to test the hypothesis
- Collection of data and analyze it to either support or refute the hypothesis
- Draw conclusions based on the results

This study employs deductive approach for its conduct. Since the approach begins with a hypothesis and after thorough observation of the data, conclusions are drawn. Through a proper reasoning process, abstract and theoretical proposals are converted into concrete date. The study analyzes events and scenarios and aims to discover new knowledge. Since a theory is already established to explain the competition between China and United States in cyberspace and how it poses normative challenge to global order, final conclusions are drawn through proper observations, perceptions of people and explanation of the events. “US-China Strategic Competition in the Cyberspace: Normative Challenges to Global Order" is a research study which employs a deductive technique which begins with a theoretical framework and followed by testing hypothesis. The main variables, including US and Chinese actions in cyberspace, international norms, and threats to the global order, are unambiguously defined in this research paper. Drawing results from the analysis, this study

[52] Soung Min Kim, “Inductive or Deductive? Research by Maxillofacial Surgeons,” *Journal of the Korean Association of Oral and Maxillofacial Surgeons* 47, no. 3 (June 30, 2021): 151–52, https://doi.org/10.5125/jkaoms.2021.47.3.151.

examines how the competition between the Washington and Beijing in cyberspace shapes global norms and how this influences global order.

3.4) Research Strategy

A Research strategy is important in giving direction to the study and aids in selecting a proper approach for data gathering.[53] Research strategies are categorized into two types: one of them is qualitative research and other is quantitative research. Qualitative research involves collecting and analyzing data which is descriptive in nature. This type of research helps in understanding concepts and can be used to gather insights and generate new knowledge for the research. Qualitative research also uses observation as a useful technique for data collection. The opposite of qualitative research is quantitative research. Quantitative research deals with data in the form of numerical and uses mathematical operations during the conduct of the research.[54]

The reason to use qualitative research for the study is because the study is aimed to explain the case study in depth. Moreover, comparative case study is used to focus on the US-China competition in cyberspace and how it poses normative challenges to the global order. Utilizing a case study approach, the study "US-China Strategic Competition in Cyberspace and Its Normative Challenges to Global Order" entails a thorough, qualitative examination of particular situations or instances within the larger framework. This study finds situations that are pertinent to the US-China cyberspace competition and that illustrate significant incidents, events, or dynamics. Cases may

[53] Jenny, "Phase #2: Clearly Define Your Research Strategy," *MacKenzie Corporation* (blog), March 27, 2014, https://www.mackenziecorp.com/phase-2-clearly-define-research-strategy/.

[54] Sharique Ahmad et al., "Qualitative v/s Quantitative Research" 6 (October 28, 2019): 2828–32, https://doi.org/10.18410/jebmh/2019/587.

involve particular cyber-attacks, diplomatic discussions, choices about policy, or reactions from other countries.

3.5) Research design

An outline or framework for conducting a research study is referred to as a research design. Its objective is to answer the research questions or testing the validity of hypotheses by describing the strategy and techniques that will be applied to data collection and analysis.[55] It can be of three types: exploratory, explanatory, and descriptive.

a. **Descriptive Research**: The descriptive research design describes a phenomenon and its characteristics. Instead of studying why or how the phenomenon occurs, it seeks to understand what it is.[56]As a result, it only summarizes the topic of the research without explaining why it occurs.
b. **Exploratory Research**: Exploratory research is a research design employed when the research problem is undefined or unclear. It aims to provide researchers with a deeper understanding of the study problem[57]and its surrounding context before undertaking further research
c. **Explanatory Research:** Explanatory research utilizes the existing limited knowledge to examine the reasons behind a particular occurrence. [58] They contribute to a deeper comprehension of a specific subject; uncover the mechanisms or factors driving a particular

[55] Harish Thakur, "Research Design," 2021, 175, https://www.researchgate.net/publication/353430802_Research_Design.

[56] Eunsook T. Koh and Willis L. Owen, "Descriptive Research and Qualitative Research," in *Introduction to Nutrition and Health Research*, ed. Eunsook T. Koh and Willis L. Owen (Boston, MA: Springer US, 2000), 219–48, https://doi.org/10.1007/978-1-4615-1401-5_12.

[57] Richard Swedberg, "Exploratory Research," in *The Production of Knowledge: Enhancing Progress in Social Science*, ed. Colin Elman, James Mahoney, and John Gerring, Strategies for Social Inquiry (Cambridge: Cambridge University Press, 2020), 17–41, https://doi.org/10.1017/9781108762519.002.

[58] Muhammad Hassan, "Exploratory Vs Explanatory Research - Research Method," November 1, 2023, https://researchmethod.net/exploratory-vs-explanatory-research/.

phenomenon, and enable predictions about future outcomes. These studies follow a chronological order, requiring the cause to precede the effect

The best study design is an explanatory one since it enables researcher to delve deeply into the causes, motivation, and processes of US-China strategic competition in cyberspace and its effects on international/global norms. As Explanatory research goal is to identify causes and effects. In this research, it can help uncover why China's activities in cyberspace are posing normative challenges to the global order, how these challenges manifest, and what outcomes they have on international relations.

With regard to the competition between US and China in cyberspace and its normative challenges to global order, an explanatory research study employing qualitative methods is being conducted, with an emphasis on examining the nuanced details and contextual elements that underpin the phenomena that are being observed. In-depth information is gathered through case studies of particular cyber events, content analysis of diplomatic communications, and qualitative interviews.

3.6) Time Horizon

Within the framework of a research study, the time horizon denotes the duration of the study and establishes the temporal context of the research.[59]A crucial component of research design, the selection of a time horizon affects the study's depth, profoundness, and relevance

There are two common kinds of time horizons in research:

[59] Zain Alamgeer, "Time Horizon in Research Onion," *THE INNOVIDEA* (blog), September 14, 2023, https://theinnovidea.com/time-horizon-in-research-onion/.

a. Cross-Sectional Time Horizon:

A cross-sectional study is carried out during a very brief time period or at a single point in time.[60] It offers a glimpse into a certain occurrence at one point in time. It is useful for investigating connections or traits that exist at a specific moment in time.

b. Longitudinal Time Horizon:

Gathering data for a longitudinal study requires a lengthy time frame. It makes it possible for academics to track advancements, trends, or changes across time.[61]It is helpful in comprehending the patterns, dynamics, and development of a phenomenon.

I have applied longitudinal time horizon on the research study, US-China strategic competition in cyberspace and normative challenges to global order, because this study employs the involvement of the historical events, incidents as well as contemporary cyberspace activities. Furthermore, patterns and causal links that might not be obvious in a snapshot study might be found using the longitudinal approach. This study sought to investigate how particular events or policy choices affected the strategic competition's course and how that affected international norms.

3.7) Data Collection

The procedure of obtaining information or data to address research questions, examine trends, or obtain understanding of an issue is known as data collection. Various methods and techniques are employed to collect data, depending on the research objectives, the nature of the research field, available resources, and ethical considerations. Qualitative research relies on a variety of sources to

[60]Julia Simkus, "Cross-Sectional Study: Definition, Designs & Examples," *Simply Psychology* (blog), July 31, 2023, https://www.simplypsychology.org/what-is-a-cross-sectional-study.html.

[61] Derek Jansen, "What Is A Longitudinal Study? A Simple Definition," *Grad Coach* (blog), June 2020, https://gradcoach.com/what-is-a-longitudinal-study/.

gather rich and detailed data that helps researchers to explore and understand complex phenomena. The sources commonly used in qualitative research include: Primary source and Secondary source.[62]

Sources of data in research refer to data that has already been collected, compiled, and published by someone else or for a different purpose. These sources provide researchers with pre-existing data that can be used to address their research questions or explore new perspectives.[63]Common examples of secondary sources of data include: Published Research Studies, Government and Official Reports

To obtain appropriate information for the study on US-China Strategic Competition in Cyberspace and its Normative Challenges to Global Order, a variety of primary sources as well as secondary sources are given consideration. Both governments have published papers, statements, and policies that are used in this research study to provide light on their respective plans and activities in cyberspace. To gather further information, I have also conducted interview with important stakeholders, including legislators, government officials, cyber security specialists, and representatives of foreign organizations.

I. Sampling Technique

In order to draw statistical conclusions about a population, a subset of elements from the wider population are chosen using sampling techniques.[64]Samplings play a crucial role in the study design of quantitative research, impacting the findings validity and generalize ability.

[62] Syed Muhammad Kabir, "METHODS OF DATA COLLECTION," 2016, 201–75, https://www.researchgate.net/publication/325846997_METHODS_OF_DATA_COLLECTION.

[63]Tesfaye Boru, *CHAPTER FIVE RESEARCH DESIGN AND METHODOLOGY 5.1. Introduction Citation: Lelissa TB (2018); Research Methodology; University of South Africa, PHD Thesis*, 2018, https://doi.org/10.13140/RG.2.2.21467.62242.

[64]AshishGulati, "What Are Sampling Techniques? Different Types and Methods," knowlegehut, September 7, 2023, https://www.knowledgehut.com/blog/data-science/sampling-techniques.

a. Quantitative Sampling Technique

In order to collect numerical data for statistical analysis, quantitative sampling procedures entail the methodical selection of a subset of people or elements from a broader population.[65] To enable researchers to draw trustworthy statistical conclusions, quantitative sampling aims to guarantee that the sample chosen accurately reflects the features of the total population.

b. Qualitative Sampling Technique

In order to ensure the depth and richness of data acquired, qualitative research uses particular sampling strategies. Choosing people from a population using subjective standards as compared to random selection is known as non-probability sampling.[66] This form of data collection is rapid, easy, and economical because it does not require a lengthy survey frame.

Purposive sampling is one such strategy. Researchers intentionally choose individuals for purposive sampling based on their possession of particular traits or experiences that are pertinent to the study topics. Participants will be able to offer in-depth insights because this method enables a targeted investigation of specific occurrences. Snowball sampling is an additional qualitative sampling method in which the original participants find and recommend other people who have comparable traits or experiences. When researching hard-to-reach populations or specialist communities, this strategy is especially helpful. While purposive sampling provides depth and focus, snowball sampling makes it easier to include people who might be difficult to identify using traditional methods. Both methods

[65] MdRahman et al., “Sampling Techniques (Probability) for Quantitative Social Science Researchers: A Conceptual Guidelines with Examples,” *SEEU Review* 17 (June 1, 2022): 42–51, https://doi.org/10.2478/seeur-2022-0023.

[66] JaskoMahmutovic, “What Is Non-Probability Sampling? | SurveyLegend,” Survey legend, February 8, 2023, https://www.surveylegend.com/sampling/non-probability-sampling/.

stress how crucial it is to choose participants who are relevant to the study's goals in order to enhance the process of gathering qualitative data.[67]

I have used Purposive sampling technique to collect the data**.** I have used deliberately select participants who possess specific characteristics or experience relevant to the research question. I have used this sampling technique to gain in-depth insights from the erudite scholars who have unique perspective and expertise.

3.8) Data Analysis

Data analysis, as used in research technique, is the methodical evaluation and scrutiny of gathered data in order to identify trends, reach conclusions, and deduce implications regarding the study questions or hypotheses. Enriching the overall understanding of the research problem, it is an essential phase in the research process that converts unprocessed data into digestible insights. Depending on the research objective and the type of data, many methodologies can be used for data analysis and data interpretation.

