iCOBEST
International Conference on Business Economics, Social Sciences & Humanities

UNIKOM

THE SETTLEMENT OF COMPETITION BETWEEN THE UNITED STATES AND CHINA IN CYBERSPACE IN THE PERSPECTIVE OF LIBERALISM

Rachel Maria Naomi Kututung
Department of International Relations, Indonesian Computer University, Bandung, Indonesia

Dewi Triwahyuni
Department of International Relations, Indonesian Computer University, Bandung, Indonesia

ABSTRACT

This research analyzes liberalism's theoretical view of the US-China cyber conflict with a focus on international cooperation frameworks, cyber ethical norms, and diplomatic mechanisms. The method used is a literature study with a liberalism theory approach to cyberwar. The goal is to find a solution to the U.S.-China rivalry through sustained efforts, strong commitment, and global cooperation. By seeing cyberwar as a common challenge, liberalism theory is expected to build a safer, fairer, and more cooperative cyber order. Research also considers the role of international institutions, the private sector, and civil society in the context of global cybersecurity. The research impact of this study may provide a foundation for further discussion of how liberalism theory can be applied in the context of global cybersecurity. This could stimulate further research and in-depth policy discussion on how to build a safer, fairer, and more cooperative cyber order.

Keywords: Cyberwar, Diplomacy, Global Security, Liberalism Theory, Rivalry

INTRODUCTION

Cyber warfare has become one of the increasingly dominating areas in the global security landscape. With the advent of increasingly sophisticated digital technologies, cyber warfare has expanded from conflicts between countries to the arenas of businesses and individuals. This is no longer just a technical issue, but also a strategic concern for governments, companies, and society at large. At the core of cyber warfare are attacks on computer systems and networks, with the aim of stealing sensitive information, damaging infrastructure, or influencing public opinion. Such attacks can be carried out by states, organized groups, or even individuals who have sufficient technical expertise. In some cases, cyber warfare can have consequences as serious as conventional military conflicts, even without a single shot being fired. One solution to this case is to prioritize cooperation between China and the US as well as with other countries. In this study, researchers took some results from previous researchers regarding cyber warfare that occurred in China and the US.

An article written by James Perez-Moron (2021) for a journal discusses how, in a time of widespread cyberwarfare, cyberattacks on Chinese supply chains are becoming more frequent. Drawing attention to the complex relationship that exists between technology, national security plans, and the dynamics of international trade, Perez-Moron emphasizes the need for coordinated approaches to lessen the damaging effects that cyber threats have on economies and trade. The susceptibility of the Chinese government to cyberattacks forces a strategic reassessment and a determined attempt to put cybersecurity at the top of the priority list. In order to prevent cyberattacks on international supply chains, Perez-Moron proposes the establishment of frameworks for multilateral cooperation that are similar to China's partnerships with other countries.

Meanwhile, Katie Lightfoot's (2020) paper delves into the intricacies of Chinese cyber-attacks, elucidating their strategic intent to bolster economic advancements through nefarious means. By targeting intellectual property and sensitive data through espionage and data theft, China seeks to gain a competitive edge, posing significant challenges to international cybersecurity. Lightfoot underscores the urgency of robust mitigation efforts, emphasizing cyber awareness training and policy implementation as critical measures to shield American networks from these insidious threats. Moreover, she stresses the imperative of international vigilance, particularly in countering threats emanating from China, given the substantial financial and national security ramifications of intellectual property theft.

Josh Gold's (2020) provides insights into the concept of Cyber Collective Operations (OCC) and its implications for the Five Eyes countries and their allies. Advocating for OCC as a proactive mechanism to enforce cybersecurity norms, gold calls for enhanced transparency and understanding surrounding this collective approach. He posits that while OCC holds promise in bolstering cybersecurity, further research is warranted to unravel its complexities and address the inherent challenges in its global application.

