



Parahyangan Catholic University
Faculty of Social and Political Sciences
Department of International Relations

Terkreditasi Unggul

SK BAN-PT NO:2579/SK/BAN-PT/AK-ISK/S/IV/2022

**The US as a Cyber Superpower and the Reluctance to
Establish Cyberspace International Legal Framework**

Undergraduate Thesis

By

Michelle Nagakanya Putrika Tandy

6091901004

Bandung

2022



Parahyangan Catholic University
Faculty of Social and Political Sciences
Department of International Relations

Terakreditasi Unggul

SK BAN-PT NO:2579/SK/BAN-PT/AK-ISK/S/IV/2022

**The US as a Cyber Superpower and the Reluctance to
Establish Cyberspace International Legal Framework**

Undergraduate Thesis

By

Michelle Nagakanya Putrika Tandy

6091901004

Advisor

Idil Syawfi, S.IP., M.Si.

Bandung

2022

Fakultas Ilmu Sosial dan Ilmu Politik
Jurusan Hubungan Internasional
Program Studi Hubungan Internasional Program Sarjana



Tanda Pengesahan Skripsi

Nama : Michelle Nagakanya Putrika Tandy
Nomor Pokok : 6091901004
Judul : *The US as a Cyber Superpower and the Reluctance to Establish Cyberspace International Legal Framework*

Telah diuji dalam Ujian Sidang jenjang Sarjana
Pada Senin, 16 Januari 2023
Dan dinyatakan **LULUS**

Tim Penguji

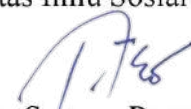
Ketua Sidang merangkap Anggota
Adrianus Harsawaskita, S.IP., M.A.

Sekretaris
Idil Syawfi, S. IP., M.Si.

Anggota
Angguntari Ceria Sari, S. IP., M. Sc .

: 
: 
: 

Mengesahkan,
Dekan Fakultas Ilmu Sosial dan Ilmu Politik


Dr. Pius Sugeng Prasetyo, M.Si.

DAFTAR PERBAIKAN NASKAH SKRIPSI

Nama : Michelle Nagakanya Putrika Tandy
Nomor Pokok Mahasiswa : 6091901004
Program Studi : Hubungan Internasional
Pembimbing : Idil Syawfi, S.IP., M.Si. (20110153) Pembimbing Tunggal
Hari dan tanggal ujian skripsi : Senin tanggal 16 January 2023
Judul (Bahasa Indonesia) : Amerika Serikat sebagai Adikuasa Ruang Siber dan Keengganan untuk Menetapkan Kerangka Legal Internasional untuk Ruang Siber
Judul (Bahasa Inggris) : The US as a Cyber Superpower and the Reluctance to Establish Cyberspace International Legal Framework

1. Perbaikan Judul Skripsi menjadi (**Judul harus ditulis lengkap menggunakan huruf besar kecil/Title Case**)

Judul (Bahasa Indonesia)

Judul (Bahasa Inggris)

2. Perbaikan Umum (meliputi : cara merujuk, daftar pustaka, teknis editing) :

3. Perbaikan di Bab 1
Teori: bukan teori tentang kebijakan negara tetapi hukum internasional. Karena berbicara communities.
Masukan: teorinya bisa di rekonstruksi agar pas dengan sudut pandang penelitian.
Fokuskan pertanyaan penelitian terkait legal framework yang mana yang Amerika Serikat enggan untuk menginisiasi.
Gunakan teori yang bisamembantu menjelaskan perilaku negara dalam multilateralisme.

4. Perbaikan di Bab 2
Buktikan keengganan Amerika Serikat dalam menginisiasi legal framework , kategori yang mana.
Jelaskan lebih lanjut maksud dari table 2.1.
Explain what is the strength and weaknesses of current framework
Combine chapter 2 and 3 into one chapter. And focus on the analysis in chapter 3.

5. Perbaikan di Bab 3

6. Perbaikan di Bab 4

7. Perbaikan di Bab 5

DOKUMEN INI TIDAK PERLU DITANDATANGANI LAGI

Bandung, 16 January 2023

Ketua Program Studi,

kaprodi_hi.fisip@unpar.ac.id
1/16/2023 9:14:52

Vrameswari Omega Wati, S.IP., M.Si. (Han)

Penguji,

adri@unpar.ac.id
1/16/2023 9:00:13

Adrianus Harsawaskita, S.IP., M.A.

Penguji (Pembimbing),

idil.syawfi@unpar.ac.id
1/16/2023 9:01:55

Idil Syawfi, S.IP., M.Si.

Penguji,

anggunтари@unpar.ac.id
1/16/2023 9:02:03

Anggunтари Ceria Sari, S.IP., M.Sc.

PREFACE

Praise to the Almighty God for His blessings, without His guidance and strength the author would not have been able to finish her undergraduate study by completing this thesis titled “The US as a Cyber Superpower and the Reluctance to Establish Cyberspace International Legal Framework.”

This thesis will explain the reason behind the US’s reluctant behaviour towards establishing cyberspace international legal framework despite being a cyber superpower. Through exhibiting the US’ cyber power in different means; technical, institutional, legal, and so on and so forth, this thesis will portray how the US is as powerful in this contemporary domain just as they are in any other domain. Furthermore it will explain how establishing the cyberspace international legal framework is perceived strategically by the US.

This undergraduate thesis serves as the requirement of acquiring the Bachelor degree of International Relations Department, Faculty of Social and Political Sciences, Parahyangan Catholic University. Regardless of the challenges and obstacles faced during the research and writing process of this thesis the author has managed to pull through with the help of significant lecturers, family and friends in many ways. However, this research is far from perfect and the author is open and would very appreciate inputs for further improvements.

