ISSN 2961-7758

Cyberwarfare: A Constructivist Analysis Towards the United States-China Cyberwar

Jalaluddin Rizqi Mulia[1]
[1]Department of International Relations, Faculty of Psychology and Socio-cultural Sciences, Universitas Islam Indonesia, Yogyakarta, Indonesia, 55584
Email: jalaluddin.rizqi@students.uii.ac.id[1]

ABSTRACT
Cyberspace is a discussion not merely related to technological advancements, but also penetrates into the socio-political realm. Cyber issues are now starting to overwhelm security issues with the spread of cyberattacks. Although only happening in cyberspace, the impact resulting from the action can be fatal for major infrastructures in the real world, including data management, public private information, and the state security system. This is what happened between the United States (US) and China. Beforehand, the US and China had an agreement in cyberspace issues to develop international norms. Nonetheless, this step was not significant given the reluctance of both parties to implement the points of agreement as they were not in line with the national interests. In addition, the two countries often accuse each other of cyberattacks occurring in their respective territories. As the world's two strong cyberpowers, the process of cyberwar becomes urgent to be analyzed through the constructivism concept, as it takes identity understanding into account. By utilizing descriptive qualitative approach through literature study, this research aims to understand the cyberspace situation between the US and China and to analyze the ongoing process of the US-China cyberwar from a constructivism perspective. Social construction plays an important role as it shapes perceptions of other actors. With China, it is difficult for the US to form sustainable cooperation given the fluctuating dynamics of the relationship between the two. Until the end, it is currently difficult to find similarities that would reduce the tension of political conflict.

Keywords: cyberwarfare, United States of America (USA), China, constructivism, national interest

INTRODUCTION

Cyberspace is an issue that was initially considered insignificant in international relations. As part of technological developments, especially the interconnected network (Internet), the cyber world is accepted as a realm that is solely for discussion of technology (private or business realm). However, it did not take long for this view to transform, adapting with the current situation: the cyber world is not only correlated to technological improvements, but also penetrates the socio-political realm (public sphere). In a scholarly discussion of international relations, for instance, this was argued by Abbasi (2021) that cyber issues have penetrated into issues of national security whose developments seem to lead to conflict or even hostility.

Until now, cyber world issues have begun to penetrate into the real world, especially in the security realm. This is related to the potential implications resulting from events in the cyber world for the real world (Ramadan, 2021). One apparently is the spread of cyber-attacks. In this case, the cyber-attacks themselves reflect how countries – in the real world, compete and fight for influence. Geopolitically, in contrast to the real world which presents the phenomenon of a limited state territory, the cyber world allows an increasingly unlimited realm.

Although happening in cyberspace, the impact resulting from this action can be fatal for important infrastructure in the real world, such as data management, public private information, and the state security system. This possibility then made many countries develop their cyber power which, if estimated, could be comparable to the development of military capabilities.

Constructivism is one of the popular theories in the study of international relations. Unlike the other concepts, its uniqueness lies in the focus on discussing the realm of ideas or ideas that play an important role in the formation of interaction norms, which were originally also produced from the interaction process itself. However, unlike a number of other theories, constructivism is rarely discussed, especially when looking at security issues such as cyberspace. Analysis through a constructivism perspective is expected to contribute to answering questions regarding the cyber conflict between the United States (US) and China because it involves the important role of identity. In regard to the background case, this study aims to analyze the understanding of the cyberspace situation between the US

ISSN 2961-7758

and China as well as analyze the ongoing process of the US-China cyberwar from a constructivism perspective.

LITERATURE REVIEW

Cyberspace and Cybersecurity

At the beginning, the cyber world (cyberspace) was an information-filled environment consisting of digitized data that was created, stored, and disseminated and was originally a realm for communication and buying and selling. But now, it has turned into a part of the important infrastructure that is often associated with the Internet. In contrast to boundaries in the real world with clear geographical boundaries, divisions in cyberspace tend to be imaginary (Singer and Friedman, 14-16). This concept is closely related to the process of globalization which is often called unlimited space and time. Cyberspace obscures many concepts in international relations, such as borderless sovereignty. Both the cyber world, the Internet, and globalization are terms that intersect with each other.