Furthermore, Myriam Dunn Cavity and Andreas Wenger's (2019) paper expounds on the evolution of cybersecurity politics research, underscoring significant interdisciplinary advancements and their policy implications. Their analysis delineates the intricate interplay between technology, politics, and science, elucidating the multifaceted dimensions of cybersecurity as a political issue. As the trajectory of cybersecurity research continues to evolve, Cavity & Wenger identify key challenges and opportunities that will shape the future direction of this field, urging for sustained interdisciplinary collaboration to navigate these complexities effectively.

Lastly, Cheetal Rohith & Ranbir Singh Batth (2019) published a journal about delve into the ominous specter of cyber warfare, portraying a future fraught with uncertainties and formidable challenges. With cybersecurity threats transcending borders and permeating various sectors, Rohith & Batth advocate for concerted efforts to fortify defenses and adapt to emerging threats. Against the backdrop of the burgeoning technology trade war

between the U.S. and China, they emphasize the imperative of coordinated responses to counter cyberattacks and mitigate their repercussions effectively. The theoretical view of liberalism on the phenomenon of cyberwar between the United States (US) and China can be seen from the perspective of the involvement of countries in cyberspace. Liberalism emphasizes the importance of international cooperation, free trade, and diplomacy as means to prevent conflict. In the context of cyberwar, the liberalism approach can be interpreted as an attempt to establish international norms that govern the behavior of states in cyberspace. (Tampubolon, 2021)

Liberalism highlights the important role of international institutions such as the United Nations (UN) and other international organizations in dealing with conflicts. Within this framework, efforts to formulate international agreements related to cyber ethics, information security, and data protection are the main focus. Liberalism also encourages dialogue and diplomacy as a way to resolve tensions, in the hope that open talks can reduce mistrust between the U.S. and China in the cyber domain.

In addition, the theory of liberalism emphasizes the importance of the global economy and international trade. In the context of cyberwar, liberal countries tend to see economic cooperation as an incentive to keep the peace. The potential negative impact of cyber conflict on world economic stability is an impetus for building cooperation and security mechanisms in cyberspace. Liberalism's view of cyberwar is not always entirely optimistic. Some critics argue that there is power inequality in cyberspace, and countries with high-tech expertise can exploit it for geopolitical gain. Therefore, although liberalism promotes international cooperation, the real challenges in managing cyberwar between the US and China still involve the complexity of global security dynamics and uncertainty regarding the implementation of new norms in cyberspace.

However, in the face of the complexities of cyberwar between the US and China, the theory of liberalism is also confronted with the reality that some countries may not always adhere to the proposed international norms. Uncertainty regarding implementation and enforcement of the rules can complicate efforts to reach consensus at the global level. In addition, differences in views between liberal countries on individual rights and online privacy can be a serious obstacle. (Ramadan, 2019)

In an effort to address this challenge, proponents of liberalism may push for a more inclusive and effective international forum. These measures could include more intensive dialogue between the parties involved, strengthening the role of international organizations in monitoring and enforcing cyber norms, and increased cooperation in the field of cybersecurity.

Although the theory of liberalism offers a framework that promotes international cooperation, its implementation in the context of the cyberwar between the US and China is not simple. The complexity of geopolitical dynamics, differences in national interests, and technical challenges necessitate a holistic and sustainable approach to achieving peace and security in this increasingly connected cyberspace.

In the face of this challenge, the theory of liberalism also highlights the importance of trust building among countries involved in cyber conflicts. Transparency in cyber policy and information exchange on cyber threats is needed to reduce mistrust and increase mutual understanding. Liberalism encourages trust and security mechanisms in the context of cyberwar, such as joint inspections and exchanges of cyber experts, to build a strong foundation for cooperation. (Faida, 2019)

Proponents of liberalism theory might also emphasize the importance of the role of civil society, the private sector, and non-governmental institutions in shaping international cyber policies and norms. Active participation from different parties can help ensure that diverse perspectives are accommodated and the resulting policies better reflect shared interests. In developing solutions to address the cyberwar between the U.S. and China, liberalism emphasizes the need for an inclusive approach, respecting human rights, and promoting shared security. In the end, amid the complex dynamics of cyberspace, the application of the principles of liberalism can be a step towards joint efforts in maintaining peace and cybersecurity in this era of globalization.