ACKNOWLEDGEMENTS

The short yet challenging journey of writing this thesis would not be very hard, if not impossible, for the author to complete. Having to juggle many things at once while trying to keep the writing process on track, this author has been challenged with insecurity and sometimes demotivation. Fortunately, the author has been surrounded by people; lecturer, family, and friends who have been supporting the author throughout the entire process. In this opportunity, the author would like to express her utmost gratitude to the people who, not only have been there since the beginning, but also those whom the author has met along the way and have stayed until the end. Hereby I present;

1. To Papi, this thesis is dedicated to you. During my undergraduate study I have rediscovered a field of interest that is so familiar and so you, cybersecurity. If you were still with us, I am sure we would geek out during my late-night research together, the way you stayed up all night to fight hackers. I hope I have made you proud.
2. To Mami, my strength and faith through the worst rainstorm. I could never thank you enough for all the support, reassurances, and most importantly your prayers that always accompany my journey, wherever its heading towards. Thank you for all the all-nighters you have pulled with me and all the affections and faith in me throughout the writing of my thesis.
3. To Mas Idil, thank you for all your thoughtful and detailed guidance in the process of researching and writing my thesis. If it was not because of your

guidance, inputs, and comments this thesis would have gone in a completely different direction, one that might not be as how I ambitiously aimed it to be. I could never thank you enough for your patience, tolerance, and optimism throughout the process that has been motivating and inspirational.

4. To Keyne Nathania, thank you for your never-ending support and prayers from miles away. Despite having no clue of what is going in each other's life most of the time, I know you always carry me in your prayers and wishes.
5. To Mattea Marjorie Tane, thank you for always catering to my big delusional dreams and making things make sense to me. I could not possibly have done it without your constant explicit "I am proud of you" s that becomes the best pick me up through my thesis journey. Of course, thank you for all the Bandung study sessions, will definitely miss them.
6. To Varaditya Syadilla, thank you for always making time to see me just to accompany me work on my thesis every week. You have been the best companion throughout, not only my thesis journey, but my entire journey in Unpar.
7. To Shofaa Fairuuz Salsabila Respati. Thank you for always reminding me of the small things to look forward to in life, in this case snatching my degree. You are my constant reminder that things will definitely get hard once in a while, but we will always pull through. I would not have seen the end of this thesis journey if you were not there.

8. To Joris Wiersma, thank you for constantly checking up on me and endlessly supporting me since the day we met. Moreover, thank you for the many times you reminded me to have fun and to slow down when I unnecessarily rushed my way through things. You have your own quirky way of showing support and I am utterly grateful for that.
9. To Dimas Andito Muhammad, my grizzly bear. Thank you for always being one call away and for giving me the goofy confidence I need to finish my thesis.
10. To Rafa Ammaara, the little sister I never had. You might think you are in this list just because of the coffee and cookies you sent me, but your role has been much more significant in the process of finishing my thesis. Thank you for curing my thesis anxiety with your TikTok DMs and new celebrity crushes every week and of course, for giving me a reason to keep moving forward.
11. To Mba Izdihar Nur Adiba, the older sister I never had. Thank you for being my ultimate supporter while I struggled to juggle my thesis with my internship.
12. To Alana Maria, Elisabeth Pricilla, and Cinantya Pragnya Nyasa Dewi, *mes amis*. Thank you for being helpful and supportive when I had to juggle between finishing my thesis in two days and Diplomacy in Practice. You are the best people that I could ever ask for to be my delegation. *Merci Beaucoup*.

13. To Brigitta Valerie, Clara Serepina Tesalonika Bernath, Hasya Arrumaisha, Madeleina Renarda, Axtell Giuseppe Chrysallino Teguh, and Elbert Gerardo Chen, my day ones. Thank you for the unexpected random check-ins, for never letting me feel like I am alone in this entire journey. I am proud of how far we have come and am looking forward to seeing you on top.
14. To IREC 2022, who I cannot mention one by one. Thank you for giving me a reason to keep fighting this constant battle. It was a challenge taking care of you while working on this but you were also the reason behind my perseverance.
15. To IREC Ambassadors and Rookies; Tasya, Gina, Vieca, Anya, Tira, Jeni, Iki, Keidi, Jess, Ashton, Mitha, Alexa, Nike, and Shiddiq. Thank you for being the most supportive crowd, for reminding me that I do not need anyone else's validation while giving me yours. You were the breath of fresh air during the last few most stressful moment of my thesis journey I never thought I needed.
16. To Mentor Chevalier. For being the most supportive people from even before I started this thesis journey. So long, Chevs.
17. To Ashton Fletcher Irwin, for unintentionally keeping me entertained, happy, and being the reason behind my tears-free thesis journey. Everytime I thought of giving up and failing, you were the voice in my head telling me to take a break and celebrate the small victories, the progresses that I have made.

18. To 5 Seconds of Summer, my rediscovered comfort band. Thank you for your wonderful music. There had not been one day spent during my thesis journey not listening to your entire discography on repeat, the daily dose of serotonin 24/7.
19. Last but not least, Michelle. I am proud of you for surviving this journey, for overcoming your insecurities, picking yourself up pieces by pieces and getting yourself up and running to achieve this. Here is to achieving more of your big dreams. This is the feeling of falling upwards.

Table of Contents

Abstract	i
Abstrak	ii
Preface	iii
Acknowledgements	iv
Table of Contents	ix
List of Tables	x
List of Charts	xi
List of Figures	xii
1. Introduction	
1.1. Research Background	1
1.2. Problem Identification.....	5
1.2.1. Scope of the Research	7
1.2.2. Research Question	7
1.3. The Purpose and Utility of Research.....	8
1.3.1. Purpose of the Research	8
1.3.2. Utility of the Research	9
1.4. Literature Review	9
1.5. Theoretical Framework	13
1.5.1. Great Powers and Responsibility	13
1.6. Research Methods	16
1.7. Structure of the Research	17
2. The US: A Cyber Superpower and Existing Cyber Norms	
2.1. US Cyber Power Measured	19
2.1.1. US Cyber Strategies and Doctrines.....	20
2.1.2. US Cyber Governance, Command and Control	26
2.1.3. US Core Cyber-Intelligence Capability	32
2.1.4. US Cyber Empowerment and Dependence	35
2.1.5. US Cybersecurity and Resilience	41
2.1.6. US Global Leadership in Cyberspace Affairs	47
2.1.7. Offensive Cyber Capability	51
2.2. Insufficiency of Existing Cyber Norms	53
3. The Absence of Responsibility to Establish Cyberspace International Legal Framework	
3.1. Minimum Accordance between the US as a Systemic Great Power and Cyber Superpower	61
3.2. Correlation between Cybersecurity and Preservation of International Order.....	64
3.3. Assignment of Responsibilities and Privileges or Rights in the Cyberspace for the US.....	68
3.4. Absence of the US' Responsibility to Establish Cyberspace International Legal Framework	71
4. Conclusion	
Bibliography	79