Qualitative Data Analysis: Finding patterns, themes, and insights in non-numerical data—such as text, photos, audio, or video—requires a methodical examination and interpretation process known as qualitative data analysis.[68] It is frequently employed in research approaches that center on comprehending the underlying contexts, meanings, and complexity of occurrences. Through the use of methods like content analysis, grounded theory, and thematic analysis, researchers can examine

[67] Grace Njeri-Otieno, “Sampling Strategies for Qualitative Research,” *Resourceful Scholars’ Hub* (blog), September 8, 2021, https://resourcefulscholarshub.com/sampling-strategies-for-qualitative-research/.

[68] Abdelhamid M. Ahmed, “Ontological, Epistemological and Methodological Assumptions: Qualitative Versus Quantitative,” *ERIC*, April 8, 2008, https://www.researchgate.net/publication/267736833_Ontological_Epistemological_and_Methodological_Assumptions_Qualitative_Versus_Quantitative.

the depth and variety of qualitative data, identify significant trends, and produce insightful interpretations.

There are further types of the Qualitative Data Analysis that can be described as following:

i. Thematic Analysis**:** Finding and analyzing themes, patterns, and trends in qualitative data is known as thematic analysis. [69] Data coding is employed in this procedure to locate recurrent themes, arrange them into a logical framework, and then analyze the results.

ii. Content Analysis: The systematic process of looking through textual or visual data to identify themes, patterns, and interpretations is called content analysis.[70]This data analysis technique uses coding and categorization based on established criteria or creates categories as it goes along.

iii. Narrative Analysis: This method of analyzing and interpreting narrative data—which includes stories, interviews, and other written or spoken materials—is called narrative qualitative data analysis.[71]Grasping the themes, patterns, and meanings woven throughout the stories is the main goal of this approach.

I have applied thematic data analysis technique in which following the collection of data, a methodical coding process takes place in which important terms, assertions, or passages pertaining to the cyber competition between the US and China and its effects on international norms are recognized and assigned descriptive codes. On the basis of recurrent themes and commonalities, these codes are then arranged. Making sure these themes encapsulate the core of the data requires further refining and

[69]Gery Ryan and H. Bernard, "Techniques to Identify Themes," *Field Methods - FIELD METHOD* 15 (February 1, 2003): 85–109, https://doi.org/10.1177/1525822X02239569.

[70] Linda Haggarty, "What Is Content Analysis?," *Medical Teacher* 18, no. 2 (January 1, 1996): 99–101, https://doi.org/10.3109/01421599609034141.

[71] prakash.srivastava, "Narrative Analysis: Methods and Examples," Harappa, October 4, 2021, https://harappa.education/harappa-diaries/narrative-analysis-in-qualititative-research/.

definition. The final themes are developed by an iterative process of review and revision, providing a thorough grasp of the normative issues raised by the strategic conflict between the US and China in the internet domain and its consequences for the international order. The topics include things like tensions and conflicts about sovereignty, tense diplomatic relations, technical espionage, and how international institutions shape.

3.9) Research Ethics

Research ethics are the code of conduct that a researcher must acknowledge and work within the limits of the rules described by the institution. Research ethics are aimed at protecting the researched material from any harm. In short, they are aimed to ensure legitimacy of the research.

The ethical considerations undertaken for my study will be following:

1) The study has been conducted according to the rules and guidelines published under Bahria University.

2) The study has been completed without any aid from a ghost writer.

3) The work is not plagiarized, and sources used in the study are properly referenced.

4) Citations have been reviewed personally.

5) Data and findings are not fabricated; rather they are original and real.

6) The study is not biased.

7) Whereas the sole purpose of the study is to give new insight to the topic.

CHAPTER 4

DATA ANALYSIS / RESULTS/ FINDINGS

4.1) US-China Strategic Competition in Cyberspace: Origin and Contemporary Conflicts

United States and China are the prominent global leaders in cyberspace and information system.[72] China is swiftly overtaking the United States of America as the unchallenged and inevitable global leader in cyber security owing to its huge potential for human as well as financial resources in cyberspace. Ever since the onset of the twenty-first century, both states have leveled allegations against one another for engaging in financial gain-oriented cyber-espionage and cyber-attacks. Similar allegations against US intelligence have been hurled by China, while the US has emphasized that the PLA, China's Military, is primarily responsible for organizing cyber-attacks. However, efforts to coordinate policies in the sector have not prevented tensions over cyber-building between resurgent China and hegemon United States and resultantly tensions are rising in the cyber domain.

Furthermore, politically driven pressures on information systems have been the focus of cyber-attacks since the start of the year 2020. From routine cyber espionage to pursuing political and security objectives, Washington observes a shift in China's aggressive tactics. Furthermore, the PLA has given China's security structures rigorous control over the origins of cyber-threats. Furthermore, China alleges that the US is employing cyber-threats in the weapons competition and cyber-influences to expand global hegemony. These remarks are made by Beijing in support of its own multipolar global strategy based on the equal representation of the emerging powers, which is basically

[72] Kenneth Lieberthal and Peter W. Singer, "Cybersecurity and U.S.-China Relations," Brookings, February 23, 2012, https://www.brookings.edu/articles/cybersecurity-and-u-s-china-relations/.

challenged by the Joe Biden administration by making efforts to fortify Western nations against Chinese cyber-attacks.[73]

In light of these two leading statecrafts' statements, cyber security is becoming a more significant topic in US-China relations. Every one of these basically employs cyber tools as a source of cyber influence and cyber tactics to advance their national goals in order to get involved in partner relationship-level strategic communication. Consequently, these issues—particularly the application of cyber illegitimate activities, from both sides, in cyberspace — impact the stability of the global order by posing normative challenges to it.[74]

4.2) Cyber-Attacks from US on China in Contemporary Era:

Cyber specialists Valeriano and Maness state that the employment of aggressive and destructive intelligence techniques to steal, alter, or destroy data in the cyber sphere is known as cyber espionage. China's prowess in taking advantage of holes in the US cyber-defense system allows it to avoid direct conflict in another area of cyberspace. Depending on the goal, cyber-espionage can be utilized for a long or short period of time.[75] According to covert acts, ‘’In order to either get access or just provide a vague indication of resolution, the short-term strategic calculus is tweaked."[76]Over an extended period, espionage aims to achieve a dominant status of economic, political and military power by manipulating the information landscape.

[73]Michael Kolton, “Interpreting China’s Pursuit of Cyber Sovereignty and Its Views on Cyber Deterrence,” *The Cyber Defense Review* 2, no. 1 (2017): 119–54.

[74]Scott Harold, Martin Libicki, and Astrid Cevallos, *Getting to Yes with China in Cyberspace* (RAND Corporation, 2016), https://doi.org/10.7249/RR1335.

[75]Brandon Valeriano and Ryan C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (Oxford University Press, 2015), https://doi.org/10.1093/acprof:oso/9780190204792.001.0001.

[76] Kurt Baker, “What Is Cyber Espionage? – CrowdStrike,” *Crowdstrike.Com* (blog), February 28, 2023, https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/.

Between 1989 and 2016, there was a period of more engagement and communication between China and the US, marked by the US maintaining a foreign policy that was largely stable and consistent. First signs of a change were brought to the Obama administration when China put up the idea of a new form of major power interaction.[77]

Barak Obama's administration acted cautiously in response to the China's plans of active interaction with the major powers. But during his second term in office[78], it became increasingly clear that the proposal had been flatly rejected, and Differences between the two nations on issues such as trade deficits, cyber-attacks, and the militarization of the South China Sea began to impact the nature of the bilateral relationship. Politicians and other high-ranking officials' rhetoric and behavior both reflect the current tension. American hostility toward China is primarily caused by their perception of a challenge to their interests and American values, which is stoked by China's increasing military and technological might as well as the Communist Party's expanding economic and social influence. China's growing cyber rivalry has prompted the US government to devise new measures, especially in operations involving cyber- and artificial intelligence. On the other hand, China alleges US of espionage activities to put Chinese cyber national interests into turmoil.

China says that "U.S. cybercriminals" broke into a Wuhan earthquake monitoring system. According to Chinese official media, the application was compromised to include a backdoor that could be used to steal seismic data.[79]Additionally, China also alleged the US National Security Agency (NSA) of

[77] Chen Weihua, "Developing a New Type of Major Power Relationship Between China and the U.S.," (China Daily), China-US Focus, March 24, 2017, https://www.chinausfocus.com/foreign-policy/developing-a-new-type-of-major-power-relationship-between-china-and-the-u-s.

[78] Wu Xinbo, "Beijing's Wish List: A Wiser China Policy in President Obama's Second Term," Brookings, December 11, 2012, https://www.brookings.edu/articles/beijings-wish-list-a-wiser-china-policy-in-president-obamas-second-term/.

[79] Liu Zhen, "Were China's Earthquake Tracking Stations Hacked for Military Secrets by US?," South China Morning Post, July 28, 2023, https://www.scmp.com/news/china/diplomacy/article/3229258/were-chinas-earthquake-tracking-stations-hacked-military-secrets-us.

conducting several cyber-attacks against Northwestern Polytechnic University in China. Authorities assert that after breaking into digital communications networks, the NSA stole user data.[80]

According to the famous Global Times report, the government, financial institutions, scientific research centers, communications providers, the military, the aerospace industry, the education sector, and the medical field were among the prime targets that the NSA orchestrated attacks on in China. [81]Expert also said that the attack has been carried out against 403 targets worldwide mainly targets were the Western European states including Germany, UK, France and South Korea, Japan, and Iran in Asia, based on the FOXCID server names provided in classified NSA papers.[82]

Amid growing geopolitical tensions between the two states, China's Ministry of State Security (MSS) has accused the US of getting into Huawei's servers since 2009, obtaining sensitive data, and installing backdoors. [83] Furthermore, the government authority claimed in a We Chat message that US intelligence agencies have "done everything possible" to use a "powerful cyber-attack arsenal" to spy on, steal secrets from, and infiltrate other countries, including China. Information on the purported hacks was kept private.

The statements further claimed that the National Security Agency (NSA) Computer Network Operations had targeted China specifically with repeatedly carried out systematic and platform-based attacks in an attempt to steal the state's important data resources. According to statista report, in 2022,

[80] Zhao Siwei, "Exclusive: Report Reveals How US Spy Agencies Stole 97b Global Internet Data, 124b Phone Records in Just 30 Days - Global Times," Global times, June 13, 2022, https://www.globaltimes.cn/page/202206/1268024.shtml.

[81] Fan Lingzhi, Cao Siqi, and Liu Caiyu, "Exclusive: China a Main Target of US NSA Cyberattacks, with Key Infrastructure under Threat - Global Times," Global times, March 2, 2022, https://www.globaltimes.cn/page/202203/1253697.shtml.

[82] "US's Most Powerful Cyberattack System Is Targeting China: Sources," 癸卯年腊月十一 People's Daily, March 22, 2022, https://peoplesdaily.pdnews.cn/tech/er/30001213112.

[83] CHENG TING-FANG and CISSY ZHOU, "China Accuses U.S. of Hacking Huawei Servers since 2009 - Nikkei Asia," September 20, 2023, https://asia.nikkei.com/Spotlight/Huawei-crackdown/China-accuses-U.S.-of-hacking-Huawei-servers-since-2009.

China recorded more than 342 thousand cyber -attacks. 850 billion dollars were spent that year on internet offenses.[84]By 2028, the calculations indicated that the expenses would have reached 4.5 trillion dollars.

In a nutshell, China, in geostrategic competition with US, has been accusing the US for all the cyber-attacks particularly cyber-espionage activities which it has been facing since the onset of 21st century.