Regarding the Internet, this technology was originally a tool for sharing information and, in its development, became a medium that developed by itself. Various information disseminated online is strongly influenced by the identity and culture of its users. Its connection with high-level affairs, such as government, requires state and other actors to adapt to the development of the Internet (Petallides, 2012).

Broadly speaking, cybersecurity can be categorized as a nontraditional security issue (Perwita and Yani, 128). Nonetheless, several points in cyberspace issues are closely related to traditional security issues, such as state security and military capabilities. According to Pinterpolitik (2021), considering the rapid growth of cyberspace, the term cyber warfare has emerged as a response to the development of new battlefields as a result of increasing state power in cyberspace. The new zone has the characteristics of unlimited "cyber army" possibilities, ease of access (which is increasing and depends on technological superiority), to anonymity (Pinterpolitik, 2021).

In the beginning, the issue of security in international relations only revolved around discussing physical spaces, including land, sea, and air. However, this focus is slowly fading with the presence of cyberspace which has the potential to damage the state in the physical space. Along with the development of the times, the cyber world has become a new arena that is very influential so that it must be regulated by state authorities.

Social construction itself has a role in shaping fear of the possibility of destructive cyber space (Isnarti, 2016). These include destroying intellectual property, undermining the credibility of the state security system, reducing trust in online transactions, and such.

Constructivism Theory in International Relations

Constructivism broadly talks about ideas and concepts. The social construction that belongs to everyone creates knowledge that is shared. The core of constructivism itself is identity. Identity points include discussing how actors see themselves and determining interest preferences. In addition, constructivism views culture as having an important role, because it contains a set of practices that give meaning to shared experiences. Given its significance, tradition does contain values up to the rules that shape identity.

The identity process is formed gradually and not suddenly (taken for granted). The results of this process can be in the form of attitudes when interacting with other actors. As for one form of medium used for interaction is communication – an effort to understand and recognize other actors which, in the end, determines friendship or hostility.

In the context of international relations, the international system is formed based on ideas, not material power (Jackson & Sorensen, 400). In the process, interaction between countries is a factor causing the presence of various identities and interests which are then defined by attitude norms. Moreover, the state's internal conditions can influence its international attitude (Jackson and Sorensen, 401). Regarding this matter, this includes certain parties that are in power as the executive or the legislature.

Constructivism is quite closely related to the formation of identity and norms. The identity itself is formed from the international and domestic environment. What's more, culture, norms, and identity are said to be included in the context of discussing the core of national security (Jackson and Sorensen, 390). In fact, the identity identification process is considered as an effort to understand the desired definition of national security and the formulation of foreign policy to be aimed at (Jackson and Sorensen, 391).

As for other things, such as communication, built through international norms that were previously constructed by actors with strong ideas. These norms then become standards and guidelines. Therefore, there is a close correlation between identities, interests, and interactions between various identities, and included in this context are state elites. The notion of constructivism can be summarized as the result of actor interactions with other actors. In the context of statehood, various ideas and discourses form this shared identity. This important point distinguishes constructivist

ISSN 2961-7758

ideas from other international relations theories, that the socio-political realm is composed of shared beliefs rather than physical entities (Jackson and Sorensen, 392).

In responding to the anarchist nature of the cyber world, in several respects, constructivism tends to be in line with the institutionalist neoliberal notion that cooperation between parties at the international level is necessary to uphold international practices that conform to norms. The norm itself is the result of the actor's interaction with various other actors. This set of norms then regulates the balance of the global world (Thomas, 2017).

METHODOLOGY

This study is using a qualitative approach. The analysis method used in this research is descriptive with literature study–obtaining information by tracing the existing literature, analyzing it, and surveying the available data (Nazir, 1988). The data for the writing collected in the form of literature data is derived from books, academic papers, news from mass media, and various other sources which are in line with the theme of this paper. The peak activity of this technique is the analysis, interpretation, and the presentation of findings.