List of Tables

Table 2.1. Existing Cyber Norm	54
--------------------------------------	----

List of Charts

Chart 2.1. US Year to Year Budget Forecast Increase for Federal Government IT (2017-2022)	24
Chart 2.2. US 2022 FY Federal Government IT Budget Allocation	26
Chart 2.3. Dominating Sectors of US 2021 Digital Economy Total Production ..	40
Chart 2.4. US 2021 ICT Product Exports and Imports	41

List of Figures

Figure 2.1. Investment Allocated for ICT Research and Development 40

Abstract

Name : Michelle Nagakanya Putrika Tandy

Student ID : 6091901004

Title : The US as a Cyber Superpower and the Reluctance to
Establish Cyberspace International Legal Framework

Acknowledging the security threats that prevail and continue to advance in the cyberspace, the US as a cyber superpower persists to safeguard the domain through operational, institutional, and ideological means. With the amount of power the US possesses in cyberspace they also have the interest and influence to legally regulate the domain to ensure its security. However, it seems that the US has not been showing any initiative to do so, to fill the void that has been a loophole exploited as open doors for cyber threats. While theoretically, establishment of cyberspace international legal framework can be addressed as a special responsibility that entails the US' cyber superpower status. To answer this anomaly, this thesis applies the theory of great powers and responsibility to understand how establishment of cyberspace international legal framework have been formulated and assigned as a responsibility to the US as a cyber superpower. The analysis exposes how such measure of norm setting in global cyber governance have failed to be formulated and assigned to the US. Lack of moral imperative and normative embodiment that should otherwise be attached to the status of superpower leaves the US' responsibility as a cyber superpower to be a mere embodiment of their interests. Instead, the US have chosen to resort to other means to show their responsibility as they find it to be more benefitting than establishing cyberspace international norms could be.

Keywords: *The US, cyberspace, cybersecurity, cyber superpower, cyber norms, cyber strategy, international legal framework, great power, responsibility*

Abstrak

Nama : Michelle Nagakanya Putrika Tandy

NPM : 6091901004

Judul : AS Sebagai Adikuasa Siber dan Keengganan untuk Menetapkan Kerangka Legal Internasional untuk Ruang Siber

Mengetahui adanya ancaman keamanan yang terus berkembang dan semakin kompleks di ruang siber, AS sebagai adikuasa siber bersikeras untuk menjadi keamanan domain ini melalui metode-metode operasional, institusional, dan ideologis. Dengan kekuatan yang begitu signifikan, AS memiliki kepentingan dan pengaruh untuk meregulasi ruang siber secara legal dalam rangka menjaga keamanannya. Tetapi, nampaknya AS tidak menunjukkan inisiatif untuk melakukan hal tersebut, untuk mengisi ruang kosong yang selama ini dieksploitasi sebagai pintu masuk ancaman siber. Secara teoritis, penetapan kerangka legal internasional di ruang siber bisa dikategorikan sebagai tanggung jawab spesial yang menempel pada kepemilikan status adikuasa siber AS. Untuk menjawab anomaly ini, penelitian ini mengaplikasikan teori great powers dan tanggung jawab untuk menjelaskan bagaimana penetapan kerangka legal internasional di ruang siber diformulasikan dan diberikan kepada AS sebagai adikuasa ruang siber. Analisis mengekspos bagaimana pembuatan norma seperti itu telah gagal untuk diformulasikan dan diberikan kepada AS sebagai bentuk tanggung jawab adikuasa ruang siber. Kurangnya tekanan moral serta perwujudan normatif yang seharusnya menempel pada kepemilikan status adikuasa membiarkan tanggung jawab AS sebagai adikuasa ruang siber menjadi sebatas media perwujudan kepentingan AS. Alih-alih, AS memilih untuk menunjukkan tanggung jawabnya melalui cara lain yang dianggap lebih menguntungkan daripada penetapan kerangka legal internasional di ruang siber.

Keywords: *The US, cyberspace, cybersecurity, cyber superpower, cyber norms, cyber strategy, international legal framework, great power, responsibility*

PREFACE

Praise to the Almighty God for His blessings, without His guidance and strength the author would not have been able to finish her undergraduate study by completing this thesis titled “The US as a Cyber Superpower and the Reluctance to Establish Cyberspace International Legal Framework.”

This thesis will explain the reason behind the US’s reluctant behaviour towards establishing cyberspace international legal framework despite being a cyber superpower. Through exhibiting the US’ cyber power in different means; technical, institutional, legal, and so on and so forth, this thesis will portray how the US is as powerful in this contemporary domain just as they are in any other domain. Furthermore it will explain how establishing the cyberspace international legal framework is perceived strategically by the US.

This undergraduate thesis serves as the requirement of acquiring the Bachelor degree of International Relations Department, Faculty of Social and Political Sciences, Parahyangan Catholic University. Regardless of the challenges and obstacles faced during the research and writing process of this thesis the author has managed to pull through with the help of significant lecturers, family and friends in many ways. However, this research is far from perfect and the author is open and would very appreciate inputs for further improvements.