4.3) China's Acts of Espionage in Cyberspace Against US

China has proven to be a highly persistent nation with advanced cyber capabilities with key infrastructure under threat –as Global Times views the sheer volume of espionage and attacks the nation has carried out.[85] National Counterintelligence Executive documents have been released criticizing China's cyber-espionage, describing it as a strategic threat to American interests. Using computer networks as a strategy to seize information dominance early in a military operation has become a fundamental part of PLA strategic campaign goals, according to the U.S.-China Economic and Security Review Commission.[86]China's data collection efforts appear to be directed toward obtaining trade secrets (commercial, military, proprietary, etc.) and other information that will enhance the country's technological prowess, military power, and other economic facets.

According to the 2023 Annual Danger Assessment by the Office of the Director of National Intelligence, China poses an immediate cyber threat to the US. China is undoubtedly the biggest, most active, and most ongoing cyber espionage threat at the moment for networks used by the US

[84] Daniel Slotta, "China: Number of Recorded Cyber Attacks 2022," Statista, August 21, 2023, https://www.statista.com/forecasts/1398710/china-number-of-recorded-cyber-attacks.

[85]Nicholas Yong, "Industrial Espionage: How China Sneaks out America's Technology Secrets," *BBC News*, January 16, 2023, sec. China, https://www.bbc.com/news/world-asia-china-64206950.

[86]"China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States," U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION, February 17, 2022, https://www.uscc.gov/hearings/chinas-cyber-capabilities-warfare-espionage-and-implications-united-states.

government and corporations.[87] China's active cyber operations and its export related to industry and technologies make the United States more vulnerable to such operations.

U.S. officials and industry security officials claim that the Chinese military is increasing its capacity to interfere with vital American infrastructure, such as communications and transportation networks, power and water utilities, and transportation systems. According to these specialists, within the past year, hackers connected to PLA have gained access to the computer networks of almost two dozen crucial organizations. According to them, these incursions are a part of a larger attempt to devise strategies meant to induce fear and bewilderment or impeding operations in the future event of a potential clashes in the Pacific region between the Washington and Beijing. A well-known port on the West Coast, and a water utility, an oil and gas pipeline in Hawaii are a few of the targets impacted. In addition, the hackers tried to compromise the Texas power grid operator, which operates independently of the country's electrical grid.[88]

The Chinese government is actively trying to disrupt vital infrastructure, according to Brandon Wales, executive director of the Department of Homeland Security's Cyber Security and Infrastructure Security Agency (CISA). Their aim is to position themselves in a way that allows them to potentially destroy or disrupt this infrastructure in the event of a conflict.[89]This could be done to hinder the United States from projecting power in the Asian region or to generate social unrest within the U.S., ultimately influencing the decision-making process during times of crisis. This is a big shift from the

[87] Anthony H. Cordesman, "The 2023 Edition of the Annual Threat Assessment of the U.S. Intelligence Community," Center for Strategic and International Studies, March 13, 2023, https://www.csis.org/analysis/2023-edition-annual-threat-assessment-us-intelligence-community.

[88] Ellen Nakashima and Joseph Menn, "China's Cyber Intrusions Have Hit Ports and Utilities, Officials Say - The Washington Post," The washington post, December 11, 2023, https://www.washingtonpost.com/technology/2023/12/11/china-hacking-hawaii-pacific-taiwan-conflict/.

[89] https://www.meritalk.com/articles/cisas-wales-us-needs-better-cyber-resilience-facing-china/

seven to ten years ago, when China's cyber activity was mainly focused on economic and political espionage. Additionally, the director of the National Security Agency's Cyber-security Collaboration Center, Morgan Adamski[90], verified through email that Volt Typhoon, a virus, activity seems to be focused primarily on targets within the Indo-Pacific region."

According to recent Pentagon study on Chinese military might, China's cyber capabilities are a bigger threat to US interests now. Even worse, the paper claims that the CCP has already shown a readiness to project power using its resources. Furthermore, the report highlights that China engages in the intellectual property theft and stealing of sensitive data from academic, economic, military, and political entities. Through this illicit activity, the Chinese Communist Party gains extensive knowledge about U.S. defense networks, deployments, logistics, and associated military capabilities.[91] The report cautions that China employs cyber methods to infiltrate and acquire sensitive information, with the aim of obtaining economic and military advantages.

Furthermore, according to Brandon Wales, the executive director of the Cyber-security and Infrastructure Security Agency (CISA), China is the United States' greatest geostrategic challenge, both broadly and then absolutely within the cyber realm. The Department of Defense issued a warning in the October 2022 report to Congress, which examined China's military and security activities throughout the year. The hackers from China are allegedly stealing "sensitive information from the critical defense infrastructure and research institutes" and have targeted U.S. government systems, including the department itself. The report highlighted three possible reasons for China's strike

[90] Nir Kshetri, "Cybercrime and Cyber-Security Issues Associated with China: Some Economic and Institutional Considerations," *Electronic Commerce Research* 13, no. 1 (March 2013): 41–69, https://doi.org/10.1007/s10660-013-9105-4.

[91] Krystal Bermudez, "Defense Department Report Highlights Cyber Threat from China," FDD, November 6, 2023, https://www.fdd.org/analysis/2023/11/06/defense-department-report-highlights-cyber-threat-from-china/.

preparations: economic and military advantage and possibly for cyber-attack preparations.[92]Chinese hackers have created tools to target vital US infrastructure in times of conflict like the interruption of a pipeline carrying natural gas.

Wales's view is supported by a number of recent assessments from the American defense and intelligence communities. According to the Defense Department's report to Congress in October 2022, Beijing's main objective is to exert significant and disruptive impacts with the intention of influencing military operations and decision-making throughout the entire duration of a conflict, starting from its initiation until its resolution. In a separate statement, China asserts these capabilities are even more potent when used against information-technology-dependent militarily superior enemies.[93]

China-based hackers not only target the United States but also extend their espionage efforts to encompass its allies, showcasing the wide-ranging nature of their operations. Palo Alto Networks, a cyber-security company, revealed in October 2022, for instance, that hackers with Chinese origins had obtained entry to over two dozen government agencies in Cambodia across important industries.[94]The hacking, it was alleged, is in line with China's geopolitical objectives, which include projecting power and expanding naval operations in the area by taking advantage of their close ties to Cambodia.

[92]Alyza Sebenius, "China's Hackers Are Expanding Their Strategic Objectives," LAWFARE, Default, December 5, 2023, https://www.lawfaremedia.org/article/china-s-hackers-are-expanding-their-strategic-objectives.

[93]"DOD Releases 2023 Report on Military and Security Developments Involving the People's Repu," October 19, 2023, https://www.defense.gov/News/Releases/Release/Article/3561549/dod-releases-2023-report-on-military-and-security-developments-involving-the pe/https%3A%2F%2Fwww.defense.gov%2FNews%2FReleases%2FRelease%2FArticle%2F3561549%2Fdod-releases-2023-report-on-military-and-security-developments-involving-the-pe%2F.

[94]Ellen Nakashima, "Analysis | Chinese Cyberspies Have Widely Penetrated Networks of Ally Cambodia," *Washington Post*, November 8, 2023, https://www.washingtonpost.com/politics/2023/11/08/cambodia-has-chinese-hacker-problem/.

China has created new instruments for carrying out digital information activities, according to an examination of a research carried out by Microsoft in September 2022. Microsoft demonstrated how China has advanced its ability to create images automatically for use in influence operations, with the goal of simulating American voters of different political persuasions and igniting controversy on the military, economic, and ideological lines. This is the way how realistic images produced by the country using artificial intelligence are made to spread on social media. China now possesses advanced tools for disseminating false material on social media, in addition to its recent hacking efforts. Social media companies previously reported on crude disinformation tactics disseminating Chinese propaganda, particularly in the run-up to the 2020 U.S. elections.[95]

According to US military, intelligence, and national security officials, Washington is searching for malicious computer code that, as US perceives Beijing government has concealed deep within the networks that control communications networks, water supplies, and electrical grids which further supply military bases in the US and around the world.[96]Concerns have been raised following the discovery of the virus that Chinese hackers, most likely affiliated with the PLA, may have inserted code designed to obstruct US military operations in the event of a confrontation, including any action Beijing may take against Taiwan in the near future. A congressional official described the program as essentially a ticking time bomb that might enable China to cut off power, water, and communications to US military installations, disrupting or slowing down resupply or deployment

[95] Clint Watts, "China, North Korea Pursue New Targets While Honing Cyber Capabilities," Microsoft On the Issues, September 7, 2023, https://blogs.microsoft.com/on-the-issues/2023/09/07/digital-threats-cyberattacks-east-asia-china-north-korea/.

[96] David E. Sanger and Julian E. Barnes, "U.S. Hunts Chinese Malware That Could Disrupt American Military Operations - The New York Times," July 29, 2023, https://www.nytimes.com/2023/07/29/us/politics/china-malware-us-military-bases-taiwan.html.

activities.[97]But according to U.S. officials, the same infrastructure frequently serves the homes and businesses of regular Americans, so its effects might be much wider.

4.4) US-China Technological Competition in Cyberspace

The competition between Beijing and the Washington in technology during Fourth Industrial Revolution has potential to be the most significant subject in emerging power politics. Future worldwide hegemony will be determined by how successful a state is in the fields of semiconductors.[98]The first hurdle to competition in these industries is paved with innovation in technology and high product production. Technological innovation is also necessary for this rivalry to succeed in modern technology, which makes the internal structure of the modern devices. Furthermore, recent advancements particularly in Internet over Things -related technologies are also generating interest.

Due to advances in industries related to the Fourth Industrial Revolution, there has been a boom in demand for high-performance semiconductors, China is aggressively pursuing technology. Furthermore, Chinese firms –Huawei and Xiaomi- are investing in low-cost smart phones with the intention of reaching both the Chinese and international markets. China is also becoming more and more technologically advanced in fields like drones, artificial intelligence, and unmanned vehicles.[99]With the passage of past three years, Chinese enterprises have surpassed US corporations in the development of technological capabilities in the supercomputer sector.

[97] Gabriel Honrada, "Private Infrastructure Complicates US Warfare Plans," Asia Times, August 2, 2023, http://asiatimes.com/2023/08/private-infrastructure-complicates-us-warfare-plans/.

[98]Rush Doshi, "The United States, China, and the Contest for the Fourth Industrial Revolution," *Brookings,* July 31, 2020, https://www.brookings.edu/articles/the-united-states-china-and-the-contest-for-the-fourth-industrial-revolution/.

[99] Anastasia Tolstukhina, "US Technology Policy amid Rivalry with China," Russian international affairs council, December 5, 2023, https://russiancouncil.ru/en/analytics-and-comments/analytics/us-technology-policy-amid-rivalry-with-china/.

