CHAPTER IV

CONCLUSION

This research has explored the US capability that makes up their power in cyberspace, naming them the cyber superpower, through observation of 7 categories. Utilizing IISS net assessment measures, the US cyber power is explicitly exhibited in; (1) the US strategies and doctrines, (2) the US governance, command, and control, (3) the US core cyber-intelligence capability, (4) the US cyber empowerment and dependence, (5) the US cybersecurity and resilience, (6) the US global leadership in cyberspace affairs, and (7) the US offensive cyber capability. For its cyber governance, the US emphasizes the democratization of cyberspace, creating a free and open network for everyone, contrary to their counterparts' authoritative cyber governance. The advancement of their technology and digital economy has allowed them to adopt holistic, comprehensive cyber strategies covering cyber defense, offensive measures, cyber risk management and reduction, and retaliatory acts. In addition, their globalized digital economy has created a global digital dependence on the US as the sole supplier. In all sectors, the US is deemed to be dominating against other states, being more advanced and open but not necessarily secure.

Furthermore, it has been shown how the existing cyber norms are insufficient to cover the cyber threats that exist in recent days. Two characteristics can be highlighted from the currently existing cyber norms; non-binding and limited coverage. The existing cyber norms have limited coverage as they are formulated to be applications of previously existing international laws like IHL and LOAC, applying terms that are usually imposed in the context of traditional security in such a contemporary domain. Many threats are left unaddressed due to this which leads to the redundancy of the norms. In addition to that, several norms have been set specifically to rule out cyber activities but these norms have non-binding nature and most cyber activities that are ruled out although still exist but considered outdated. This calls for a legally binding framework that specifically addresses the issues in cyberspace.

Establishment of cyberspace international framework in this research has been addressed as a responsibility of the US as a cyber superpower. Through theoretical analysis, it has been displayed how such responsibility has failed to be formulated and assigned by the international community to the US due to factors such as; 1) lack of need for the US to legitimize their status as a cyber superpower; 2) non-existence of culpability as a creating factor of responsibility; 3) allowed flexibility for the US to choose the means to express their responsibility; 4) lack of incentive that can be offered to the US as a cyber superpower; 5) minimum moral imperative to adhere to norms and fulfil responsibilities. These factors are caused mostly by differing power dynamics in the systemic international order and global cyber governance, problem of attribution for cyber threats, as well as cyber capacity and capability disparity within states that causes global dependency to the US.

These findings accentuated the cost-benefit calculation of establishing a cyberspace international legal framework by the US, and it turns out that it would costs them more than it benefits. It is clear that the non-initiative of the US to establishment of cyberspace international legal framework is not an expectation of responsibility that has failed to be met. Rather, it is a responsibility that have never been formulated, addressed, and assigned by the international community within global cyber governance towards the US as a cyber superpower. Therefore, such norm making process exist as an option for the US that they can choose to resort to as a mean to show their responsibility of withholding a significant status in the domain. However, the process itself have been considered to be costly and burdensome for the US as they have to support the notion with initiatives to close the disparity that exist now and pursue the capability of attribution towards cyber threats. If such measures are not taken prior or along the establishment of cyberspace international legal framework, then it would end up being redundant just like the existing non-binding norms. The cost of this process if combined with the ever-existing high degree of global dependency towards the US to safeguard cyberspace becomes much burdensome for the US.

Meanwhile, the US could barely gain anything from it. Committing to fulfil this responsibility does not offer them any additional special rights and privileges more than what they already have now. Their special rights in decision making processes regarding cybersecurity have been ensured through the fulfillment of their responsibilities in the systemic international order. The privileges of technological advancement and access to information have also been procured through their ownership of cyber capacity and capability as well as conduct of cyber diplomacy, strategies, and operations. There seem to be nothing else at this point that could be offered or desired by the US as an incentive to voluntarily take the extra burden of responsibility.

In conclusion, the answer to why the US as a cyber superpower is reluctant to establish a cyberspace international legal framework is because responsibility of the US within the global cyber governance have only been a manifestation of their interests that does not extend to be a moral imperative nor a normative embodiment of their cyber superpower status. Not having much expectations of responsibilities attached to the status, the US have the liberty to choose the means they would like to use to express their responsibility. Establishment of cyberspace international legal framework have not been a rational option for the US as according to the calculation of cost and benefit, it would cost them more than it benefits them. Hereafter, for now the US have resorted to fulfilling their sense of responsibility through their leadership in the global cyber governance. Compared to establishing cyberspace international legal framework, leadership is a potentially a more benefitting option as it could cater the US' interest better and freely.