ACKNOWLEDGEMENTS

The short yet challenging journey of writing this thesis would not be very hard, if not impossible, for the author to complete. Having to juggle many things at once while trying to keep the writing process on track, this author has been challenged with insecurity and sometimes demotivation. Fortunately, the author has been surrounded by people; lecturer, family, and friends who have been supporting the author throughout the entire process. In this opportunity, the author would like to express her utmost gratitude to the people who, not only have been there since the beginning, but also those whom the author has met along the way and have stayed until the end. Hereby I present;

1. To Papi, this thesis is dedicated to you. During my undergraduate study I have rediscovered a field of interest that is so familiar and so you, cybersecurity. If you were still with us, I am sure we would geek out during my late-night research together, the way you stayed up all night to fight hackers. I hope I have made you proud.
2. To Mami, my strength and faith through the worst rainstorm. I could never thank you enough for all the support, reassurances, and most importantly your prayers that always accompany my journey, wherever its heading towards. Thank you for all the all-nighters you have pulled with me and all the affections and faith in me throughout the writing of my thesis.
3. To Mas Idil, thank you for all your thoughtful and detailed guidance in the process of researching and writing my thesis. If it was not because of your

guidance, inputs, and comments this thesis would have gone in a completely different direction, one that might not be as how I ambitiously aimed it to be. I could never thank you enough for your patience, tolerance, and optimism throughout the process that has been motivating and inspirational.

4. To Keyne Nathania, thank you for your never-ending support and prayers from miles away. Despite having no clue of what is going in each other's life most of the time, I know you always carry me in your prayers and wishes.
5. To Mattea Marjorie Tane, thank you for always catering to my big delusional dreams and making things make sense to me. I could not possibly have done it without your constant explicit "I am proud of you" s that becomes the best pick me up through my thesis journey. Of course, thank you for all the Bandung study sessions, will definitely miss them.
6. To Varaditya Syadilla, thank you for always making time to see me just to accompany me work on my thesis every week. You have been the best companion throughout, not only my thesis journey, but my entire journey in Unpar.
7. To Shofaa Fairuuz Salsabila Respati. Thank you for always reminding me of the small things to look forward to in life, in this case snatching my degree. You are my constant reminder that things will definitely get hard once in a while, but we will always pull through. I would not have seen the end of this thesis journey if you were not there.

8. To Joris Wiersma, thank you for constantly checking up on me and endlessly supporting me since the day we met. Moreover, thank you for the many times you reminded me to have fun and to slow down when I unnecessarily rushed my way through things. You have your own quirky way of showing support and I am utterly grateful for that.
9. To Dimas Andito Muhammad, my grizzly bear. Thank you for always being one call away and for giving me the goofy confidence I need to finish my thesis.
10. To Rafa Ammaara, the little sister I never had. You might think you are in this list just because of the coffee and cookies you sent me, but your role has been much more significant in the process of finishing my thesis. Thank you for curing my thesis anxiety with your TikTok DMs and new celebrity crushes every week and of course, for giving me a reason to keep moving forward.
11. To Mba Izdihar Nur Adiba, the older sister I never had. Thank you for being my ultimate supporter while I struggled to juggle my thesis with my internship.
12. To Alana Maria, Elisabeth Pricilla, and Cinantya Pragnya Nyasa Dewi, *mes amis*. Thank you for being helpful and supportive when I had to juggle between finishing my thesis in two days and Diplomacy in Practice. You are the best people that I could ever ask for to be my delegation. *Merci Beaucoup*.

13. To Brigitta Valerie, Clara Serepina Tesalonika Bernath, Hasya Arrumaisha, Madeleina Renarda, Axtell Giuseppe Chrysallino Teguh, and Elbert Gerardo Chen, my day ones. Thank you for the unexpected random check-ins, for never letting me feel like I am alone in this entire journey. I am proud of how far we have come and am looking forward to seeing you on top.
14. To IREC 2022, who I cannot mention one by one. Thank you for giving me a reason to keep fighting this constant battle. It was a challenge taking care of you while working on this but you were also the reason behind my perseverance.
15. To IREC Ambassadors and Rookies; Tasya, Gina, Vieca, Anya, Tira, Jeni, Iki, Keidi, Jess, Ashton, Mitha, Alexa, Nike, and Shiddiq. Thank you for being the most supportive crowd, for reminding me that I do not need anyone else's validation while giving me yours. You were the breath of fresh air during the last few most stressful moment of my thesis journey I never thought I needed.
16. To Mentor Chevalier. For being the most supportive people from even before I started this thesis journey. So long, Chevs.
17. To Ashton Fletcher Irwin, for unintentionally keeping me entertained, happy, and being the reason behind my tears-free thesis journey. Everytime I thought of giving up and failing, you were the voice in my head telling me to take a break and celebrate the small victories, the progresses that I have made.

18. To 5 Seconds of Summer, my rediscovered comfort band. Thank you for your wonderful music. There had not been one day spent during my thesis journey not listening to your entire discography on repeat, the daily dose of serotonin 24/7.
19. Last but not least, Michelle. I am proud of you for surviving this journey, for overcoming your insecurities, picking yourself up pieces by pieces and getting yourself up and running to achieve this. Here is to achieving more of your big dreams. This is the feeling of falling upwards.

Table of Contents

Abstract	i
Abstrak	ii
Preface	iii
Acknowledgements	iv
Table of Contents	ix
List of Tables	x
List of Charts	xi
List of Figures	xii
1. Introduction	
1.1. Research Background	1
1.2. Problem Identification.....	5
1.2.1. Scope of the Research	7
1.2.2. Research Question	7
1.3. The Purpose and Utility of Research.....	8
1.3.1. Purpose of the Research	8
1.3.2. Utility of the Research	9
1.4. Literature Review	9
1.5. Theoretical Framework	13
1.5.1. Great Powers and Responsibility	13
1.6. Research Methods	16
1.7. Structure of the Research	17
2. The US: A Cyber Superpower and Existing Cyber Norms	
2.1. US Cyber Power Measured	19
2.1.1. US Cyber Strategies and Doctrines.....	20
2.1.2. US Cyber Governance, Command and Control	26
2.1.3. US Core Cyber-Intelligence Capability	32
2.1.4. US Cyber Empowerment and Dependence	35
2.1.5. US Cybersecurity and Resilience	41
2.1.6. US Global Leadership in Cyberspace Affairs	47
2.1.7. Offensive Cyber Capability	51
2.2. Insufficiency of Existing Cyber Norms	53
3. The Absence of Responsibility to Establish Cyberspace International Legal Framework	
3.1. Minimum Accordance between the US as a Systemic Great Power and Cyber Superpower	61
3.2. Correlation between Cybersecurity and Preservation of International Order.....	64
3.3. Assignment of Responsibilities and Privileges or Rights in the Cyberspace for the US.....	68
3.4. Absence of the US' Responsibility to Establish Cyberspace International Legal Framework	71
4. Conclusion	
Bibliography	79