The theory of liberalism, as one of the schools of thought in the science of international relations, emphasizes values such as freedom, human rights, and international cooperation. In general, liberalism believes that cooperation and interdependence between countries can reduce conflict and bring progress. In the context of international relations, this theory presupposes that states can cooperate through international institutions to achieve common goals.

Liberalism views the international world as an arena that can be governed by international norms and agreements. The existence of institutions such as the United Nations (UN) is seen as a means to facilitate dialogue and peaceful resolution of conflicts. Liberalism also emphasizes the importance of free trade as an instrument to promote peace, connect countries' economies, and create interdependence that can promote stability.

Liberalism offers the view that democracy and people's political participation can reduce the potential for conflict. Democratic countries are considered more likely to establish peace with fellow democratic countries. In addition, the theory advocates the protection of human rights as a central cornerstone in international relations. Although liberalism offers an optimistic view of the possibilities of cooperation and peace, criticisms of this theory arise mainly in the context of power inequality and not always consistent implementation of norms. Overall,

however, the theory of liberalism nevertheless provides a significant view in understanding the dynamics of modern international relations.

This research provides a better understanding of the dynamics of cyber conflict between the US and China from the perspective of liberalism. This can help policymakers and practitioners in the field of cybersecurity to develop more effective strategies in managing tensions in cyberspace. Second, the study's findings highlight the importance of international cooperation, both between countries and with international institutions, the private sector, and civil society. It emphasizes the need for a shared commitment to creating cyber ethical norms that can reduce conflict risk and improve cyber security. Third, the results of this study provide a foundation for further discussion of how the theory of liberalism can be applied in the context of global cybersecurity. This could stimulate further research and in-depth policy discussion on how to build a safer, fairer, and more cooperative cyber order

.LITERATURE REVIEW

Theory of Liberalism It also focuses on the concept of economic interdependence between countries. Economic liberalism encourages free trade and international investment as a means of creating a win-win situation, where economic growth and prosperity can be felt together. Economic interdependence is considered a potential barrier to armed conflict, as states have an incentive to maintain stability in order to protect their economic interests. (Saputra & Waluyo, 2015)

The theory of liberalism emphasizes the importance of global institutions in addressing common problems such as climate change, poverty, and regional conflicts. The existence of these institutions, according to the liberal view, can create a collaborative mechanism to find joint solutions that involve active participation from various parties. Liberalism offers an alternative to military solutions by promoting diplomacy, dialogue, and conflict resolution through negotiation. Proponents of this theory believe that democracy and liberal principles can ease tensions between countries, because of society democrats tend to prefer the peaceful path of resolving disputes.

The cyberwar between the United States (US) and China reflects the complexity and intensity of competition in the digital realm. Understanding cyberwar can be interpreted as a form of conflict or battle that occurs in cyberspace, where both countries use information and communication technology to achieve political, economic, or military goals. In the U.S.-China context, this rivalry involves a series of cyberattacks, espionage, and information manipulation attempts exchanged between the two sides. (Minchah, 2020)

The cyber battle between the U.S. and China often involves stealing classified data, especially over military and economic technology. Both countries are trying to secure each other's technological advantage, both in military and business contexts. Cyberattacks carried out by government-linked entities or hacking groups working on behalf of the state characterize this conflict.

In addition, the political dimension also plays a role in the cyberwar between the US and China. Cyberattacks can be directed to influence public opinion, derail democratic processes, or damage a country's image. The manipulation of information through social media and cyberattacks on critical infrastructure are part of the strategies used to achieve each country's political goals.

In addressing the complexities of the cyberwar between the U.S. and China, it is important to understand that this conflict is not only limited to the technical realm, but also includes political, economic, and national security aspects. The two countries have conflicting strategic interests, and this dynamic of competition can create serious challenges to global stability.