Data analysis was carried out through several stages, namely collecting a number of data related to the research object from various literature and documents, sorting data relevant to the topic and problem formulation in this study, interpreting the data that has been collected relating to the research object, and drawing a connecting line from the results of data interpretation into a conclusion as an answer to the problem statements of this paper.

RESULT AND DISCUSSION

- **Phenomenon of US-China Relations in Cyberspace**

As the two dominant powers in a multipolar world structure, both the US and China actually had an agreement in cyberspace called the Cybersecurity Agreement in 2015. Several matters were agreed on at the occasion, such as efforts to reduce espionage in the economic sphere, increase communication and cooperation between the two countries, preventing cybercrime from both sides, and the two countries' governments are not allowed to support cyber theft of intellectual property. More than that, both the US and China also agreed to develop new state norms in the cyber world for the international community and establish a high-level dialogue mechanism to fight cybercrime (Brown and Yung, 2017). Although this step shows progress towards reducing the conflict, of course many points have not been realized due to various obstacles that have occurred. The most important of them: reluctance to make points of agreement because they are not in line with national interests.

In a report released by Microsoft, China is listed as the country of origin of hackers with 8 percent of the number of cyber-attacks that occur. Even though it is small compared to Russia which reaches 58 percent or North Korea with 23 percent, the probability of success from hacking from China is said to be the highest, namely at 44 percent (Pinter Politik, 2021). This data indicates the rise of China's cyber power along with the rise of the country's position in the global arena.

This can be traced back to President Xi Jinping's statement that he wants China to immediately become a cyber power (Austin, 2015). China has its own characteristics regarding the development of the Internet because it is adapted to combine the basic principles of Marxism and the local development of the Internet in China (Kania et. al., 2017). This is what makes the characteristics of cybersecurity in China focused on national security.

Until now, China is claimed to have supported a number of hackers who took action against a number of agencies in the US. The Bamboo Curtain country has been proven to have carried out various offensive cyber operations, including online spying, stealing intellectual property, to disinformation campaigns against the US and its allies (Warrell, 2021). China's capabilities cannot be underestimated since a series of cyber-attack cases against numerous countries, even though in fact many of the hackers are not directly supported by the communist government.

Despite this, there are still those who doubt the rise of China's cyber power, considering that the focus of China's strength is on domestic cyber security to suppress information that is harmful to the communist government. In addition, compared to the Five Eyes alliance (including the US, UK, Canada, Australia, to New Zealand), US cyber intelligence tends to be driven by the ideological drives and political ambitions of the leaders of the Chinese Communist Party (Warrell, 2021).

Various efforts have been made to strengthen China's cyber power. Philosophically, the Four Pillars and Five Propositions are concepts presented by Xi Jinping to support this effort. The Four Pillars themselves are aimed at promoting changes in the global Internet management system, namely (1) respect for cyber sovereignty; (2) maintaining peace and security; (3) stimulate the opening of cooperation; and (4) establish the right order.

ISSN 2961-7758

In addition, the Five Propositions are intended to form a common community in cyberspace to promote the development of the global Internet which includes: (1) accelerating the development of global network infrastructure and stimulating interconnection and interactivity; (2) building a common platform for online cultural interaction, and stimulating efforts to exchange knowledge; (3) promoting the innovation and development of the digital economy, and stimulating its development process in general; (4) ensure cyber security and promote orderly development; and (5) building an Internet management system and promoting justice efforts (Kania et. al., 2017).

Apart from these basic reasons, China has poured out quite a lot of effort to adapt to the development of potential war on a new front. The People's Liberation Army Strategic Support Force (PLASSF), for example, is part of the Chinese national army directed at "information warfare" (Pinterpolitik, 2021). What's more, China's military units are among those supported by large disbursement of funds, namely USD 168.2 billion. This position places China right below the US for the highest military budget in the world (Michael, 2019).

These strengthening efforts are considered by the US as a threat. As a power that still dominates the world order, the US does not want any power to compete with its capabilities. Apart from simply being a matter of developing opponents, cyberattacks that frequently occur are also the reason why the US responds by strengthening the country's cyber security structure.