List of Tables

Table 2.1. Existing Cyber Norm	54
--------------------------------------	----

List of Charts

Chart 2.1. US Year to Year Budget Forecast Increase for Federal Government IT (2017-2022)	24
Chart 2.2. US 2022 FY Federal Government IT Budget Allocation	26
Chart 2.3. Dominating Sectors of US 2021 Digital Economy Total Production ..	40
Chart 2.4. US 2021 ICT Product Exports and Imports	41

List of Figures

Figure 2.1. Investment Allocated for ICT Research and Development 40

CHAPTER 1

INTRODUCTION

1.1. Research Background

The ever-rising utilization of cyberspace has become globally undeniable, creating opportunities and challenges. Any word with “cyber” as a prefix would automatically be associated with digitalization by computers and other electronic devices, meaning that modernization has pushed global civilization towards progressive digitalization and automation.¹ Unlike any other territory or space, cyberspace interconnects the world, topples traditional boundaries, and henceforth challenges the concept of state sovereignty.² Despite its significance to modern civilization and utilization daily, debates still surround cyberspace, even from the most fundamental aspect: its definition.

After more than two decades of development and rising significance, cyberspace has not yet had a universal definition or understanding that states consensually accept and use. States and non-state actors still struggle to entirely understand the nature of cyberspace as it is distinctly different from territories, areas, or spaces known before. Furthermore, states cannot keep up with the growth pace as proven by how until now there is still not one clear definition of cyberspace accepted globally until now.³ This lack of

¹ Joseph S Nye, *The Future of Power* (New York: Public Affairs, 2011), 18.

² Ibid, 21.

³ Kubo Mačák, “From Cyber Norms to Cyber Rules: Re-Engaging States as Law-Makers,” *Leiden Journal of International Law* 30 (2017): 889, <https://ssrn.com/abstract=2961821>.

understanding is rooted in the non-existence of cyberspace's physical territory, making it challenging to understand and define and determine its borders and reach.⁴ According to Joseph Nye, cyberspace is identified as a space of information access and exchange through hardware and software facilities connected to the internet.⁵ Furthermore, Nye defined cyberspace as a layered physical infrastructure subject to the economic laws of resources and political laws of sovereignty and control. As a domain of unlimited utilization probability, cyberspace, just like any other space or territory, becomes a subject of power projection and conflict.

The contemporary and anomalous nature of cyberspace leaves it only partially explored, with many possibilities of utilization left to discover and blind spots to exploit. Many entities, state and non-state, have been utilizing this domain to their advantage by intervening in others' sovereignty in this domain, causing economic losses, political disarray, and even putting lives in danger, especially when critical infrastructures and industries are involved.⁶ Cybersecurity becomes an unavoidable consequence of rapid digitalization and automation, exposing cyber vulnerabilities in plain sight.⁷ Moreover, the interconnectedness reached globally now gives more advantages to those who

⁴ Brandon Valeriano and Ryan C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System*, (Oxford: Oxford University Press, 2015), 35.

⁵ Joseph S Nye, *The Future of Power* (New York: Public Affairs, 2011), 19.

⁶ Brandon Valeriano and Ryan C. Maness, "International Relations Theory and Cybersecurity: Threats, Conflicts, and Ethics in an Emergent Domain," in *The Oxford Handbook of International Political Theory* ed. Chris Brown and Robyn Eckersley, (Oxford: Oxford University Press, 2018), 287.

⁷ J.R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22 (3): 367.

intend to misuse cyberspace to conduct illicit activities.⁸ Hence, the nature of cyberspace allows states to be unlimitedly competitive in utilizing the domain and even in executing misconduct and illicit activities for their advantage.

How power is projected and measured in cyberspace is still a matter of debate and research, but first, how power is defined and perceived in this domain must be understood. As Nye already defined cyberspace as an infrastructure capable of accommodating political and economic activities, why cyberspace can be a place of power projection should be prominent. Hannah Ardent's concept of power can be referenced as she argued that power should be contextualized according to the space of its appearance.⁹ It was tracing back the origin of international relations discourse, the emergence of power first identified within Greek polis, a space of public democracy in which everyone was perceived as equal and had the same chances of having a public opinion.¹⁰ Later in history, power always appears in spaces or circumstances where political freedom thrives and suffices. Applying Ardent's conceptualization of power to the definition of cyberspace by Nye, it can be understood that as cyberspace becomes more viable for the accommodation of political and economic activities, the tendency of power to emerge within the domain rises.

⁸ Kubo Maćák, "From Cyber Norms to Cyber Rules: Re-Engaging States as Law-Makers," *Leiden Journal of International Law* 30 (2017):889, <https://ssrn.com/abstract=2961821>.

⁹ Joseph Marks, "The Cybersecurity 202: The United States Is Still Number One in Cyber Capabilities," *Washington Post*, June 28, 2021, <https://www.washingtonpost.com/politics/2021/06/28/cybersecurity-202-united-states-is-still-number-one-cyber-capabilities/>.

¹⁰ Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cybersecurity, and the Copenhagen School," *International Studies Quarterly* 53: 1165.

The strata of power in cyberspace might differ from how it is in conventional international politics, but the United States of America still holds significant power even in this partially explored domain. Valerio and Maness define cyber power as the capability to exhibit control and domination in cyberspace.¹¹ The US is considered one of the few countries with most resources in cyberspace and has been making significant advancements within its cyber infrastructure, allowing them the advantage of leading cyber capabilities and security strategies.¹² This reputation has earned the US the title of cyber superpower in most cybersecurity discourses.