Diplomacy and dialogue efforts are key in dealing with tensions in cyberspace. The establishment of internationally acceptable norms of behavior, especially related to cyber ethics and information security, is an important step to prevent the escalation of conflicts. International forums, such as the G20 Meeting or other initiatives, can be a platform to discuss these issues collaboratively.

In addition, increasing cyber defense capacity is a must for both countries. Investment in cybersecurity technologies, training of cyber experts, and cooperation between the public and private sectors are crucial elements in protecting critical infrastructure and sensitive data. to create a transparency mechanism that allows the exchange of information between the U.S. and China to prevent misunderstandings and build trust. In the face of these complex challenges, international collaboration and shared understanding will be key to achieving stability and security in an ever-evolving cyberspace.

METHODOLOGY

The literature study research method is used to deepen the understanding of a topic by detailing the views and arguments expressed in relevant literature. In exploring liberalism's theoretical views on cyberwar between the United States (US) and the People's Republic of China (PRC), the first step is to conduct a literature review of works that discuss the theory of liberalism in the context of international relations and cyberwar.

The theoretical approach of liberalism to cyberwar can be identified through theoretical works that discuss liberal frameworks in international security. Analysis of the literature can involve an understanding of the concepts of international cooperation, free trade, the role of international institutions, and ethical norms in the context of cyberwar. The classical works of liberal thinkers such as Immanuel Kant or contemporary international relations theorists who developed liberal views can be the basis for identifying liberal views on cyber conflict.

A liberalist view of the U.S.-China cyberwar, literature study research may include analysis of empirical research, policy reports, and cybersecurity analyses that provide insight into the practices of liberal countries, especially the U.S., in responding to and addressing cyber challenges from countries, including China.

The purpose of this study is to analyze the conflict in cyber space between the United States and China from the perspective of liberalism theory which can then produce solutions by establishing and promoting international cooperation. This research provides a better understanding of the dynamics of cyber conflict between the US and China from the perspective of liberalism. This can help policymakers and practitioners in the field of cybersecurity to develop more effective strategies in managing tensions in cyberspace. The study's findings highlight the importance of international cooperation, both between countries and with international institutions, the private sector, and civil society. It emphasizes the need for a shared commitment to creating cyber ethical norms that can reduce conflict risk and improve cyber security. The results of this study provide a foundation for further discussion of how the theory of liberalism can be applied in the context of global cybersecurity. This could stimulate further research and in-depth policy discussion on how to build a safer, fairer, and more cooperative cyber order

RESULT AND DISCUSSION

Liberalism's theoretical view of cyberwar between the United States (US) and the People's Republic of China (PRC) tends to emphasize diplomatic solutions and international cooperation as a way to address tensions in cyberspace. Within the theoretical framework of liberalism, efforts to shape international norms governing the behavior of states in cyberspace are the main focus. This theory believes that international institutions, such as the United Nations (UN), can be a platform to facilitate dialogue, negotiate, and reach consensus to reduce conflict. (Marsiti & Ritonga, 2018)

Liberalism also highlights the role of free trade as a driver of international stability. In the context of cyberwar, this theory can emphasize the importance of economic cooperation as an incentive to maintain peace. This cooperation is expected to create interdependence that provides incentives to countries, including the US and China, to avoid cyber conflicts that can harm mutually beneficial economic exchanges.

In addition, the theory of liberalism underscores the need to uphold human rights and individual freedoms, even in the cyber domain. This view may reflect a drive to avoid cyberwar practices that could involve violations of privacy and human rights. In essence, liberalism theory supports a values-based approach and ethical norms in dealing with cyber conflicts, in the hope of forming a more stable and civilized cyber order.

The theory of liberalism also highlights the importance of transparency and mutual understanding between the two sides. Mechanisms of diplomacy and active dialogue are considered more effective avenues to manage tensions than relying on aggressive actions or the spread of conflict. Liberal thinking considers that the establishment of norms of behavior in cyberspace, such as prohibitions against cyberattacks on critical infrastructure or theft of confidential data, can create a more solid basis for preventing conflict escalation. (Febrianti, Hara &; Sunarko, 2022)

In addition, liberalism emphasizes the role of civil society, non-governmental organizations, and the private sector in shaping policy and raising awareness of cybersecurity risks. The active involvement of these parties is expected to provide a broader and inclusive perspective in designing solutions to cyber conflicts.