For instance, the development of China's cyber power is marked by cyber espionage in the form of hacking classified information, namely various military projects, including aircraft, combat vehicle designs, to missile systems (Iman and Azzqy, 49). In just 5 years, namely 2013 to 2017, the total losses resulting from cyberattacks in the US amounted to USD 5.52 billion (Nugroho and Windiani, 2018). On the other hand, China also accused the US of hacking that occurred in Chinese universities (Kurnia, 2022).

The form of response to the issue is quite diverse. For the US, the main form is to tighten cybersecurity as stipulated in formal policies, such as the Cyberspace Policy Review to the International Cyberspace Policy Strategy (Nugroho and Windiani, 2018). This task is not only delegated to the government, but is also open to private, local actors, and to individuals in the network to help protect the digital environment.

The cyber arms race between the US and China is inevitable. The competition is heavily influenced by international agreements between the two countries which then affect the growth of the technology industry and ultimately impact the stability of international cybersecurity (Setiawan et. al., 154). Even though the US and China had originally communicated intensely at certain times to stop competition, the result was insignificant due to each party focusing on pursuing their own national interests.

- **The Process of US-China Cyberwar from Constructivism Perspective**

According to constructivism theory, where social construction is formed as shared knowledge in an international arena, the stronger a state is, the greater its role in shaping collective identity that apply in the interaction process which eventually become part of the international norm. Therefore, the dominant country will shape the way it views itself, other countries, and how other countries should view their country.

The main essence of the constructivist framework of thinking lies in how countries process the ideal identity they want internationally. Social construction plays an important role because it shapes perceptions of other actors. The state forms a strong conception of their rights and roles independently (Jamison, 2021). If there is a discrepancy between a country's perception of itself and other countries' perceptions of that country, especially if the international community rejects the identity of the country concerned as a whole, then such differences can escalate into tensions that lead to conflict.

The attitudes of the US and China towards each other in cyberspace are highly correlated with actions in the real world. Isnarti (2016) conveys his views on the important role of construction in collective identity formation, both friend and foe. For example, if China – from the military or civilian side, is claimed to have hacked US cyber systems, then this action will be considered as a cyber-attack that undermines national security. As for other scenarios, for example teenagers from Australia hack actors from the US, then this attitude will only be responded to as an act of espionage, not until it becomes a frightening attack (Isnarti, 2016). This happened considering that Australia is a US ally, while China is perceived as an enemy.

A set of cybersecurity policies in the US is the result of the interaction of actors with their environment along with the participation of the international community's anarchist political culture (Nugroho and Windiani, 2018). The issue of national security, for example, is something that is decided based on a compromise between the various actors involved.

ISSN 2961-7758

In this case, including the government and society in the cyber world (cyberspace). Here, social construction becomes an important player because it shapes the perception of other actors. For example, with China, it is difficult for the US to form sustainable cooperation given the fluctuating dynamics of the relationship between the two. It's different when the US cooperates with its traditional allies, such as Australia and Britain. Until the end, it is difficult to find similarities that would reduce the political tension of both parties.

Additionally, this assumption is also based on the stigmatization of the state. In essence, China is an authoritarian communist country by government. Various issues reflect this, such as the existence of a social credit system (Kyle, 2021) to re-education camps in Xinjiang (Wong and Buckley, 2021), all of which are considered undemocratic in the US. The difference in government culture also occurs in the cyber world, where China's cyberspace is adapted to the goals of national interests. For example, the great firewall program, which requires sites and applications to suit political interests (Economy, 2018). This is also indicated by the existence of acts of mutual attack in the cyberspace of the two countries, such as Google applications being forced by censorship rules in China and the threat of blocking TikTok in the US (Xiao, 2021; Morrison, 2023).

On the other hand, China also considers the US to play too dominant a role in the international cyber world. The implicit aim of China's rise is in reducing the dependence of many countries on US-based technology and, at the same time, influencing global internet usage activities (Martin-Shields, 2021). Martin-Shields (2021) also highlights a number of advantages of China's presence in cyber-related markets, such as marketplaces (Alibaba), internet conglomerates (Tencent), digital infrastructure and device manufacturers (Huawei), to global satellite systems (BeiDou).