As a cyber superpower, the US has exercised legal and practical measures to safeguard its cybersecurity. Amongst all things, the US has advanced cyber military operations designated to defend and retaliate against any cyber threats towards the US.¹³ They have also been collaborating in joint cyber operations within international and regional organizations like the North Atlantic Treaty Organization (NATO), thereby safeguarding international cybersecurity. Other than that, the US has bilateral agreements on cyber activities with allies, which include the emphasis on responsible conduct in cyberspace, and ensuing consequences shall any agreeing parties ever conduct illicit cyber activities that might harm and also put other nations at a disadvantage. At the same time,

¹¹ Brandon Valeriano and Ryan C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System*, (Oxford: Oxford University Press, 2015), 28.

¹² Joseph Marks, "The Cybersecurity 202: The United States Is Still Number One in Cyber Capabilities," *Washington Post*, June 28, 2021, <https://www.washingtonpost.com/politics/2021/06/28/cybersecurity-202-united-states-is-still-number-one-cyber-capabilities/>.

¹³ Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cybersecurity, and the Copenhagen School," *International Studies Quarterly* 53: 1167.

domestically, the US has been highlighting cyberspace in its domestic legislation and national security plan. Although the US has been exhibiting its cyber capabilities in defensive and offensive measures, that does not guarantee its security in cyberspace. Again, due to global interconnectivity and the rapid advancement of automation and digitalization, the US is just as vulnerable as any other state in cyberspace.

1.2. Problem Identification

Despite the acknowledgement of rising exploitation of cyberspace by states, which supposedly raises the need for an international legal framework to conduct activities in the domain, such framework does not exist just yet. There has not been any proactiveness from states to establish an international framework in the cyberspace, which pushes non-state actors and institutions to fill in the gap.¹⁴ However, non-state actors do not have the mandate and power to establish binding international legal frameworks. Therefore, non-state actors and institutions have filled the gap by establishing cyber norms however it is not fulfilling enough to deter states from conducting harming exploitation of cyberspace.

The notion that existing applicable international law in cyberspace is not impactful to safeguard the cyberspace as its focus is inaccurate. As argued by Hansen and Nisserbaum, the majority of literature on cybersecurity, tend to

¹⁴ Kubo Mačák, "From Cyber Norms to Cyber Rules: Re-Engaging States as Law-Makers," papers.ssrn.com (Rochester, NY, April 27, 2017), 889, <https://ssrn.com/abstract=2961821>.

overexaggerate the scale of cyber threat itself, especially regarding its threat assessment and prediction, putting the spotlight on cyber war.¹⁵ War itself is defined by Clausewitz as the exploitation of violence and death to reach political goals.¹⁶ Meanwhile, more often the majority of threats in cyberspace can be characterized as low-impact threats like espionage, spying, and Denial of Service—these are effective enough to reach strategic objectives but does not necessarily put lives in danger, although it's possible if critical infrastructures are badly attacked. Therefore, cyberspace demands a special and more specified international legal framework that puts the spotlight on the utilization of cyber technology for malicious purposes to achieve security or diplomatic objectives.¹⁷

With the understanding of the insecurity prospects in the cyberspace and its fatal implications to state and international security, it is imperative that this domain is ruled under an international legal framework—of which, the US as a cyber superpower has the influence, power, and interest needed to initiate its establishment. Faced with comparable issues in other contemporary territory such as the outer space and the Arctic, the US had been proactive in initiating the establishment of international legal frameworks for both.¹⁸ The result of these initiatives have been recognized as the basis of security in both

¹⁵ Brandon Valeriano and Ryan C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System*, (Oxford: Oxford University Press, 2015), 21.

¹⁶ Kubo Mačák, “From Cyber Norms to Cyber Rules: Re-Engaging States as Law-Makers,” *papers.ssrn.com* (Rochester, NY, April 27, 2017), 889, <https://ssrn.com/abstract=2961821>.

¹⁷ Brandon Valeriano and Ryan C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System*, (Oxford: Oxford University Press, 2015), 36.

¹⁸ Lene Hansen and Helen Nissenbaum, “Digital Disaster, Cybersecurity, and the Copenhagen School,” *International Studies Quarterly* 53: 1167.

territories. As one with enough resources and influence in the cyberspace, the US could do the same, and thus not only guarantee their national security but also foster international security in the cyberspace.

Having exhibited its power in cyberspace, proving its claim as one of the cyber superpowers while also having strong political power and influence in international politics, the US should be capable of initiating global cooperation to establish an international legal framework on cyberspace. This step is not something they have not done before nor gained an advantage from in another case of territory. In fact, for decades, the US has been the driving force behind the establishment of many international legal frameworks for contemporary territories or security issues.

1.2.1.Scope of the Research

In order to narrow down the scope of this research, the following analysis will be limited to the US cybersecurity strategy, be it through policies, technical operations, and capacity building. The scope of research will focus on the cyber strategy measures done by cyber superpower, the United States of America observed until 2022.

1.2.2.Research Question

The absence of an international legal framework governing cyberspace is yet another gap to be filled. Fulfilling this gap would create certainty for states,

especially the US as a cyber superpower, in guaranteeing their cybersecurity. However, the status quo in a cyberspace international legal framework remains absent, instead filled by norms established by non-state actors. The US, as a cyber superpower, has exhibited its power and influence, not only in international politics but also specifically in cyberspace—have yet not persevered in attempts to initiate cyberspace international legal framework. Hence, it leads to the research question of **“Why is the US as a cyber Superpower reluctant to establish an international legal framework in cyberspace?”**

1.3.The Purpose and Utility of Research

1.3.1. Purpose of the Research

The main objective of this research is to show that the US is indeed one of the most powerful states in cyberspace which makes them a competent and credible actor to establish cyberspace international legal framework. However, there seems to be factors that hinder the US from doing so as up until now such framework does not exist yet. This research exhibits these hindering factors through exposing current conditions and adherence to existing non-binding cyber norms that could become a strategic consideration of the US. From that, these considerations are to answer why the US, regardless of the power they possess, have not been initiating the establishment of cyberspace international law for a strategic point of view.