Network equipment is a major problem in the US-China technology conflict. America's Cisco, a manufacturer of telecom gear, commands 60–80% of the Chinese market. By the end of 2012, Cisco controlled over 70% of the finance industry and over 50% of government enterprises in the fields of education, fantasy, public security, and maritime. Additionally, Cisco controlled roughly 60% of the railroad industry.[100]Regarding Cisco's control over the integral part of the Chinese economy, Pang Sing Dong, the founder of the Internet Lab, claimed that Beijing would not be able to absorb the shocks of disputes between the United States and China. Following Edward Snowden's disclosures, the Chinese government increased its influence over Cisco.[101]

In the midst of these developments, Washington, during Trump regime, has prohibited Huawei from acquiring network equipment due to concerns that its close affiliations with the Chinese government that may compromise national security. Additionally, ZTE, a Chinese manufacturer of telecom equipment, was prohibited from conducting business with US companies for seven years. Similarly, it is also challenging for Chinese CCTV manufacturer Hikvision and world-renowned Chinese drone manufacturer DJI to join the US markets. This is similar to the US-Japan struggle from the 1990s, which involved sectors and technology with dual uses and had significant security ramifications for hegemonic competition.[102]

Considering the size of the Chinese domestic market, it is noteworthy that Chinese businesses are promoting joint ventures, mergers, and acquisitions. Chinese companies first embraced technology

[100]Anu Bradford, "The Battle for Technological Supremacy: The US–China Tech War," in *Digital Empires: The Global Battle to Regulate Technology*, ed. Anu Bradford (Oxford University Press, 2023), 183–220, https://doi.org/10.1093/oso/9780197649268.003.0006.

[101] Adam Segal, "Chinese Cyber Diplomacy in a New Era of Uncertainty," The Lawfare Institute, July 30, 2017, https://www.lawfaremedia.org/article/chinese-cyber-diplomacy-new-era-uncertainty-0.

[102]ZeevMaoz, "Networks of Nations: The Evolution of Structure and Effects of International Networks, 1816-2001," December 1, 2009, 1816–2001. https://www.researchgate.net/publication/228705322_Networks_of_Nations_The_Evolution_of_Structure_and_Effects_of_International_Networks_1816-2001

through invention and learning in the early stages of development, but they now use mergers and acquisitions in addition to technology development to accept it after they reach a certain scale.[103]Chinese businesses are employing enormous pay to entice top talent to China through the recruitment of top human resources, much like there have been cases recently in the field of artificial intelligence. China has a competitive advantage in the Internet of Things (IoT) market due to its sizable domestic market and the favorable conditions brought forth by its rapid economic growth. The health of China's system will ultimately determine whether or not the country succeeds in crossing the threshold into manufacturing and network technology. The 13th five-year plan, Made in China 2025, Internet Plus, AI Action Plan, and other policy measures have been launched by the Chinese government.[104] For instance, Internet Plus describes eleven main goals to be pursued, one of which is the integration of artificial intelligence and the Internet. The objective of the "Made in China 2025" initiative is to position China as a global manufacturing leader by promoting the adoption of information technology (IT), robotics, and electric vehicles.[105]US Internet companies continue to lead the competition in this space. However, Chinese businesses have recently put the US dominance under pressure. Tencent takes on Face book, Baidu directly competes with Google, Alibaba takes on Amazon, and Xiaomi takes on Apple.[106]Of course, the analogies cited above do not provide a clear picture of their animosity; rather, contemporary events have painted more complex pictures.

The Chinese government, instead of following global norms headed by the US, has attempted to implement a ―Informatization Model of Chinese Characteristics in this process. Beijing government

[103] Peter J. Williamson and Anand Raman, "The Globe: How China Reset Its Global Acquisition Agenda," *Harvard Business Review*, April 1, 2011, https://hbr.org/2011/04/the-globe-how-china-reset-its-global-acquisition-agenda.

[104] MeiaNouwens and Helena Legarda, "China's Pursuit of Dual-Use Technologies," *IISS*, December 18, 2018, https://www.iiss.org/research-paper//2018/12/emerging-technology-dominance.

[105] Keith Belton, John Graham, and Suri Xia, "'Made in China 2025' and the Limitations of U.S. Trade Policy," *SSRN Electronic Journal*, 2020, 2–7, https://doi.org/10.2139/ssrn.3664347.

[106] Nicholas Borst, "China's Tech Rush – How the Country's Strategic Technology Campaign Is Shaping Markets," *Seafarerfunds,* September 2018, 7–10.

has enforced self-censorship and filtering restrictions on Internet service providers in this particular situation[107]; American businesses are not exempt from this policy. Beyond just the dispute between US corporations and the Chinese government, these policies have ramifications for the political and economic structures of the two nations. Accordingly, the battle between the US and China for the suitability of their respective systems is mirrored in the competition at the threshold of standards.

The growing power struggle in cyberspace is getting far more intricate than it used to be. In other words; the competition within this prominent industry goes beyond simply vying for control of market share or creating innovative products. [108]It also involves a rivalry in terms of establishing and promoting platforms, considering factors such as standardization, widespread adoption, scalability, and the characteristics of the overall system.

4.5) US-China Strategic Competition in Cyberspace: Normative Challenges to The Global Order

a. Significance of Norms in Global Order

During the research study, I conducted interviews with different cyber security experts and took their views on the ongoing competition between China and United States in Cyberspace and how this competition in posing multifaceted normative challenges to the global order. While responding to my questions, **cyber security expert 1** responded that fundamentally, normativity is a philosophical theory and trans-disciplinary notion that deals with moral judgments and seeks to uphold morality or guard against corruption and wrongdoing. It creates a framework for defining what is right and wrong.

[107] Maria Repnikova, “How Chinese Authorities and Individuals Use the Internet,” Hoover Institution, October 29, 2018, https://www.hoover.org/research/how-chinese-authorities-and-individuals-use-internet.

[108] Sangbae Kim, “Cyber Security and Middle Power Diplomacy: A Network Perspective,” *The Korean Journal of International Studies* 12, no. 2 (December 31, 2014): 323–52.

He stated that normative theory in international relations (IR) deals with standards, norms, values, and laws in world politics. In international relations, normativity refers to rules of conduct for people, governments, and the international state system. It also includes duties, rights, and responsibilities. It includes the ethical and moral aspects of many international political subjects. When it comes to normativity significance in forming the international order, it is vital since it shapes state conduct, especially after World War 2. The fundamental laws governing relations between states were established by historical conventions and practices. Treaties, agreements, and protocols were the means by which normativity was put into practice.

According to the **cyber security expert 1,** there are key aspects of normativity in shaping global order. Norms like sovereignty, territorial integrity, and non-aggression contribute to the establishment of states. Moreover, Norms led to the promotion of peace and cooperation through international organizations like the UN and justice through international law, and set expectations for how people should be treated globally, promoting equality, liberty, and human dignity. Norms pertaining to space, cyberspace, and climate are becoming increasingly important in the modern era. The prevalence of Western viewpoints in influencing global discourse and structural flaws are some of the obstacles that impede its importance. As a foundation for normative conduct, normativity establishes standards, directs behavior, and creates a stable, cooperative international system.

According to the **cyber security expert 2,** the unseen set of rules that governs behavior worldwide is known as normativity. Like a dynamic network, it changes as strong actors via with one another and marginalized voices fight to be heard. Comprehending it enables us to take part in forming the international system, maintaining current standards or advocating for new ones that represent our ideal of a fair and equitable society.

The concept of normativity in international relations is multifarious- according to the **cyber expert3.** There is the English school of thought, in which Buzan has defined that normativity is a values-based international order which has its guiding principles; there are principal actors, agents, secondary actors, and institutions. The expert states that by keeping all that theoretical debate aside, basically we need to understand that it all boils down to the fact that each country or each nation state has its own set of socio-cultural ideas based on which the values are derived in their unique national context. And those values ultimately determine its behavior on the regional stage as well as the international stage. The western world has, by and large which means the US and NATO are trying to influence it in its own way. To a large extent with the United States, it is more of a liberal international order which has norms which are not focused particularly on their national context but on a larger global level. And those are values-based norms which may not be interlinked with the perspective of their national sovereignty.

According to cyber expert 4, normativity defines guidelines, ideas and rules that actually shape the behavior of a certain society or center maybe a communication. Adherence to these norms is normativity. So norm is actually the ideas and rules that shape behavior and once adherence to those norms or those rules, those standards- whether it be social, cultural, legal or whatever- it becomes normativity. When it comes to the term's global world order, it is actually the structure and the arrangements of power that influences the relations among the states. So, to run that global world order, there are certain norms which actually shape and maintain that global world order. These norms are related to international relations revolving around diplomacy, human rights, justice, global governance, trade economics, environmental angles, conflict resolution, security, culture. All these things are governed through some global world order and these are shaped through some norms. The responder states that international relation is governed by various rules and treaties, for example, NPT is one of the treaties which governs states relations in nuclear domain. Similarly, laws of human rights predominantly govern the justice among the states. In the same essence, trade and economic institutions have sea lines of communication which cannot be docked in even in war like situations. Furthermore, in environment domain conference of parties is one of the norms which is working to control the greenhouse gas emissions. According to the responder, there are also technological norms which govern the global order in cyberspace. In a nutshell, it can be stated that norms and norms building that play a vital role in shaping the global order is an ambiguous process. There is not a single definition on cyber security experts or International Relations scholars show consent.

b. Normative Challenges to the Global Order

The rules and principles of the international system are significantly impacted by the activities of both China and the United States in the cyberspace. Due to their significant reliance on cyberspace for operations, planning, and communication, both countries are engaged in a cyber-arms race and continuous competition.[109] Complexities arise from this complicated and ambiguous pattern of strategic struggle in the twenty-first century, especially in the area of cyberspace.

In perspective of **cyber security expert 5,** there are worries that responsible state behavior may be compromised as a result of the competition between US and China in cyberspace. Cyberspace activities can put established norms and standards for governmental behavior in cyberspace in jeopardy. Cyberspace information warfare poses a threat to democratic values including free flow of information, digital communication security, and the protection of democratic processes from outside interference. The fundamental tenets of democratic society are in danger because of this. The competitive nature of the cyberspace poses a direct danger to diplomatic principles such as

[109] Michael Kolton, "Interpreting China's Pursuit of Cyber Sovereignty and Its Views on Cyber Deterrence," *The Cyber Defense Review* 2, no. 1 (2017): 119–54. https://www.jstor.org/stable/26267405

sovereignty, non-intervention, and aspects of national security. Traditional ideas of territorial integrity are challenged by the borderless nature of cyberspace. Cyber technology's dual-use character calls for a reassessment of fundamental ideas in nuclear policy, including non-proliferation, deterrence, and non-aggression.

According to this **cyber-security expert 6**, it is true that the US-China strategic struggle in cyberspace poses a normative threat to the international order. Discourse building cannot be the only solution to the real problems posed by cyber espionage, intellectual property theft, and information warfare. These problems touch many different sectors. Nonetheless, in international politics, it is imperative to recognize the influence of language and narrative-building instruments on public opinion and diplomatic ties. In their ongoing global strategic rivalry, the US and China both use discourse to further their goals and sway public opinion. This includes framing issues to support their respective national agendas, such as the creation of international cyber rules. Although the issues in cyberspace have practical ramifications; the narrative-building component complicates the problem in general.

Another security expert7responded that US-China strategic competition ultimately poses normative challenges to the global order. Indeed, it is a real problem that serves to further the plot. For instance, Hollywood films were classified as Chinese or Russian in the UK. In order to create a story that suggests these men are criminals with a poor reputation worldwide. The author states an example that by saying ‘’ if you look at Kaspersky and conduct business with Russia, the first thing that is asked is, ‘You are Russian; Russians are supposed to be criminals; how can we trust you?’. They have so established a transparency center and a third-party visibility center in order to respond to it. However, if you use data in any way and you're American, that will not be considered.’’