According to Triwahyuni and Yani (2018), the US and China have the same perspective regarding the military, economy, and politics in the cyber world. However, there are differences that give uniqueness to each point of view. For example, as a country that promotes liberal democracy in various parts of the world, the characteristics of the cyber world in the US perspective are full of views of freedom of expression. Meanwhile for China, the cyber world is not just a matter of control, regulation of information, or network assets, but also a matter of interests. The benefits gained from strengthening power in cyberspace are really used to pursue the goals of national interests.

Meanwhile, other differences also exist in the perception of one another. Regarding this, Brown and Yung (2017) write that, on the one hand, Washington considers Beijing to interfere too much in their business interests. Meanwhile, on the other hand, China views the US as being too hypocritical with its domination in managing (governing) the Internet and taking advantage of its position which "leads" cyber space to obtain information that is in line with their intelligence interests. This difference in perceptions results in a lack of common ground between the two parties which will only reduce the potential for conflict resolution dialogue.

From a constructivism perspective, the US attitude to strengthen national security in the context of cyberspace is the fruit of its intense interaction with China. So far, relations with China have tended to be hostile, although in some respects they still experience cooperation, such as clinical technology collaboration and environmental achievements (Flannery, 2022). Even so, this effort still requires the authority of the government's attitude to reduce ego–manage perceptions of other actors. In this case, the US should be able to reduce the intensity of its conflict by opening opportunities for cooperation in areas that do not directly intersect with high-level interests, such as national security.

In the context of security, constructivism views that security is the result of social construction, considering that security is a consideration for various actors in responding to potential threats to the state (Nugroho and Windiani, 398). China's capability to carry out espionage, for example, is a concern for the US' ability to protect national sovereignty and the security of its citizens. In addition, the news reported by the media also influences public opinion towards China, so that it can have an impact on collaboration in other fields.

For the US, the threat of war in the cyber world is as dangerous as the threat of physical war, considering the fatal consequences that can occur in the event of a cyber-attack, such as paralyzing important infrastructure, state information systems, and damaging the government's credibility (Saputera, 12).

Relationships are increasingly tenuous due to not finding a common attitude. In addition, there have been no attempts at follow-up dialogue, even though it had previously been carried out since 2015. For example, Gady (2016) wrote how US-China relations had dialogue but had not produced significant progress. Dialogue itself is important in order to find commonalities that hopefully can together form the latest international norms.

ISSN 2961-7758

Furthermore, social construction is not permanent, but can be reconstructed by adjusting the ongoing dynamics. In this context, the US and China can reconstruct their perceptions of each other, so that if an agreement is reached, conflicts and differences of opinion can be minimized. Meanwhile, identity still plays an important role in formulating the construction of the interests to be achieved (Jackson and Sorensen, 392).

Promoting dialogue between people has the potential to equalize the perception of the interests of each country. However, this hope will certainly be difficult to achieve because both parties are trying to spread their influence in line with their respective national interests. This action can be predicted based on the identity held by each actor in the arena of international interaction.

CONCLUSION

The US and China had an agreement in cyberspace to develop international norms. Nonetheless, this step was not significant given the reluctance of both parties to implement the points of agreement because they were not in line with national interests. China's cyber power is among those experiencing a renaissance.

The development of China's internet itself has a characteristic, namely its adjustment to the basic principles of Marxism. The capabilities of the Bamboo Curtain country cannot be underestimated since the series of cyber-attack cases against a number of countries, including hacking attempts. China itself has poured a lot of effort into developing military capabilities in the cyber world as a new battlefield. These efforts are considered by the US, the dominant force in cyberspace, as a threat. Apart from the question of the progress of the opponent, cyberattacks that often occur are also a reason.

The development of China's cyber power is marked by cyber espionage in the form of hacking classified information, such as various military projects. Therefore, a cyber arms race is inevitable. Intense communication that was supposed to be carried out by both parties became insignificant due to each party focusing on pursuing the goals of their own national interests.

Regarding constructivism theory, the dominant state will shape the way it views itself, other countries, and how other countries should view their country. With China, it is difficult for the US to form sustainable cooperation given the fluctuating dynamics of the relationship between the two. Until in the end, it is difficult to find similarities that would reduce the tension of political conflict.