1.3.2. Utility of Research

This research aims to contribute to the study of cybersecurity, in particular regarding cyber power, conflict, and strategy by taking assessments on the US cyber strategy. With this research being done, the writer expects it to be valuable to other researchers or any individual in particular who has interest in the field of cybersecurity and furthermore would like to understand the implications of one's cyber strategy to their attempt to pursue national interest. Moreover, this research also aims to assess the consequences that might appear upon trying to fill in the legal void currently existing in the cyberspace and how it affects the US in determining their cyber strategy.

1.4. Literature Review

Prior to starting with this research, pre-existing literature surrounding the topic of US cyber strategy, moreover how the option of legalization is considered or perceived and shaped their cyber policies, have been procured to map further direction and focus of this research. In summary, these procured literature exposes the debate on the favorability the establishment of a cyber international legal framework as part of US cyber strategy.

Ryan David Kiggins argued that being an initiator of the establishment of cyberspace legal framework could help the US in achieving their cybersecurity objective.¹⁹ By assessing existing policies, as well as understanding the drive

¹⁹ Ryan David Kiggins, "US Leadership in Cyberspace: Transactional Cybersecurity and Global Governance," in *Cyberspace and International Relations: Theory, Prospects and Challenges*, ed. J.F. Kremer and Benedikt Muller (Berlin: Springer-Verlag, 2014), 161-180.

that affects US policymakers' decision making, Kiggins emphasized how the US recognizes the significance of the Internet as a political and security domain. Furthermore, the objective of the US' cyber strategy is simply to ensure the domain's functionality. Henceforth, Kiggins asserts that in order to pursue the US' interest to ensure the global functionality of cyberspace, the US is indeed needed to step up as a leader in global cyber governance.

At first aligning with Kiggins' standpoint, Andreas Schmidt argued that international norms, if established by those in highest spot in the power strata, would give them advantages as an outcome. Schmidt perceived the cyberspace not as an anarchic domain but rather controlled through a networked system in which hierarchy still applies.²⁰ It is argued that the networked security approach allows alteration from within the established network in the cyberspace environment, or so called global cyber governance, including alterations done to put forth the networking actors' interests that makes it a more effective and rational approach. From there, Schmidt further explained several measures that can be implemented as a network, one of them being the establishment of international norms by those in the highest spot of the hierarchy. However, although Schmidt argued that this measure could give benefits to those who established it, he also emphasized on how this measure could cause backlash. Having the possibility of escalating the deterrence, causing bad reputation, and limiting the possible alterations within the

²⁰ Andreas Schmidt, "Hierarchies in Networks: Emerging Hybrids of Networks and Hierarchies for Producing Internet Security," in *Cyberspace and International Relations: Theory, Prospects and Challenges*, ed. J.F. Kremer and Benedikt Muller (Berlin: Springer-Verlag, 2014), 181-202.

network, establishment of international norms would be more restraining than benefitting. Hence, it can be concluded that Schmidt does not recommend it as a strategy.

Reflecting Schmidt's sentiment, Tim Stevens argued that establishment of a cyberspace international legal framework perceived as a deterrence strategy would be redundant.²¹ In perceiving establishment of international legal framework, Stevens categorized it under a normative cyber deterrence strategy. As often mentioned in discourses on cybersecurity strategy, deterrence in the cyberspace through military approach is something that has not yet been proven, regardless of the measures being deployed to pursue it. Pursuing deterrence through 'softer' approach - the establishment of norms - also does not guarantee that it will have a chance to be carried out. Stevens argued that, indeed, the establishment of international legal framework would be significant, especially in determining the limitations of actions in cyberspace. To add into consideration, Stevens mentions how there is more effort needed to be put into international norm-making and negotiating their way into making others comply to it rather than military capacity building. Although Stevens acknowledges the potential impact in terms of limitations and sense of order in cyberspace should such international legal framework exist, the dominating projection of non-compliance makes it unfavorable to include this as a cybersecurity strategy.

Lastly, countering Stevens' pessimism, Zhixiong Huang and Kubo Mačák

²¹ Tim Stevens, "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace," *Contemporary Security Policy* 33(1): 148-170, DOI:10.1080/13523260.2012.659597.

reaffirmed optimism in the establishment of cyberspace international legal framework.²² At first, Huang and Mačák elaborated on the different original stances between China and the US regarding the international legal framework and how they clashed. However, they acknowledged that as both states representing the East and West have grown to possess better understanding of the interdependence that the cyberspace has created, as well as the consequences that came along with it, they have also been slowly progressing with small convergences. Despite the popular conception that states do not have a common understanding regarding cyber norms, it should be recognized that they have indeed reached a consensus regarding the applicability of the international law in cyberspace—although compliance is still yet an issue. Moving forward with this optimism, Huang and Mačák highlighted the real problem, that is within the application of the existing international law itself is deemed incompatible to the nature of cybersecurity threats, as they usually do not surpass the use of force threshold.

The four aforementioned literatures have given much consideration into this research on what is explored, where it is heading towards, and how it should be carried on. Seeing the existing debate within the discourse of cyberspace international law as an option for the US cybersecurity strategy, this research will focus on how the US as a cyber superpower possess the ability to initiate the establishment of cyberspace international legal

²² Zhixiong Huang and Kubo Mačák, “Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches,” *Chinese Journal of International Law* 16(2): 271-310, <https://doi.org/10.1093/chinesejil/jmx011>.

framework, and whether or not legalization would be a strategy of choice.

1.5.Theoretical Framework

In order to analyze the US' reluctance to establish cyberspace international legal framework, this research utilizes the theory of great powers and responsibility. This theory helps to understand the formulation and assignment of special responsibilities that entails the possession of great power status, in this case the US' possession of cyber superpower status. The debate and identification of possible missing links that might cause failure of formulation and assignment of responsibility helps to understand the stem of the US' reluctance to establish cyberspace international framework.