This research has attempted to explore the correlation of cyber power and the establishment of cyberspace international legal framework through analyzing the US cyber governance, infrastructures, institutions, strategies, and leadership in the global cyber governance. The anomaly of one state having such a great power in a domain but yet not attempting to regulate it have been answered by a hypothesis from a theory that explains the dynamic of interpretation in legal discourse. Furthermore, it would be interesting to further figure out the bargaining power and aspects that might lead states into having an understanding of the importance of creating collectiveness in cybersecurity. This is due to the unique nature of cyberspace, borderless and integrated at all means, it’s impossible to guarantee any sense of security through technical or regulative means if collectiveness is not first established.

References

Books

Austin, Greg. "US Policy: From Cyber Incidents to National Emergencies." in *National Cyber Emergencies: The Return to Civil Defence,* edited by Greg Austin, 31-59, Abingdon: Routledge, 2020.

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

Creswell, John W. and J. David Creswell. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches 4th* Edition. Thousand Oaks, CA, US: SAGE Publications, Inc, 2014.

Fish, Stanley. *Is There a Text in This Class? The Authority of Interpretive Communities*. London: Harvard University Press, 1980.

Henkin, Louis. *How Nations Behave*. New York: Columbia University Press, 1979.

Johnstone, Ian. "The Power of Interpretive Communities." in *Power in Global Governance*, ed. Michael Barnett and Raymond Duvall, 185-204, Cambridge: Cambridge Studies in International Relations, 2004.

Keohane, Robert O. "International Relations and International Law: Two Optics," in *Power and Governance in a Partially Globalized World,* 487-502, New York: Routledge, 2002.

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

Meyer, Paul. "Norms of Responsible State Behaviour in Cyberspace." in *The International Library of Ethics, Law and Technology* Vol. 21, edited by Markus Christen, Bert Gordjin and Michele Loi, New York: Springer, 2020.

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

Schmidt, Andreas. “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, 181-202, Berlin: Springer-Verlag, 2014.

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

_________________. “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, 259-272, Oxford: Oxford University Press, 2018.

Journal

Austin, Greg and Pavel Sharikov. “Preemption Is Victory: Aggravated Nuclear Instability of the Information Age.” *Non-proliferation Review* 23, No, 5-6: 691-704.

Chayes, Abram and Antonia Handler Chayes. “On Compliance.” *International Organization* 47 (2): 118-119.

Hansen, Lene and Helen Nissenbaum. “Digital Disaster, Cybersecurity, and the Copenhagen School.” *International Studies Quarterly* 53, No. 4 (2009): 1155-1175.

Huang, Zhixiong 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.

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

Mačák, Kubo. “From Cyber Norms to Cyber Rules: Re-Engaging States as Law-Makers.” *Leiden Journal of International Law* 30 (2017): 887-916. https://ssrn.com/abstract=2961821.

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

Official Documents

Australian Strategic Policy Institute International Cyber Policy Centre. *The UN Norms of Responsible State Behavior in Cyberspace.* March, 2022. https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf

Clarke, Richard A. “Securing Cyberspace Through International Norms: Recommendations for Policymakers and the Private Sector.” Good Harbor Security Risk Management, LLC. (2013). https://carnegieendowment.org/files/Good-Harbor_Securing-Cyberspace-Through-International-Norms_2013.pdf.

Congressional Research Service. *Global Research and Development Expenditures: Fact Sheet.”* April 29, 2020. https://fas.org/sgp/crs/misc/R44283.pdf.

Cybersecurity and Infrastructure Security Agency. *Joint Cyber Defense Collaborative.* March, 2022. https://www.cisa.gov/sites/default/files/publications/JCDC_Fact_Sheet.pdf.

_________________. *Year in Review 2021.* Accessed on December 20, 2022. https://www.cisa.gov/sites/default/files/publications/21-0860_EOY_REPORT_508c.pdf.

Defense Information Systems Agency (DISA) and National Security Agency (NSA) Engineering Team. *Department of Defense (DoD) Zero Trust Reference Architecture Version 2.0.* July, 2022. https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf

Executive Office of the President Office of Management and Budget. *Memorandum for the Heads of Executive Departments and Agencies.* January 26, 2022. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

Government Publishing Office. *U.S. Government Publishing Office Budget Justification Fiscal Year 2022.* February 16, 2021. https://www.govinfo.gov/content/pkg/BUDGET-2022-PER/pdf/BUDGET-2022-PER-6-2.pdf.

Governments of the United States. *Joint Statement on Advancing Responsible State Behavior in Cyberspace.* September 23, 2019. https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/.

Governments of the United States and Mexico. *Joint Statement on U.S.-Mexico Working Group on Cyber Issues.* August 18, 2022. https://www.state.gov/joint-statement-on-u-s-mexico-working-group-on-cyber-issues/.