Contrary to others, another **cyber security expert 8** states that he does not think that there is an actual attempt at rivalry from the Chinese side, but he does personally view that there is a competition from the American side. The fundamental truth is that China has made tremendous strides in technology advancement—such as quantum computing—and is steadily establishing itself as a rising power. Based on that, it is genuinely beginning to rise at this time since they have made significant progress that is at least ten to twenty years ahead of what the West had predicted. For this reason, they perceive themselves as being challenged by the West, especially America, and feel intimidated and excluded. As a result, the author does not view that any global online norms will be imposed or implied. To be completely honest, according to expert, there are not any globally recognized norms of cyberspace behavior at this time. Indeed, the United Nations group of state experts has made decisions on several cyber-related issues, and national forums such as NATO have worked on the Talon manual to define terms like cyber war and cyber defense, among other things. China is not, in his opinion, in a competitive market with the United States. They are only making it clear that they will not submit to a western-led assault on what they view as the principles of an open internet. China is not, according to him, in a competitive market with the United States. No Chinese researcher, whether an expert in international relations or a practitioner dealing with cyberspace matters, has ever argued in favor of trying to outmaneuver the US or the west in cyberspace. They are only making it clear that they will not submit to a western-led assault on what they view as the principles of an open internet. China is certain that we should safeguard our interests as a nation online. Cyberspace can be defined as a global common within the territory since it is a worldwide common, just like the maritime domain and outer space. However, neither the Chinese nor the US has any real competition. Instead, the US and Chinese governments have largely created a lot of hype around the issue, thanks to the aggressive narratives that academics and think tanks in Washington have been pushing. In particular, some of these think tanks, called "hawks," reject the Chinese Communist Party as the legitimate government in China and are deeply hostile to China. According to the U.S. government’s official statements, cyber threats from China represent serious concerns to national security, including the possibility of key infrastructure outages, the theft of confidential data, and the penetration of defense systems.

According to cyber expert 9, normative challenge posed by US-China competition is a genuine concern because it has impact on the other countries, for example, cyber espionage or intellectual property theft. In this case, if a country steals intellectual property rights, it puts impacts directly on the other country. The National Security Agency of America, Sarthe five I's and the five L's, in which the NSA is collecting data from social media and in the result of social media interactions, this is going to the Prism software in USA which is used by the NSA for the strategic purposes- a clear indication of espionage. Similarly, the gospel is also Wolf pack software which is used for the cyber espionage. Coming to the digital trade, trade secret, advanced technologies, and hacking, countries actually do the cyber-attack and actually hack the trade secrets and advanced technologies design to manufacture the copies secretly. Through cyber, disinformation campaigns run by China and USA, states are performing act of intellectual property theft. According to the author, China and Cuba have an exhibition of engaging in cyber information operation and disinformation campaigns to shape the narratives globally- China against USA, USA against China. Both of them run a disinformation campaign. During Covid-19, USA used to call the virus as China virus that was actually the disinformation campaign.

4.6) MAJOR FINDINGS OF THE PRIMARY AND SECONDARY SOURCES

The competition between the United States and China in cyberspace is characterized by its multifaceted and ever-changing nature. Both countries are actively engaged in a constant pursuit of dominance, employing a combination of legitimate and illegitimate strategies to achieve their respective goals. The primary findings from expert opinions reveal distinct perspectives on the normative challenges posed by this strategic competition to the global order. On one hand, there is a belief that China's involvement in cyber espionage, cyber theft, and violations of property rights presents a significant normative threat, as these acts are illegal and contravene established global norms of data protection, privacy, and respect for property rights. However, contrasting views suggest that China is not necessarily seeking to challenge the existing norms in cyberspace, and instead highlight the United States' active violation of global order tenets. These experts argue that the US constructs a narrative portraying Chinese activity as a threat to the normative basis of the global order. It is evident that the US-China strategic competition in cyberspace encompasses diverse dimensions and interpretations, with varying perspectives on the impact of normative challenges to the global order. Ultimately, the perception of such challenges is a constructed reality influenced by individual viewpoints and interests. To sum up, the ever-changing terrain of strategic conflict between the United States and China in cyberspace poses significant moral obstacles to the current global order.

CHAPTER 5

RECOMMENDATIONS AND CONCLUSION

5.1) Recommendations

In order to effectively handle and regulate the competition that exists between US and the China in cyberspace, a multipronged strategy involving technological, legal, diplomatic, and policy measures is needed. Cyberspace presents opportunities as well as obstacles for US-China cooperation in governance. Growing cyber-attacks necessitate collaboration to set standards and stop a digital arms race. Global interconnection and common risks present a bridge for cooperation in the fight against cybercrime. Historical mistrust continues to be a barrier that requires sincere dedication to getting past obstacles. Cyberspace's future depends on its ability to navigate this complicated terrain for the sake of cooperative gain or hostile competition, highlighting the necessity of bravery and forethought in the quest for a safer society.

a. Diplomatic Measures

A diplomatic strategy should place a high priority on communication, openness, and the creation of international standards in order to manage any clash or competition between the US and China in cyberspace. Firstly, in order to promote mutual understanding and trust, both countries should hold high-level diplomatic discussions. A forum for candid discussion and the sharing of concerns can be established by creating a specific bilateral dialogue mechanism centered on cyber issues. To further minimize mistrust and the possibility of misunderstanding, the US and China should cooperate to increase transparency in their respective cyber operations by exchanging details about cyber doctrines, tactics, and military might.

Promoting international standards and guidelines for acceptable conduct in cyberspace is another essential component. By actively participating in existing multilateral forums, both countries can contribute to the creation of consensus-driven norms that promote responsible state behavior in cyberspace. For instance, the UN GGE (Group of Governmental Experts on Developments in Information and Telecommunications in a Context of International Security).[110] Mutual trust and collaboration between the two countries can be further enhanced by cooperative measures to combat cybercrime, the setting up of hotlines for cyber incidents, and the development of cooperative cyber-security initiatives.

In addition, the US and China ought to investigate the potential for cooperative projects in areas where their interests coincide, such countering non-state actors' cyber-attacks or tackling shared issues with safeguarding vital infrastructure. These kinds of joint initiatives can act as measures to boost confidence and support the general stability of cyberspace. Ultimately, the United States and China can manage their strategic competition in cyberspace through diplomacy that prioritizes open communication, transparency, adherence to international norms, and cooperative efforts. Additionally, by using such strategies, the chance of a dispute might be decreased and foster a more secure and resilient global digital environment.[111]

b. Economic Measures

Economic policies can have a big impact on how people behave. For example, the United States could think about using trade agreements to reward countries that follow established cyber- security standards. In addition, encouraging creativity and teamwork in cutting-edge fields like quantum

[110] Paul Meyer, "Seizing the Diplomatic Initiative to Control Cyber Conflict," *The Washington Quarterly* 38, no. 2 (April 3, 2015): 47–61, https://doi.org/10.1080/0163660X.2015.1064709.
[111] S. Jayawardane, J. E. Larik, and E. Jackson, "Cyber Governance: Challenges, Solutions, and Lessons for Effective Global Governance," December 10, 2015, https://hdl.handle.net/1887/48177.

computing and artificial intelligence can help one gain a competitive edge in cyberspace. The overall cyber-security posture can be strengthened by promoting collaboration between the business and public sectors through cooperative research and development projects. Additionally, creating a structure by both states to share information on cyber threats can aid in preventing miscommunication and lower the possibility of unintentional escalation. A comprehensive plan to negotiate the complicated terrain of U.S.-China strategic competition in cyberspace can be developed by combining diplomatic efforts, financial incentives, and technological cooperation. The creation of a cyber-security dialogue mechanism at the highest governmental levels would, last but not least, offer a forum for ongoing communication that would enable both countries to discuss issues, exchange viewpoints, and identify points of agreement in order to manage the complicated world of cyberspace. To sum-up, both countries should collaborate to shield critical non-military domains like energy, transportation, finance, education, and climate from cyber threats. This protection will benefit both nations and the global community by ensuring stability and safeguarding economic activities. Joint efforts can enhance resilience and contribute to a secure digital environment. Ultimately, to advance stability, lowers the likelihood of conflict, and improves collaboration between the US and China in the area of cyberspace, a mix of diplomatic and technological measures is required.[112]

c. Confidence Building Measures

More stability in the cyberspace can be achieved through the creation of bilateral agreements on cyber standards, rules of engagement, and confidence-boosting initiatives. Collaboration and trust-building can be further fostered and increased by supporting both countries' involvement in

[112] Unal Tatar, Bilge Karabacak, and Adrian Gheorghe, “An Assessment Model to Improve National Cyber Security Governance,” *Proceedings of the 11th International Conference on Cyber Warfare and Security, ICCWS 2016, March 17-18, 2016 Boston, MA*, January 1, 2016, 312–19. https://digitalcommons.odu.edu/emse_fac_pubs/114/

international conferences and projects focused on cyber governance. Cooperation can also be built on shared interests and values by working together to combat common cyber threats like terrorism and International Cybercrime.

Several Key Confidence-Building Measures Include:

i. Information sharing mechanisms play a crucial role in cyber security. Collaborative efforts, such as joint exercises as cyberspace provides an opportunity to both states to minimize the tensions, incident response coordination, and the sharing of cyber threat intelligence, should be encouraged to enhance information sharing among countries. This will facilitate a better understanding of the evolving cyber landscape and enable the adoption of effective preventive measures.

ii. International organizations, particularly the United Nations: should be strengthened to address cyber security challenges. This can be achieved by empowering specialized agencies or bodies within these organizations to govern cyberspace effectively. By leveraging the expertise and resources of international organizations, countries can collectively address the complex and evolving nature of cyber threats.

iii. Public-private collaborations are vital in promoting cyber security: Securing cyberspace requires public-private cyber security cooperation. Through these collaborations, the public sector may harness the knowledge and experience of the business sector, exchange resources and data, and create more effective plans to counteract cyber-attacks. Both the public and private sectors have interests in the same infrastructure, and they share responsibility for keeping it safe and dependable. These collaborations have the potential to increase trust and open up dialogue about issues pertaining to cybercrime. Addressing cybersecurity concerns requires cooperation, and public-private partnerships offer a crucial environment for enhancing this cooperation. There are organizational and governance concerns to consider, in addition to the different cooperation and conflicts that these partnerships entail. They entail cooperation between the public and commercial sectors; public-private partnerships can be an effective tactic for developing robust cybersecurity.[113]Both the public and commercial sectors must take efforts to improve cybersecurity. These partnerships are valuable because they provide the private sector the freedom and resources to look into threats in ways that the public sector might not be able to. In addition to being advantageous for national cybersecurity, public-private cooperation in cybersecurity also promotes corporate success and commercial innovation. The Center for Threat Informed Defense, INTERPOL Gateway, MITRE Ingenuity, NATO Industry Cyber Partnership, Cyber Threat Alliance, and NIST's National Cybersecurity Excellence Partnership are a few of these global partnerships.[114]

iv. Regional cyber security initiatives: Since regional cybersecurity issues transcend national boundaries, they are essential to tackling common issues. International agreements on cybersecurity information sharing encompass cooperative measures to counteract threats and support the safeguarding of vital infrastructure. The issues these communities face are highlighted in the U.S. National Cybersecurity Strategy, which also presents a vision of shared purpose and priorities. The nation's cybersecurity resilience is strengthened in large part by the Department of Homeland Security. In contrast to American policy, China's concept of "shared security" places a strong emphasis on mutual benefit and collaboration. Some states' confidence in total supremacy is the reason for the lack of progress in resolving security

[113] Derek Manky, “Cybersecurity Public-Private Partnership: Where Do We Go Next?,” SecurityWeek, July 24, 2023, https://www.securityweek.com/cybersecurity-public-private-partnership-where-do-we-go-next/.