1.5.1. Great Powers and Responsibility

The link between great powers and their responsibility is explained by the English School (ES) scholars which stems from other international theories such as realism, neo-realism, liberalism, and constructivism. While some might argue that the term great power encompasses the ownership of capability and capacity to lead, Hedley Bull regarded the concept to have more normative and positive connotation. Based on Bull's argumentation, military capacity and capability are simply pre-determined variables of what consist of the concept

of great power.²³ Beyond that, the concept of great power is built on how one state is regarded by themselves and others of the possession of special rights and responsibilities. To combine both understanding, great power's capacity and capability to lead, if exerted effectively, would create an impression within states of what it means to be a great power which is usually followed with the connotation of possessing special rights and responsibilities in certain multilateral settings.

With that understanding, responsibility of great powers is argued to go beyond the expression of self-interest. Furthermore, it extends as a manifestation of moral imperative to validate and legitimate the special rights and authority that comes with the status of great power.²⁴ This validation and legitimation comes from normative social recognition from other states especially towards the additional burden that great powers are willing to carry as a cost of their special rights and authority. Henceforth, the status of great power is naturally costed with special responsibilities.

These responsibilities are then usually constituted under certain norms and rules to be abided. Although compliance is expected from all states but the great powers have extra moral burden to abide as it becomes one of the focal points of other states' assignment of their great power status.²⁵ Other states'

²³ Hedley Bull, "The great irresponsible? The United States, the Soviet Union, and world order," *International Journal: Canada's Journal of Global Policy Analysis* 35(3): 271-310, <https://doi.org/10.1177/002070208003500302>.

²⁴ Ian Clark, *Hegemony in International Society* (Oxford: Oxford University Press, 2011), 4-6.

²⁵ Steven Bernstein, "The absence of great power responsibility in global environment politics," *European Journal of International Relations* 1(25): 8-11, <https://doi.org/10.1177/002070208003500302>.

expectation and judgement towards the great powers fulfillment of responsibility can also be affected by how much they perceive the great powers are involved in the threats or insecurities happening in regards to certain issues. The more involved the great powers are the higher level of responsibility fulfillment is expected, if not higher degree than some sort of initiatives are expected of the great powers. This judgement can also be amplified by the managerial role great powers play within the international institutions that govern related issues.²⁶ Having the role of leaders within a global governance would level up expectations towards the great powers. Special and extra responsibilities of the great powers is not simply a manifestation of their interest to ensure their security but also a form of commitment of conflict management in the larger scope of international governance.

The absence of great powers responsibility on certain issue could indicate missing links between their status and the shaping of the responsibility itself. Borrowed from a theoretical framework originally applied to address the missing responsibility in environmental issues, this theory is also utilized for the same purpose in the issue of cybersecurity.²⁷ The missing links that can be analyzed as indicators that explains the US' absence of responsibility in establishing a cyberspace international legal framework are as follows; 1) the congruence of systemic and cyber powers; 2) correlation between cybersecurity and preservation of international order; and 3) association between assignment of responsibilities and privileges or rights in the cyberspace for the US.

²⁶ Ibid, 13.

²⁷ Ibid, 15-18.

1.6. Research Methods

In carrying out this research the method that will be utilized is qualitative research method. The focus of the qualitative research method is data collection, analysis, and writing.²⁸ The qualitative research method supports the analysis of study cases conducted in this research. In summary, the steps of the qualitative research method start with data collection which then will be followed by data analysis which furthermore will be processed into a comprehensive analysis of the research scope.²⁹ These steps are sufficient enough to conduct this research on cyber superpowers' behavior in cyberspace as well as their perspective on the non-existence of an international legal framework for cyberspace.

To carry on with this research, furthermore methods from the qualitative research method is utilized. The foundation of the method, as have previously been mentioned, is study case analysis which at its core relies on textual data. The qualitative research method aims to understand the context of how entities ascribe to social problems.³⁰ The method is chosen as it is deemed fitting to explain the issue in this research with the explanatory quality of this method. Furthermore, it is applied to discuss cyber superpowers' behavior in cyberspace

²⁸ John W. Creswell and J. David Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, Fourth (Thousand Oaks, CA, US: SAGE Publications, Inc, 2014).

²⁹ Ibid.

³⁰ Ibid.

and how they view the status quo on international legal framework for cyberspace.

To match the qualitative research method, the technique chosen to support this research focuses on text-based data that is able to give a comprehensive understanding of the issue.³¹ The technique heavily relies on literary study which means collected data will be in the form of documents, reports, and scholarly articles on cybersecurity issues that involve the cyber superpowers and also regarding international legal frameworks on cyberspace or any other related domain. These data are categorized as secondary data in this research method.³²

1.7. Structure of the Research

The research is constructed of four chapters. **Chapter I** consists of an introduction to the topic including background context of cyberspace advancement and possibility of threats due to illicit exploitation, the status quo of cyberspace international legal framework, and the US as a cyber superpower. Next, this chapter breaks down the identification and limitation of this research which is defined towards the US capability and capacity as a cyber superpower and what they have done that to initiate the establishment of cyberspace international legal framework. Other than that, purpose and utility of the

³¹ Umar Suryadi Bakry, *Metode Penelitian Hubungan Internasional*, (Yogyakarta: Pustaka Pelajar, 2016).

³² Ibid.

research, literature review, theoretical framework, and research methodology are also included in the chapter.

Chapter II, titled *The US: A Cyber Superpower and Existing Cyber Norms*, focuses on displaying US' cyber capacity and capabilities and currently existing cyber norms. First, this chapter explores the US' advanced cyber capacity and capability through International Institute of Strategic Studies (IISS) 7 indicators of cyber power net assessment. Next, is also explored, the currently existing cyber norms to give and understanding of why there needs to be a cyberspace international legal framework.

Chapter III is given the title *The Absence of Responsibility to Establish Cyberspace International Legal Framework* which provides analysis regarding the US' current status quo as a cyber superpower regarding establishment of cyberspace international legal framework. Utilizing the theory of great power sand responsibility this chapter elaborates how the US' reluctance is due to the absence of responsibility to do so that should otherwise be attached to its cyber superpower status.

Chapter IV consists of the conclusion of this research. This chapter is dedicated to answer the research question imposed in Chapter I as well as to completely fulfill the goal to have an analysis that gives understanding of US' view on the international legal framework on cyberspace.