Highfill, Tina, and Christopher Surfield "New and Revised Statistics of the U.S. Digital Economy 2005-2021." U.S. Department of Commerce Bureau of Economic Analysis. *(*March 2019). https://www.bea.gov/system/files/2022-11/new-and-revised-statistics-of-the-us-digital-economy-2005-2021.pdf.

International Counter Ransomware Initiative (CRI). *International Counter Ransomware Initiative 2022 Joint Statement.* November 1, 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/international-counter-ransomware-initiative-2022-joint-statement/.

Moncada-Paterno-Castello, P. and N. Grassano. "The EU vs US coporate R&D intensity gap: Investigating key sectors and firms." European Comission. 2022. https://joint-research-centre.ec.europa.eu/system/files/2020-03/jrc120008.pdf.

Organization for Economic Co-Operation and Development. *Measuring the Digital Transformation: A Roadmap for the Future.* March 11, 2019. https://doi.org/10.1787/9789264311992-en.

Semiconductor Industry Association. *2020 – State of the U.S. Semiconductor Industry.* 2020. https://www.semiconductors.org/wp-content/uploads/2020/07/2020-SIA-State-of-the-Industry-Report-FINAL-1.pdf.

Smit, Sven, Magnus Tyreman, Jan Mischke, Philipp Ernst, Eric Hazan, Jurica Novak, Solveigh Hieronimus, and Guillaume Dagorret. *Securing Europe's* *competitiveness: Addressing its technology gap.* McKinsey Global Institute. (September, 2022). https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/securing-europes-competitiveness-addressing-its-technology-gap.

The International Insititute for Strategic Studies. *Cyber Capabilities and National Power: A Net Assessment.* June 28, 2021.

The White House. *National Security Strategy.* October 2022. https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

The White House Office of Management and Budget. *Budget of the U.S. Government Fiscal Year 2022.* December 2021. https://www.whitehouse.gov/wp-content/uploads/2021/05/budget_fy22.pdf.

United States of America Cyberspace Solarium Commission. *CSC Final Report.* March 2020. https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view.

World Economic Forum. *The Global Risk Report 2020 15th Edition.* December 2020. https://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

Legislations

United States of America. National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*. Washington D.C.: National Institute of Standards and Technology, 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

United States of America. US Library of Congress. *Cyber Diplomacy Act of 2021*. Washington D.C.: US Congress, 2021. https://www.congress.gov/bill/117th-congress/house-bill/1251.

_________________. US Library of Congress. *Cybersecurity Enhancement Act of 2014.* Washington D.C.: US Congress, 2014. https://www.congress.gov/bill/113th-congress/senate-bill/1353/text.

Websites

Bikhchandani, Raghav. “What is ‘Five Eyes’ the intelligence alliance US wants South Korea, India, Japan to be part of.” *The Print*. September 9, 2021. https://theprint.in/world/what-is-five-eyes-the-intelligence-alliance-us-wants-south-korea-india-japan-to-be-part-of/730475/.

Bureau of Cyberspace and Digital Policy. “Global Emerging Leaders in International Cyberspace Security (GEL-ICS) Fellowship.” *U.S. Department of State*. Accessed on December 20, 2022. https://www.state.gov/global-emerging-leaders-in-international-cyberspace-security-gel-ics-fellowship/.

Cybersecurity and Infrastructure Security Agency. “CISA Launches a Space Systems Critical Infrastructure Working Group.” May 13, 2021. https://www.cisa.gov/news/2021/05/13/cisa-launches-space-systems-critical-infrastructure-working-group.

________________. “CISA Strategic Plan 2023-2025.” Accessed on December 19, 2022. https://www.cisa.gov/strategy.

________________. “The President’s National Infrastructure Advisory Council.” Accessed on December 20, 2022. https://www.cisa.gov/niac.

________________. “Zero Trust Maturity Model.” Accessed on December 1, 2022. https://www.cisa.gov/zero-trust-maturity-model.

Federal Department of Foreign Affairs. “Eleven norms of responsible state behaviour in cyberspace.” Accessed on December 20, 2022. https://www.eda.admin.ch/eda/en/fdfa/fdfa/aktuell/newsuebersicht/2021/04/uno-cyber-normen.html.

International Cable Protection Committee. “Member List.” Accessed on December 20, 2022. https://www.iscpc.org/about-the-icpc/member-list/.

Lin, Herb. “President Biden’s Policy Changes for Offensive Cyber Operations.” *Lawfare*. May 17, 2022. https://www.lawfareblog.com/president-bidens-policy-changes-offensive-cyber-operations.