[114] VaGreiman, “Public/Private Partnerships in Cyberspace: Building a Sustainable Collaboration,” *Journal of Information Warfare* 14, no. 3 (2015): 30–42.

challenges in cyberspace.[115]The US seeks to enhance collaboration with its regional allies by utilizing their assets and knowledge. The alliance between the United States and India seeks to improve cybersecurity capabilities by utilizing AI. A standard baseline of security and assistance in managing agencies' cyber risk are provided by the government, in particular through the Cybersecurity and Infrastructure Security Agency (CISA).

By focusing on regional cooperation, nations can develop tailored solutions that align with their specific needs and foster a more secure cyber environment. In addition to this, the vital physical infrastructure and cyberspace of the country are now far more secure owing to the efforts of the Department of Homeland Security (DHS). The goal of the Emergency Services Sector Cybersecurity Initiative is to better understand and manage cyber threats and to organize the sharing of cyber tools and information. The White House's National Cybersecurity Strategy outlines plans to jointly protect against and counteract cyber threats from authoritarian governments. Member governments of the Organization of American governments receive assistance in creating their own national cybersecurity plans. [116]The Biden-Harris Administration has released the National Cybersecurity Strategy Implementation Plan (NCSIP) to maintain transparency and a sustained focus on cybersecurity. In addition, the Department of Defense has developed cybersecurity initiatives as part of the National Security Strategy for 2022.

v. Capacity building and technical assistance: These measures are also essential for nations that lack cyber capabilities. Support should be provided to help these countries develop their cyber security capacities. This can be done through technical training programs, knowledge transfers

[115] Theresa Hitchens and Nilsu Goren, "International Cybersecurity Information Sharing Agreements" (Center for International & Security Studies, U. Maryland, October 1, 2017), https://www.jstor.org/stable/resrep20426.

[116] "Secure Cyberspace and Critical Infrastructure | Homeland Security," homeland security, n.d., https://www.dhs.gov/secure-cyberspace-and-critical-infrastructure.

initiatives, and partnerships with more advanced nations, ultimately benefiting global cyber security efforts.

vi. The establishment of common cyber security standards and interoperability is paramount. By adopting internationally recognized frameworks, countries can ensure secure communication and information exchange. This will enhance collaboration, facilitate cyber defense efforts, and establish a more unified global approach to cyber security.

vii. Lastly, multilateral cyber crisis management mechanisms need to be implemented. These mechanisms should enable timely reporting, preventive measures, and coordinated responses to cyber-attacks. By establishing frameworks for managing cyber crises at an international level, countries can effectively address cyber incidents and minimize their impact on global security.

These measures promote collaboration, transparency, and understanding, ultimately reducing the risk of cyber conflicts and promoting global cyber security. Experts from both states may strengthen their relationship and improve technological cooperation through regular cyber-security exchanges, cooperative research projects, and joint training exercises.[117]

d. Addressing the Normative Challenges of Cyberspace within the Laws of War:

i. Distinction: In traditional warfare, it is clear who the attacker is, but in cyber warfare, attribution becomes challenging. Additionally, distinguishing between civilian and military targets is blurred in cyberspace. Efforts should be made to develop mechanisms for identifying and attributing cyber-attacks to specific actors, thereby enabling a clearer distinction between targets.

[117] Mark Raymond, "Managing Decentraliz0ed Cyber Governance: The Responsibility to Troubleshoot," *Strategic Studies Quarterly* 10, no. 4 (2016): 123–49. https://www.jstor.org/stable/26271532

ii. Proportionality: Unlike traditional warfare, cyber-attacks can potentially cause disproportionate damage, affecting critical infrastructure, industries and even entire cities. It is essential to establish guidelines and norms that ensure cyber operations are proportionate to the intended objectives, avoiding undue harm to civilian populations and infrastructure.

iii. Precautions in Attack: Precision attacks and minimizing collateral damage, which are common in traditional warfare, are difficult to achieve in cyberspace. However, measures should be taken to minimize unintended consequences and potential collateral damage. This includes developing sophisticated cyber defense systems, conducting thorough risk assessments, and adopting responsible cyber strategies.

iv. Responsibility: While the responsibility in traditional warfare lies with authorized individuals or states, attribution in cyber-attacks is often challenging due to the involvement of non-state actors or state-sponsored entities. International agreements and norms should be established to attribute cyber-attacks and hold responsible parties accountable, even when direct state involvement is not evident.

v. International Humanitarian Law**:** The framework of international humanitarian law should be examined to determine its applicability to cyberspace. Evaluating and updating existing laws and treaties can help address the unique challenges posed by cyber operations. This includes clarifying the responsibilities of states, establishing accountability mechanisms, and ensuring compliance with international norms and principles.

To sum-up, coordinated efforts are needed to create attribution mechanisms, set rules for proportionate cyber operations, reduce unintended consequences, hold accountable parties, and adapt international humanitarian law to the digital sphere in order to address the normative challenges of cyberspace within the laws of war.

5.2) CONCLUSION

In conclusion, it can be stated that the competition between United States and China in cyberspace is multifarious and dynamic in nature that both states are striving to dominate the cyberspace through both legitimate and illegitimate means. Both states alleged each other of cyber espionage activities against each other; however, United States officials and policy makers, as evident in their official documents, are trying to construct that China is a real danger to norms and values in cyberspace. The dynamic cyberspace landscape of competition between the United States and China reflects the complex interactions between security imperatives, geopolitical objectives, and technological breakthroughs. There are significant political, military, and economic implications in this competition between the two states in order to gain supremacy in the digital sphere. To sum up, the ever-changing terrain of strategic conflict between the United States and China in cyberspace poses significant moral obstacles to the current global order. The ramifications for international norms, regulations, and governance in the cyber realm are growing in importance as these two major countries negotiate the intricacies of technology breakthroughs and geopolitical rivalries. Different approaches to cyberspace and the pursuit of national interests online could undermine established standards of conduct, including those concerning data privacy, cyber sovereignty, and intellectual property rights. The competition for cyberspace norms not only mirrors the US-China power conflict but also has global ramifications that affect both states and non-state actors. In order to reduce the likelihood of unintentional escalation and advance a more stable and secure cyberspace, there is an urgent need for more international collaboration, rules, and agreements. This is highlighted by the rising tensions in cyberspace. Establishing a basis for a cooperative and secure global cyberspace and navigating the complexity of this digital age need cultivating communication, transparency, and mutual understanding despite the inevitable rivalry.

The normative complexity underlying the strategic conflict between the United States and China is further compounded by the divergent opinions on matters like data governance, intellectual property, and the bounds of state sovereignty in cyberspace. In order to develop a shared framework that reflects the various interests and concerns of the global community, a concerted multilateral strategy is necessary in addition to bilateral efforts to effectively address these difficulties. In the context of growing geopolitical competition between the US and China, the establishment of internationally accepted standards for responsible state behavior in cyberspace is essential to promoting trust, reducing risks, and maintaining a stable international order. US state officials are working to construct the impression that Chinese cyber activity poses a threat to accepted standards and norms that could destabilize the global order in cyberspace. The international community cannot aspire to comprehend the complex terrain of cyberspace and guarantee that the changing dynamics do not jeopardize broader norms that underpin the contemporary global order.

In order to address these normative issues, coordinated actions at the bilateral and global levels are needed, with a focus on inclusive discourse, diplomatic discussions, and the creation of consensus around cyber standards. The safety and integrity of the international order also depend on developing a common understanding of the dangers and repercussions of normative deterioration in cyberspace. Addressing the normative issues raised by the strategic cyber-competitiveness between the United States and China is not only a national interest but also an international community responsibility in an era where the digital world is deeply entwined with global governance. In a nutshell, to manage the competition, both states need to collaborate and International Organizations should establish framework to avoid any kind of escalation of conflict in cyberspace.

BIBLIOGRAPHY

Ahmad, Sharique, Saeeda Wasim, Sumaiya Irfan, Sudarshana Gogoi, Anshika Srivastava, and Zarina Farheen. "Qualitative v/s Quantitative Research" 6 (October 28, 2019): 2828–32. https://doi.org/10.18410/jebmh/2019/587.

Ahmed, Abdelhamid. "Ontological, Epistemological and Methodological Assumptions: Qualitative Versus Quantitative," 2008. https://files.eric.ed.gov/fulltext/ED504903.pdf.

Ahmed, Abdelhamid M. "Ontological, Epistemological and Methodological Assumptions: Qualitative Versus Quantitative." *ERIC*, April 8, 2008. https://www.researchgate.net/publication/267736833_Ontological_Epistemological_and_Methodological_Assumptions_Qualitative_Versus_Quantitative.

Alamgeer, Zain. "Time Horizon in Research Onion." *THE INNOVIDEA* (blog), September 14, 2023. https://theinnovidea.com/time-horizon-in-research-onion/.

Alharahsheh, Husam Helmi, and Abraham Pius. "A Review of Key Paradigms: Positivism VS Interpretivism." *Global Academic Journal of Humanities and Social Sciences*, Global Academic Journal of Humanities and Social Sciences, June 30, 2020, 39–43.

Ali, Fawad. "Everything You Need to Know About Operation Aurora." MUO, March 16, 2022. https://www.makeuseof.com/operation-aurora/.

Austin, Greg. "China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain, Edited by Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron." *The China Journal* 75 (January 2016): 161–63. https://doi.org/10.1086/684056.

Azap, Bojan. "What Is Cyberspace?" *phoenixNAP IT Glossary* (blog), October 18, 2022. https://phoenixnap.com/glossary/what-is-cyberspace.

Baker, Kurt. "What Is Cyber Espionage? – CrowdStrike." *Crowdstrike.Com* (blog), February 28, 2023. https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/.

Barrinha, André, and Thomas Renard. "Power and Diplomacy in the Post-Liberal Cyberspace." *International Affairs* 96, no. 3 (May 1, 2020): 749–66. https://doi.org/10.1093/ia/iiz274.

Belton, Keith, John Graham, and Suri Xia. "'Made in China 2025' and the Limitations of U.S. Trade Policy." *SSRN Electronic Journal*, 2020, 2–7. https://doi.org/10.2139/ssrn.3664347.

Bermudez, Krystal. "Defense Department Report Highlights Cyber Threat from China." FDD, November 6, 2023. https://www.fdd.org/analysis/2023/11/06/defense-department-report-highlights-cyber-threat-from-china/.

Borst, Nicholas. "China's Tech Rush – How the Country's Strategic Technology Campaign Is Shaping Markets." *Seafarerfunds*, September 2018, 7–10.

Boru, Tesfaye. *CHAPTER FIVE RESEARCH DESIGN AND METHODOLOGY 5.1. Introduction Citation: Lelissa TB (2018); Research Methodology; University of South Africa, PHD Thesis*, 2018. https://doi.org/10.13140/RG.2.2.21467.62242.

Bradford, Anu. "The Battle for Technological Supremacy: The US–China Tech War." In *Digital Empires: The Global Battle to Regulate Technology*, edited by Anu Bradford, 183–220. Oxford University Press, 2023. https://doi.org/10.1093/oso/9780197649268.003.0006.