The theoretical view of liberalism towards the U.S.-China cyberwar opens the door to a more cooperative and multilateral approach. Although challenges and differences of interest remain, the theory offers a more optimistic view of the possibilities of cooperation and conflict resolution in cyberspace, which in turn can form a more stable and secure basis in relations between states.

The theory of liberalism towards the US-China cyberwar, the economic aspect is also the focus of attention. Liberalism emphasizes that economic interdependence between the U.S. and China can be a motivating factor for maintaining stability and avoiding cyber conflicts that harm both sides. Cooperation in technological innovation, trade in digital products, and cross-border investment in the technology sector are key elements in building the foundations of interdependence that can promote peace. (Angrand, 2021)

Liberalism's view of cyber conflict also highlights the need to promote cyber defense capacity building and information security together. Within this framework, the theory encourages collaboration between agencies, both national and international levels, to develop effective policies to protect critical infrastructure and sensitive data.

In an effort to address tensions and potential cyber conflicts between the US and China, the theory of liberalism also highlights the importance of establishing effective and transparent dispute resolution mechanisms at the international level. The development of legal instruments and norms governing cyber actions can be a significant step in steering countries' behavior towards more responsible and globally acceptable practices.

In addition, the theory of liberalism encourages active participation from civil society, cybersecurity experts, and technology industry players in the policy-formulation process. By involving various parties, it is hoped that a more holistic approach can be produced and reflect common interests in maintaining global cybersecurity.

Implementing a liberalistic approach to the U.S.-China cyberwar, strengthening international institutions such as the United Nations (UN) could be key. Liberalism encourages more use of international forums as a forum for dialogue and cooperation, whether in the context of developing cyber ethical norms, exchanging information, or resolving conflicts. Through global collaboration, it is hoped that a more robust framework can be produced to manage tensions in cyberspace and reduce the potential for escalation of cyber conflicts. (Faulks &; Mahadi, 2021)

The implementation of liberalism, the promotion of cyber literacy and awareness of cybersecurity risks are also crucial aspects. Better education and understanding of technology and cybersecurity issues can help shape the attitudes of civil society, industry players, and other stakeholders toward cyberwar practices. This, in turn, can support the establishment of an atmosphere more conducive to collaboration and prevention of cyber conflict.

Although the theory of liberalism provides an optimistic view of the solution of cyberconflict, the challenges of its implementation remain complex. Countries tend to protect their national interests, and ideological differences and interpretations of proposed norms can complicate the diplomatic process. In the face of evolving dynamics in cyberspace, the liberalism approach still relies on a shared commitment to create a safer, fairer, and more cooperative cyber order.

The theory of liberalism also creates the stage for preemptive diplomacy and risk mitigation. Parties involved need to commit to preventing conflict escalation and responding to cyber threats in a constructive manner. Proactive cyber diplomacy, ongoing dialogue, and information exchange mechanisms can help avoid conflict escalation and ease tensions. (Hashemi, 2021)

Ultimately, implementing liberalism's view of the U.S.-China cyberwar requires sustained efforts, strong commitment, and global cooperation. By viewing cyberwar as a shared challenge that requires a common solution, liberalism theory can provide a foundation for building a safer, fairer, and more cooperative cyber order.

CONCLUSION AND RECOMMENDATION

The theoretical view of liberalism on cyberwar between the United States (US) and the People's Republic of China (PRC) reflects optimism about the potential for international cooperation and conflict resolution in cyberspace. This theory emphasizes the importance of normative frameworks that govern the behavior of states in the cyber domain, through dialogue, diplomacy, and the establishment of international agreements. Liberalism also highlights the role of international institutions, the private sector, and civil society in shaping policy and raising awareness of cybersecurity risks. The theory of liberalism is faced with a number of complex challenges, including different interpretations of international norms, uncertainty regarding the compliance of states, and the rapid pace of technological development.