Lygass, Sean. "State Department launches cyberbureau amid concerns over Russia and China's authoritarianism." *CNN*. April 4, 2022. https://edition.cnn.com/2022/04/04/politics/state-department-cyber-bureau/index.html.

Komaitis, Konstantinos and Justin Sherman. "US and EU tech strategy aren't as aligned as you think." *Brookings*. May 11, 2021. https://www.brookings.edu/techstream/us-and-eu-tech-strategy-arent-as-aligned-as-you-think/.

Marks, Joseph. "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/.

National Institute of Standards and Technology. "Journey to 2.0." December 3, 2022. https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20.

Office of the Director of National Intelligence. "History." Accessed on December 20, 2022. https://www.dni.gov/index.php/who-we-are/history.

________________. "Mission, Vision & Values." Accessed on December 20, 2022. https://www.dni.gov/index.php/who-we-are/mission-vision.

Office of the Spokesperson. "Establishment of the Bureau of Cyberspace and Digital Policy." *U.S. Department of State*. April 4, 2022. https://www.state.gov/establishment-of-the-bureau-of-cyberspace-and-digital-policy/.

________________. "Ad Hoc Committee to Elaborate a UN Cybercrime Convention Third Negotiating Session at the United Nations in New York." *U.S. Department of State*. August 29, 2022. https://www.state.gov/ad-hoc-committee-to-elaborate-a-un-cybercrime-convention-third-negotiating-session-at-the-united-nations-in-new-york/.

________________. "The 6th U.S. – Republic of Korea Cyber Policy Consultations." *U.S. Department of State*. December 15, 2022. https://www.state.gov/the-6th-u-s-republic-of-korea-cyber-policy-consultations/.

________________. "Quad Foreign Minister's Statement on Ransomware." *U.S. Department of State.* September 23, 2022. https://www.state.gov/quad-foreign-ministers-statement-on-ransomware/.

Purplesec. "Recent Cybrattacks." Accessed on December 20, 2022. https://purplesec.us/resources/cyber-security-statistics/#Recent.

Sanger, David E. and William J. Broad. "Trump Inherits a Secret Cyberwar against North Korean Missiles." *New York Times*. March 4, 2017, https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html?action=click&module=RelatedCoverage&pgtype=Article&region=Footer.

Smalley, Suzan. "Biden set to approve expansive authorities for Pentagon to carry out cyber operations." *Cyberscoop*. November 17, 2022. https://www.cyberscoop.com/biden-nspm-13-pentagon-cyber-operations/.

The National Counterintelligence and Security Center. "Five Eyes Intelligence Oversight and Review Council (FIORC)." Accessed on December 20, 2022. https://www.dni.gov/index.php/ncsc-how-we-work/217-about/organization/icig-pages/2660-icig-fiorc.

The White House. "Computing Infrastructure for AI R&D." Accessed on December 20, 2022. https://trumpwhitehouse.archives.gov/ai/ai-american-innovation/.

________________. "Memorandum on Renewing the National Security Council System." February 4, 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/02/04/memorandum-renewing-the-national-security-council-system/.

________________. "Office of the National Cyber Director." Accessed on December 20, 2022. https://www.whitehouse.gov/oncd/.

U.S. Cyber Command. "Our History." Accessed on December 20, 2022. https://www.cybercom.mil/About/History/.

U.S. Department of Homeland Security. “Fiscal Year 2022 State and Local Cybersecurity Grant Program Fact Sheet.” September 16, 2022. https://www.fema.gov/fact-sheet/fiscal-year-2022-state-and-local-cybersecurity-grant-program-fact-sheet#:~:text=In%20fiscal%20year%20(FY)%202022,state%2C%20local%20and%20territorial%20governments.

U.S. Department of State. “Cyber Capacity Building.” November 27, 2022. https://www.state.gov/cyber-capacity-building/.

U.S. Department of the Treasury. “How much has the U.S. government spent this year?.” Accessed on December 1, 2022. https://fiscaldata.treasury.gov/americas-finance-guide/federal-spending/#:~:text=Spending%20Trends%20Over%20Time%20and,the%20United%20States%20that%20year.

Multimedia

Weitzner, Danny. “Defensive Cybersecurity Practices.” 2022. Massachusetts Institute of Technology Online Course on Cybersecurity for Critical Urban Infrastructure. 8:44. https://learning.edx.org/course/course-v1:MITx+11.S198x+3T2022/block-v1:MITx+11.S198x+3T2022+type@sequential+block@9aefcba2e61840a69ac2ac6f35b2e1f3/block-v1:MITx+11.S198x+3T2022+type@vertical+block@9728c3b760624fc8822e4785f29c5aac.