China's cyberspace itself is adjusted to the goals of national interests, such as the great firewall program. The implicit aim of China's rise is in reducing countries' dependence on US-centric technologies and, at the same time, influencing global internet usage activities. In addition, the use of constructivism can also highlight differences in the cyber world of the two countries. The characteristics of the cyber world in the US perspective are full of views on freedom of expression. Washington considers Beijing to be too meddling in their business interests. Meanwhile in China, the cyber world is not only a matter of control, regulation of information and network assets, but also a matter of interests. China also thinks that the US is too dominating in managing the internet, and even tends to abuse its power for intelligence purposes.

The US attitude to strengthen national security in the context of cyberspace is the result of its intense interaction with China. So far, relations with China have tended to be hostile. China's capability to carry out espionage is a concern for the US ability to protect the sovereignty of the country and its citizens. Even so, social construction is not permanent and can be reconstructed by adjusting the ongoing dynamics.

REFERENCES

Abbasi, M. (2021, Mei 1). Security in Cyberspace in the Field of International Relations. *Journal of Archives in Military Medicine*, 8(4), 1-9. https://doi.org/10.5812/jamm.114485

Austin, G. (2015, Juli 31). *2015 is the year of Chinese cyber power*. East Asia Forum. Retrieved Februari 11, 2023, from https://www.eastasiaforum.org/2015/07/31/2015-is-the-year-of-chinese-cyber-power/

Brown, G., & Yung, C. D. (2017, Januari 19). Evaluating the US-China Cybersecurity Agreement, Part 1: The US Approach to Cyberspace. *The Diplomat*. https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/

Economy, E. C. (2018, Juni 29). The great firewall of China: Xi Jinping's internet shutdown. *The Guardian*. https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown

Flannery, R. (2022, Januari 17). Two Areas Where The U.S. And China Can Still Work Together. *Forbes*. https://www.forbes.com/sites/russellflannery/2022/10/08/two-areas-where-the-us-and-china-can-still-work-together/?sh=5a00ebf26783

ISSN 2961-7758

Gady, F.-S. (2016, Juni 16). China-US Relations in Cyberspace: A Half-Year Assessment. *The Diplomat*. https://thediplomat.com/2016/06/china-us-relations-in-cyberspace-a-half-year-assessment/

Imam, M., & Azzqy, A. (2018). Aktivitas Spionasi Republik Rakyat Tiongkok ke Amerika Serikat Terkait Proyek Militer Pesawat F-35 Joint Strike Fighter Pada Tahun 2014-2017. *Balcony*, *2*(1), 43-54. https://jom.fisip.budiluhur.ac.id/index.php/balcony/article/view/51

Isnarti, R. (2016, November). A Comparison of Neorealism, Liberalism, and Constructivism in Analysing Cyber War. *Andalas Journal of International Studies*, *5*(2), 151-165. https://doi.org/10.25077/ajis.5.2.151-165.2016

Jackson, R., & Sorensen, G. (2013). *Pengantar Studi Hubungan Internasional*. Pustaka Pelajar.

Jamison, B. C. (2021, Mei). A Constructivist Approach to a Rising China. *Journal of Indo-Pacific Affairs*. https://www.airuniversity.af.edu/JIPA/Display/Article/2624409/a-constructivist-approach-to-a-rising-china/

Kania, E., Sacks, S., Triolo, P., & Webster, G. (2017, September 25). *China's Strategic Thinking on Building Power in Cyberspace*. New America. Retrieved Februari 11, 2023, from https://www.newamerica.org/cybersecurity-initiative/blog/chinas-strategic-thinking-building-power-cyberspace/

Kurnia, T. (2022, September 29). China Berang Akibat Serangan Siber AS ke Universitas Politeknik. *Liputan6.com*. https://www.liputan6.com/global/read/5083723/china-berang-akibat-serangan-siber-as-ke-universitas-politeknik

Martin-Shields, C. (2021, Agustus 24). Defining the new digital world order. *D+C - Development + Cooperation*. https://www.dandc.eu/en/article/us-and-china-are-locked-battle-dominance-cyberspace