REFERENCES

Fukuyama, F. (2022). Liberalism And Its Discontents. Great Britain: Profile Book.

Gold, J. (2020). The Five Eyes and Offensive Cyber Capabilities: Building a 'Cyber Deterrence Initiative'. 4-30.

Jennifer L. Bayuk, J. H. (2012). Cyber Security Policy. Canada: John Wiley & Sons, Inc.,

Lightfoot, K. (2020). Examining Chinese cyber-attacks: Targets and threat mitigation. 1-9.

Perez-Moron, J. (2021). Eleven years of cyberattacks on Chinese supply chains in an era of cyber warfare, a review and future research agenda. 2-26.

STEPHEN MCGLINCHEY, R. W. (2017). International Relations Theory. Bristol: Creative Commons CC BY-NC 4.0 license.

Wenger, M. D. (2019). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. 2-29.

Angrand, G. N. (2021). PEMILIHAN STRATEGI GEOPOLITIK DAN GEOEKONOMI INDONESIA, CHINA DAN AMERIKA SERIKAT DI KAWASAN LAUT CHINA SELATAN. Ekonomi Perthane, 7(1), 1-25.

Faida, R. E. (2019). Sensor Internet dan Securitization di Era Cyberwarfare: Studi Kasus Tiong Kok. Journal Houngan International, 1, 31-46.

Faulks, K., & Mahadi, H. (2021). Sociology Politik: Teori-Teori Kontemporer Tentang Negara dan Masyarakat Sipil. Nusamedia.

Febrianti, R., Hara, A. E., & Sunarko, B. S. (2022). Persaingan Kekuasaan Antara India dan Cina: Dari Kekuasaan Militer Sampai Dengan Konflik Siber. Intermestic: Journal of International Studies, 6(2), 292-314.

Hashemi, N. (2021). Islam, Sekularisme dan Demokrasi Liberal. Islamic Renaissance Front.

Marsetio, M., & Ritonga, R. (2018). Representasi Kapal Selam Indonesia dalam Perspektif Pertahanan Regional. Jurnal Kajian Stratejik Ketahanan Nasional, 1(2), 87-94.

Minchah, N. (2020). Perkembangan Teknologi Artificial Intelligence Cina: Ancaman dan Implikasinya terhadap Keamanan Nasional Amerika Serikat. Jurnal Studi Diplomasi Dan Keamanan, 12(2).

Ramadhan, I. (2019). Strategi Keamanan Cyber Security di Kawasan Asia Tenggara. Jurnal Asia Pacific Studies, 3(2), 181-192.

Saputera, M. Y., & Waluyo, T. J. (2015). Pengaruh Cyber Security Strategy Amerika Serikat Menghadapi Ancaman Cyber Warfare (Doctoral dissertation, Riau University).

Tampubolon, S. (2021). Analisis Politik Keamanan Nasional dalam Isu Larangan Aplikasi Tiktok Milik China Oleh Pemerintahan Amerika Serikat (Doctoral dissertation, Universitas Sumatera Utara).

Batth, C. R. (2019). Cyber Warfare: Nations Cyber Conflicts, Cyber Cold War Between Nations and its Repercussion. 1-6.

ABOUT THE AUTHORS

Rachel Kututung, email: rachelmariakututung@icloud.com

Rachel Kututung is a student in the Department of international relations, Faculty of social and political sciences, Universitas Komputer Indonesia, Indonesia.

Dr. Dewi Triwahyuni, MSi, S.IP is is head of Department of International Relations at the Indonesian Computer University since 2018. Started her career as a lecturer since 2005. She obtained his Bachelor's, Master's and Doctoral degrees in the same field of International Relations. As a professional lecturer and has a Certified International Qualitative Researcher (CIQaR), Dr. Dewi Triwahyuni actively conducts research and writes scientific papers with a focus on International Relations, U.S. Foreign Policy and Cybersecurity