Center for Strategic and International Studies. "Significant Cyber Incidents | Strategic Technologies Program | CSIS." Accessed January 5, 2024. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

Charlotte, Nickerson. "Social Construction of Reality," April 20, 2023. https://simplysociology.com/social-construction-of-reality.html.

Cordesman, Anthony H. “The 2023 Edition of the Annual Threat Assessment of the U.S. Intelligence Community,” Center for Strategic and International Studies, March 13, 2023. https://www.csis.org/analysis/2023-edition-annual-threat-assessment-us-intelligence-community.

Costigan, Johanna. “Determining the Future of the Internet: The U.S.-China Divergence.” Asia Society, January 2023. https://asiasociety.org/policy-institute/determining-future-internet-us-china-divergence.

Council on Foreign Relations. “Connect the Dots on State-Sponsored Cyber Incidents - Titan Rain,” August 2005. https://www.cfr.org/cyber-operations/titan-rain.

D. O’Brien, Robert, and Shiran Shen. “The U.S., China, and Cybersecurity: The Ethical Underpinnings of a Controversial Geopolitical Issue.” *Carnegie Council*, May 24, 2013. https://www.carnegiecouncil.org/media/article/the-u-s-china-and-cybersecurity-the-ethical-underpinnings-of-a-controversial-geopolitical-issue.

Detel, W. “Social Constructivism - an Overview | ScienceDirect Topics.” International Encyclopedia of the Social & Behavioral Sciences, 2001. https://www.sciencedirect.com/science/article/abs/pii/B008043076701086X.

Dobák, Imre. “Thoughts on the Evolution of National Security in Cyberspace.” *Security and Defence Quarterly* 33, no. 1 (March 1, 2021): 75–85. https://doi.org/10.35467/sdq/133154.

“DOD Releases 2023 Report on Military and Security Developments Involving the People’s Repu,” October 19, 2023. https://www.defense.gov/News/Releases/Release/Article/3561549/dod-releases-2023-report-on-military-and-security-developments-involving-the-pe/https%3A%2F%2Fwww.defense.gov%2FNews%2FReleases%2FRelease%2FArticle%2F3561549%2Fdod-releases-2023-report-on-military-and-security-developments-involving-the-pe%2F.

Domingo, Francis C. “Conquering a New Domain: Explaining Great Power Competition in Cyberspace.” *Comparative Strategy* 35, no. 2 (March 14, 2016): 154–68. https://doi.org/10.1080/01495933.2016.1176467.

Doshi, Rush. “The United States, China, and the Contest for the Fourth Industrial Revolution.” *Brookings*, July 31, 2020. https://www.brookings.edu/articles/the-united-states-china-and-the-contest-for-the-fourth-industrial-revolution/.

Erskine, Toni, and Madeline Carr. “Beyond ‘Quasi-Norms’: The Challenges and Potential of Engaging with Norms in Cyberspace,” 2016, 1–22.

Fischer, Frank. “Constructing Policy Theory: Ideas, Language, and Discourse.” In *Reframing Public Policy: Discursive Politics and Deliberative Practices*, edited by Frank Fischer, 0. Oxford University Press, 2003. https://doi.org/10.1093/019924264X.003.0002.

Frizzell, Connie. “Ghost Fleet: A Novel of the Next World War, by P. W. Singer and August Cole.” *Naval War College Review*69 : No. 3 , (2016). https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1172&context=nwc-review.

Green, Kieran. “People’s War in Cyberspace: Using China’s Civilian Economy in the Information Domain.” *Military Cyber Affairs* 2, no. 1 (December 20, 2016). https://doi.org/10.5038/2378-0789.2.1.1022.

Greiman, Va. “Public/Private Partnerships in Cyberspace: Building a Sustainable Collaboration.” *Journal of Information Warfare* 14, no. 3 (2015): 30–42.

Gulati, Ashish. “What Are Sampling Techniques? Different Types and Methods.” knowlegehut, September 7, 2023. https://www.knowledgehut.com/blog/data-science/sampling-techniques.

Haggarty, Linda. “What Is Content Analysis?” *Medical Teacher* 18, no. 2 (January 1, 1996): 99–101. https://doi.org/10.3109/01421599609034141.

Harold, Scott, Martin Libicki, and Astrid Cevallos. *Getting to Yes with China in Cyberspace*. RAND Corporation, 2016. https://doi.org/10.7249/RR1335.

Hassan, Muhammad. "Exploratory Vs Explanatory Research - Research Method," November 1, 2023. https://researchmethod.net/exploratory-vs-explanatory-research/.

He, Kai, and Huiyun Feng. "International Order Transition and US-China Strategic Competition in the Indo Pacific." *The Pacific Review* 36, no. 2 (March 4, 2023): 234–60. https://doi.org/10.1080/09512748.2022.2160789.

Hitchens, Theresa, and Nilsu Goren. "International Cybersecurity Information Sharing Agreements." Center for International & Security Studies, U. Maryland, October 1, 2017. https://www.jstor.org/stable/resrep20426.

Hjortdal, Magnus. "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence." *Journal of Strategic Security* 4, no. 2 (2011): 1–24.

Honrada, Gabriel. "Private Infrastructure Complicates US Warfare Plans." Asia Times, August 2, 2023. http://asiatimes.com/2023/08/private-infrastructure-complicates-us-warfare-plans/.

Hsu, Kimberly. "China and International Law in Cyberspace." *U.S.-China Economic and Security Review Commission Staff Repor*, May 6, 2014, 1–10.

Jansen, Derek. "What Is A Longitudinal Study? A Simple Definition." *Grad Coach* (blog), June 2020. https://gradcoach.com/what-is-a-longitudinal-study/.

Jayawardane, S., J. E. Larik, and E. Jackson. "Cyber Governance: Challenges, Solutions, and Lessons for Effective Global Governance," December 10, 2015. https://hdl.handle.net/1887/48177.

Jenny. "Phase #2: Clearly Define Your Research Strategy." *MacKenzie Corporation* (blog), March 27, 2014. https://www.mackenziecorp.com/phase-2-clearly-define-research-strategy/.

Jinghua, Lyu. "What Are China's Cyber Capabilities and Intentions?" Carnegie Endowment for International Peace, April 1, 2019. https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734.

Kabir, Syed Muhammad. "METHODS OF DATA COLLECTION," 201–75, 2016. https://www.researchgate.net/publication/325846997_METHODS_OF_DATA_COLLECTION.

Kennedy, Andrew B., and Darren J. Lim. "The Innovation Imperative: Technology and US–China Rivalry in the Twenty-First Century." *International Affairs* 94, no. 3 (May 1, 2018): 553–72. https://doi.org/10.1093/ia/iiy044.

Kim, Sangbae. "Cyber Security and Middle Power Diplomacy: A Network Perspective." *The Korean Journal of International Studies* 12, no. 2 (December 31, 2014): 323–52.

———. "US-China Competition in Cyberspace: A Perspective of Emerging Power Politics and Platform Competition." *The East Asia Institute*, January 2019. http://www.sangkim.net/us-china-c-in-c.pdf.

Kim, Soung Min. "Inductive or Deductive? Research by Maxillofacial Surgeons." *Journal of the Korean Association of Oral and Maxillofacial Surgeons* 47, no. 3 (June 30, 2021): 151–52. https://doi.org/10.5125/jkaoms.2021.47.3.151.

Koh, Eunsook T., and Willis L. Owen. "Descriptive Research and Qualitative Research." In *Introduction to Nutrition and Health Research*, edited by Eunsook T. Koh and Willis L. Owen, 219–48. Boston, MA: Springer US, 2000. https://doi.org/10.1007/978-1-4615-1401-5_12.

Kolton, Michael. "Interpreting China's Pursuit of Cyber Sovereignty and Its Views on Cyber Deterrence." *The Cyber Defense Review* 2, no. 1 (2017): 119–54.

———. "Interpreting China's Pursuit of Cyber Sovereignty and Its Views on Cyber Deterrence." *The Cyber Defense Review* 2, no. 1 (2017): 119–54.

Kshetri, Nir. “Cybercrime and Cyber-Security Issues Associated with China: Some Economic and Institutional Considerations.” *Electronic Commerce Research* 13, no. 1 (March 2013): 41–69. https://doi.org/10.1007/s10660-013-9105-4.

Lee, Kai-Fu. “Book Review: AI Superpowers - China, Silicon Valley, and the New World Order.” Thinking Ahead Institute, September 25, 2018. https://www.thinkingaheadinstitute.org/research-papers/book-review-ai-superpowers-china-silicon-valley-and-the-new-world-order/.

Lieberthal, Kenneth, and Peter W. Singer. “Cybersecurity and U.S.-China Relations.” Brookings, February 23, 2012. https://www.brookings.edu/articles/cybersecurity-and-u-s-china-relations/.

Lindsay, Jon R. “The Impact of China on Cybersecurity: Fiction and Friction | International Security | MIT Press.” Accessed August 9, 2023. https://direct.mit.edu/isec/article/39/3/7/30310/The-Impact-of-China-on-Cybersecurity-Fiction-and.

Lingzhi, Fan, Cao Siqi, and Liu Caiyu. “Exclusive: China a Main Target of US NSA Cyberattacks, with Key Infrastructure under Threat - Global Times.” Global times, March 2, 2022. https://www.globaltimes.cn/page/202203/1253697.shtml.

Liudmyla Balke. “China’s New Cybersecurity Law and U.S-China Cybersecurity Issues.” *Santa Clara Law Review* 58, no. 1 (June 4, 2018): 137.

M. SPADE, COLONEL JAYSON. “China’s Cyber Power and America’s National Security.” Defense Technical Information Center, March 24, 2011. https://apps.dtic.mil/sti/citations/ADA552990.

Mahmutovic, Jasko. “What Is Non-Probability Sampling? | SurveyLegend.” Survey legend, February 8, 2023. https://www.surveylegend.com/sampling/non-probability-sampling/.

Manky, Derek. “Cybersecurity Public-Private Partnership: Where Do We Go Next?” SecurityWeek, July 24, 2023. https://www.securityweek.com/cybersecurity-public-private-partnership-where-do-we-go-next/.

Manson, George Patterson. “Cyberwar: The United States and China Prepare For the Next Generation of Conflict.” *Comparative Strategy* 30, no. 2 (May 3, 2011): 121–33. https://doi.org/10.1080/01495933.2011.561730.

Maoz, Zeev. “Networks of Nations: The Evolution of Structure and Effects of International Networks, 1816-2001,” December 1, 2009, 15–23.

Maurer, Christian Ruhl, Duncan Hollis, Wyatt Hoffman, Tim. “Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads.” Carnegie Endowment for International Peace, February 26, 2020. https://carnegieendowment.org/2020/02/26/cyberspace-and-geopolitics-assessing-global-cybersecurity-norm-processes-at-crossroads-pub-81110.

Mazanec, Brian M. “Why International Order in Cyberspace Is Not Inevitable.” *Strategic Studies Quarterly*, 2015, 78–95.

McGeachy, Hilary. “US-CHINA TECHNOLOGY COMPETITION: IMPACTING A RULES-BASED ORDER.” *UNITED STATES STUDIES CENTRE*, May 2019. https://publicsectornetwork.com/wp-content/uploads/2020/01/US-China-technology-competition-impacting-a-rules-based-order.pdf.

Meyer, Paul. “Seizing the Diplomatic Initiative to Control Cyber Conflict.” *The Washington Quarterly* 38, no. 2 (April 3, 2015): 47–61. https://doi.org/10.1080/0163660X.2015.1064709.