McSorley, K. (2021). *Exploring and Analyzing American Perspectives of the Chinese Social Credit System* [Master's thesis, University of Tampa]. The University of Tampa Institutional Repository. http://hdl.handle.net/20.500.11868/2768

Michael, J. (2019, September 12). Melihat Kekuatan Pasukan Siber China. *Merdeka.com*. https://www.merdeka.com/teknologi/melihat-kekuatan-pasukan-siber-china.html

Morrison, S. (2023, Februari 2). The US government's TikTok bans, explained. *Vox*. https://www.vox.com/recode/2023/1/17/23552716/tiktok-ban-cfius-bytedance

Nazir, M. (1988). *Metode Penelitian*. Ghalia Indonesia.

Nugroho, K. A., & Windiani, R. (2018, Agustus). Pengaruh Cyber Attack terhadap Kebijakan Cyber Security Amerika Serikat. *Journal of International Relations*, *4*(3), 393-401. https://doi.org/10.14710/jirud.v4i3.21048

Perwita, A. A. B., & Yani, Y. M. (2020). *Pengantar Ilmu Hubungan Internasional*. PT Remaja Rosdakarya.

Petallides, C. J. (2012). Cyber Terrorism and IR Theory: Realism, Liberalism, and Constructivism in the New Security Threat. *Inquiries Journal/Student Pulse*, *4*(03). http://www.inquiriesjournal.com/a?id=627

PinterPolitik. (2021, Oktober 13). *Rusia-Tiongkok Pemantik Perang Siber?* PinterPolitik.com. Retrieved Februari 11, 2023, from https://www.pinterpolitik.com/in-depth/rusia-tiongkok-pemantik-perang-siber/

Ramadhan, I. (2021). The Implication of Cyberspace Towards State Geopolitics. *POLITICON: Jurnal Ilmu Politik*, 3(2), 161-184. https://doi.org/10.15575/politicon.v3i2.12660

Saputera, M. Y., & Waluyo, T. J. (2015, Oktober). Pengaruh Cyber Security Strategy Amerika Serikat Menghadapi Ancaman Cyber Warfare. *Jurnal Online Mahasiswa Fakultas Ilmu Sosial dan Ilmu Politik Universitas Riau*, *2*(2), 1-14. https://jom.unri.ac.id/index.php/JOMFSIP/article/view/7446

Setiawan, R., Reksoprodjo, A. H.S., & Suhirwan. (2020). Analisa Perlombaan Senjata Siber Antara Amerika dan China 2014-2018 Menggunakan Richardson Model of Arms Race. *Jurnal Peperangan Asimetris*, *6*(2), 136-156. https://jurnalprodi.idu.ac.id/index.php/PA/article/view/909

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.

Thomas, E. (2017, November 13). *Taming the 'Wild West': The Role of International Norms in Cyberspace*. E-International Relations. Retrieved Februari 11, 2023, from https://www.e-ir.info/2017/11/13/taming-the-wild-west-the-role-of-international-norms-in-cyberspace/

Triwahyuni, D., & Yani, Y. M. (2018, Juni). Dampak Pembangunan Cyberpower Tiongkok Terhadap Kepentingan Amerika Serikat. *Jurnal Ilmu Politik dan Komunikasi*, *8*(1), 1-14. https://ojs.unikom.ac.id/index.php/jipsi/article/view/883

Warrell, H. (2021, Juni 27). China's cyber power at least a decade behind the US, new study finds. *Financial*

ISSN 2961-7758

Times. https://www.ft.com/content/3350bce7-7f19-4a45-a749-79aa9b3b265e

Wong, E., & Buckley, C. (2021, Juli 27). U.S. Says China's Repression of Uighurs Is 'Genocide'. *The New York Times*. https://www.nytimes.com/2021/01/19/us/politics/trump-china-xinjiang.html

Xiao, B. (2021, Januari 29). Google pulled its service from China more than a decade ago — can Australia learn from that? *ABC*. https://www.abc.net.au/news/2021-01-30/google-leave-australia-what-to-learn-from-china-legislation-law/13102112