Michael, George. “A Review of: ‘Richard A. Clarke and Robert K. Knake. Cyber War: The Next Threat to National Security and What To Do About It.’” *Terrorism and Political Violence* 23, no. 1 (December 7, 2010): 124–26. https://doi.org/10.1080/09546553.2011.533082.

Nakashima, Ellen. “Analysis | Chinese Cyberspies Have Widely Penetrated Networks of Ally Cambodia.” *Washington Post,* November 8, 2023. https://www.washingtonpost.com/politics/2023/11/08/cambodia-has-chinese-hacker-problem/.

Nakashima, Ellen, and Joseph Menn. “China’s Cyber Intrusions Have Hit Ports and Utilities, Officials Say - The Washington Post.” The washington post, December 11, 2023. https://www.washingtonpost.com/technology/2023/12/11/china-hacking-hawaii-pacific-taiwan-conflict/.

Nelles, Mattia. “China’s Growing Cyber War Capacities.” *E-International Relations* (blog), July 29, 2012. https://www.e-ir.info/2012/07/29/chinas-growing-cyber-war-capacities/.

Njeri-Otieno, Grace. “Sampling Strategies for Qualitative Research.” *Resourceful Scholars’ Hub* (blog), September 8, 2021. https://resourcefulscholarshub.com/sampling-strategies-for-qualitative-research/.

Nouwens, Meia, and Helena Legarda. “China’s Pursuit of Dual-Use Technologies.” *IISS*, December 18, 2018. https://www.iiss.org/research-paper//2018/12/emerging-technology-dominance.

Pestana, Randy. “Cybersecurity: The Next Frontier of U.S.-China Competition in the Americas.” *Americas Quarterly* (blog), July 25, 2023. https://www.americasquarterly.org/article/cybersecurity-the-next-frontier-of-u-s-china-competition-in-the-americas/.

Pijović, Nikola. “The Cyberspace ‘Great Game’. The Five Eyes, the Sino-Russian Bloc and the Growing Competition to Shape Global Cyberspace Norms.” In *2021 13th International Conference on Cyber Conflict (CyCon)*, 215–31, 2021. https://doi.org/10.23919/CyCon51939.2021.9468296.

prakash.srivastava. “Narrative Analysis: Methods and Examples.” Harappa, October 4, 2021. https://harappa.education/harappa-diaries/narrative-analysis-in-qualititative-research/.

Pujanes, Kristel Marie. “Philosophy 101: The Six Branches of Philosophy.” *The Quarter-Life Experiment* (blog), April 8, 2020. https://thebadbread.com/2020/04/08/philosophy-101-the-six-branches-of-philosophy/.

Rahman, Md, Mosab Tabash, Aidin Salamzadeh, Selajdin Abduli, and Md. Saidur Rahaman. “Sampling Techniques (Probability) for Quantitative Social Science Researchers: A Conceptual Guidelines with Examples.” *SEEU Review* 17 (June 1, 2022): 42–51. https://doi.org/10.2478/seeur-2022-0023.

Raymond, Mark. “Managing Decentralized Cyber Governance: The Responsibility to Troubleshoot.” *Strategic Studies Quarterly* 10, no. 4 (2016): 123–49.

Repnikova, Maria. “How Chinese Authorities and Individuals Use the Internet.” Hoover Institution, October 29, 2018. https://www.hoover.org/research/how-chinese-authorities-and-individuals-use-internet.

Ryan, Gery, and H. Bernard. “Techniques to Identify Themes.” *Field Methods - FIELD METHOD* 15 (February 1, 2003): 85–109. https://doi.org/10.1177/1525822X02239569.

Sanger, David E., and Julian E. Barnes. “U.S. Hunts Chinese Malware That Could Disrupt American Military Operations - The New York Times,” July 29, 2023. https://www.nytimes.com/2023/07/29/us/politics/china-malware-us-military-bases-taiwan.html.

Sebenius, Alyza. “China’s Hackers Are Expanding Their Strategic Objectives.” LAWFARE. Default, December 5, 2023. https://www.lawfaremedia.org/article/china-s-hackers-are-expanding-their-strategic-objectives.

“Secure Cyberspace and Critical Infrastructure | Homeland Security.” Homeland security, n.d. https://www.dhs.gov/secure-cyberspace-and-critical-infrastructure.

Segal, Adam. “Chinese Cyber Diplomacy in a New Era of Uncertainty.” The Lawfare Institute, July 30, 2017. https://www.lawfaremedia.org/article/chinese-cyber-diplomacy-new-era-uncertainty-0.

Senlin, Li. “The Origin of Security Dilemma between China and US in Cyber Space,” 2018, 995–99.

Simkus, Julia. “Cross-Sectional Study: Definition, Designs & Examples.” *Simply Psychology* (blog), July 31, 2023. https://www.simplypsychology.org/what-is-a-cross-sectional-study.html.

Siwei, Zhao. “Exclusive: Report Reveals How US Spy Agencies Stole 97b Global Internet Data, 124b Phone Records in Just 30 Days - Global Times.” Global times, June 13, 2022. https://www.globaltimes.cn/page/202206/1268024.shtml.

Slotta, Daniel. “China: Number of Recorded Cyber Attacks 2022.” Statista, August 21, 2023. https://www.statista.com/forecasts/1398710/china-number-of-recorded-cyber-attacks.

Steup, Matthias, and Ram Neta. “Epistemology.” In *The Stanford Encyclopedia of Philosophy*, edited by Edward N. Zalta and Uri Nodelman, Spring 2024. Metaphysics Research Lab, Stanford University, 2024. https://plato.stanford.edu/archives/spr2024/entries/epistemology/.

Swedberg, Richard. “Exploratory Research.” In *The Production of Knowledge: Enhancing Progress in Social Science*, edited by Colin Elman, James Mahoney, and John Gerring, 17–41. Strategies for Social Inquiry. Cambridge: Cambridge University Press, 2020. https://doi.org/10.1017/9781108762519.002.

Tatar, Unal, Bilge Karabacak, and Adrian Gheorghe. “An Assessment Model to Improve National Cyber Security Governance.” *Proceedings of the 11th International Conference on Cyber Warfare and Security, ICCWS 2016, March 17-18, 2016 Boston, MA*, January 1, 2016, 312–19.

Thakur, Harish. “Research Design,” 175, 2021. https://www.researchgate.net/publication/353430802_Research_Design.

Thomas, David R. “A General Inductive Approach for Qualitative Data Analysis,” School of Population Health, University of Auckland, 2003, 2–9.

Thomas, Elizabeth. “US-China Relations in Cyberspace: The Benefits and Limits of a Realist Analysis.” *E-International Relations* (blog), August 28, 2016. https://www.e-ir.info/2016/08/28/us-china-relations-in-cyberspace-the-benefits-and-limits-of-a-realist-analysis/.

TING-FANG, CHENG, and CISSY ZHOU. “China Accuses U.S. of Hacking Huawei Servers since 2009 - Nikkei Asia,” September 20, 2023. https://asia.nikkei.com/Spotlight/Huawei-crackdown/China-accuses-U.S.-of-hacking-Huawei-servers-since-2009.

Tolstukhina, Anastasia. “US Technology Policy amid Rivalry with China.” Russian international affairs council, December 5, 2023. https://russiancouncil.ru/en/analytics-and-comments/analytics/us-technology-policy-amid-rivalry-with-china/.

Urie, Edwin. “Dawn of the Code War: America’s Battle Against Russia, China, and the Rising Global Cyber Threat. By John P. Carlin, with Garrett M. Graff. New York: Hatchett Book Group, 2018.” *Journal of Strategic Security* 12, no. 3 (October 1, 2019). https://doi.org/10.5038/1944-0472.12.3.1766.

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION. “China’s Cyber Capabilities: Warfare, Espionage, and Implications for the United States,” February 17, 2022. https://www.uscc.gov/hearings/chinas-cyber-capabilities-warfare-espionage-and-implications-united-states.

Val Sanchez, Karina Veronica, and Nezir Akyesilmen. “Competition for High Politics in Cyberspace: Technological Conflicts between China and the USA.” *Polish Political Science Yearbook* 50 (2021): 43.

Valeriano, Brandon, and Ryan C. Maness. *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. Oxford University Press, 2015. https://doi.org/10.1093/acprof:oso/9780190204792.001.0001.

Watts, Clint. “China, North Korea Pursue New Targets While Honing Cyber Capabilities.” Microsoft On the Issues, September 7, 2023. https://blogs.microsoft.com/on-the-issues/2023/09/07/digital-threats-cyberattacks-east-asia-china-north-korea/.

Weihua, Chen. “Developing a New Type of Major Power Relationship Between China and the U.S.” (China Daily). China-US Focus, March 24, 2017. https://www.chinausfocus.com/foreign-policy/developing-a-new-type-of-major-power-relationship-between-china-and-the-u-s.

“What Are Norms? - PHILO-Notes,” March 21, 2023. https://philonotes.com/2023/03/what-are-norms.

Williamson, Peter J., and Anand Raman. “The Globe: How China Reset Its Global Acquisition Agenda.” *Harvard Business Review*, April 1, 2011. https://hbr.org/2011/04/the-globe-how-china-reset-its-global-acquisition-agenda.

Wortzel, Larry M. “China’s Approach to Cyber Operations: Implications for the United States.” *U.S.-China Economic and Security Review Commission. H*, March 10, 2010, 4–5.

Wu, Xiangning. “Technology, Power, and Uncontrolled Great Power Strategic Competition between China and the United States.” *China International Strategy Review* 2, no. 1 (June 1, 2020): 99–119. https://doi.org/10.1007/s42533-020-00040-0.

Xinbo, Wu. “Beijing’s Wish List: A Wiser China Policy in President Obama’s Second Term.” Brookings, December 11, 2012. https://www.brookings.edu/articles/beijings-wish-list-a-wiser-china-policy-in-president-obamas-second-term/.

Yarusso, Lowell. “Constructivism vs. Objectivism.” *Performance + Instruction* 31, no. 4 (1992): 7–9. https://doi.org/10.1002/pfi.4170310404.

Yong, Nicholas. “Industrial Espionage: How China Sneaks out America’s Technology Secrets.” *BBC News*, January 16, 2023, sec. China. https://www.bbc.com/news/world-asia-china-64206950.

Zhao Geng. “An Analysis of Cyberspace Rule-Making in China-U.S. Relations.” *International Relations and Diplomacy* 6, no. 1 (January 28, 2018). https://doi.org/10.17265/2328-2134/2018.01.002.

Zhen, Liu. “Were China’s Earthquake Tracking Stations Hacked for Military Secrets by US?” South China Morning Post, July 28, 2023. https://www.scmp.com/news/china/diplomacy/article/3229258/were-chinas-earthquake-tracking-stations-hacked-military-secrets-us.

Zhou, Hongren. “Strategic Stability in Cyberspace: A Chinese View.” *China Quarterly of International Strategic Studies* 05, no. 01 (January 2019): 81–95. https://doi.org/10.1142/S2377740019500088.

Федонюк, Сергій, and Сергій Магдисюк. “US-China Confrontation in Cyber Security.” *Історико-Політичні Проблеми Сучасного Світу*, no. 45 (June 27, 2022): 113–27. https://doi.org/10.31861/mhpi2022.45.113-127.

癸卯年腊月十一 People’s Daily. “US’s Most Powerful Cyberattack System Is Targeting China: Sources,” March 22, 2022. https://peoplesdaily.pdnews.cn/tech/er/30001213112.