CYBER RIVALITY BETWEEN CHINA AND UNITED STATES IN 2016-2020

Hendra Maujana Saragih**,** Fitri Nurani Solichan, James Baron Universitas Nasional
hendramaujanasaragih@civitas.unas.ac.id (Corresponding Author), fitriansolichah@gmail.com,
Jamesbaron66@gmail.com *(Submission 1)*

Abstract

The development of China's Cyber Power has become a threat to the position of the United States. Almost every aspect of life has been connected with technology, and every country makes every effort to maintain or achieve their respective national goals. Cyber rivalry both show the conditions of competition to become cyber hegemony. This study will analyze the cyber rivalry between China and the United States in 2016-2020 through various sectors of life that can be a threat and an advantage for each. Therefore, the author provides the formulation of the problem, namely How is cyber power competition between China and the United States?. This study aims to be able to understand and also to determine the power of cyber power, especially China related to its rivalry with the United States. In this study the author uses the concept of Cyber Power and Competitive Advantage Theory. To support the results of a more comprehensive research the author uses a qualitative approach research method. The results of this study explain that cyber power competition between China and the United States is increasing, but the United States is superior to China because the United States has previously had global power dominance compared to China. Although China in recent times has experienced rapid cyber development, especially in the field of technology. However, the influence of the United States in the global order is irreplaceable and China still needs time to gain global recognition to replace the United States.

Keywords*:* Technology; Cyber Power; Cyber Rivality; Cyber Hegemony.

Abstrak

Perkembangan Cyber Power China telah menjadi ancaman bagi posisi Amerika Serikat. Hampir setiap aspek kehidupan telah terhubung dengan teknologi, dan setiap negara melakukan segala upaya untuk mempertahankan atau mencapai tujuan nasionalnya masing- masing. Persaingan dunia maya sama-sama menunjukkan kondisi persaingan untuk menjadi hegemoni dalam dunia maya. Kajian ini akan menganalisis persaingan dunia maya antara China dan Amerika Serikat pada tahun 2016-2020 melalui berbagai sektor kehidupan yang dapat menjadi ancaman dan keuntungan bagi masing-masing. Oleh karena itu, penulis memberikan rumusan masalah yaitu Bagaimana persaingan cyber power antara China dan Amerika Serikat terjadi?. Penelitian ini bertujuan untuk dapat memahami dan juga untuk mengetahui kekuatan cyber power khususnya China terkait persaingannya dengan Amerika Serikat. Dalam penelitian ini penulis menggunakan konsep Cyber Power dan Competitive

Advantage Theory. Untuk mendukung hasil penelitian yang lebih komprehensif penulis menggunakan metode penelitian pendekatan kualitatif. Hasil penelitian ini menjelaskan bahwa persaingan cyber power antara China dan Amerika Serikat semakin meningkat, namun Amerika Serikat lebih unggul dari China karena Amerika Serikat sebelumnya memiliki dominasi kekuatan global dibandingkan dengan China. Padahal China belakangan ini mengalami perkembangan siber yang pesat, terutama di bidang teknologi. Namun, pengaruh Amerika Serikat dalam tatanan global tidak tergantikan dan China masih membutuhkan waktu untuk memperoleh pengakuan global guna menggantikan Amerika Serikat.

Kata Kunci: Teknologi; Kekuatan Cyber; Rivalitas Cyber; Hegemoni Cyber.

PENDAHULUAN

World Wide Web atau lebih dikenal dengan WWB ibarat sebuah kunci yang memutar berbagai aspek kehidupan masyarakat global, misalnya dalam bidang ekonomi dimana pelayanan dan transaksi menjadi lebih efektif dan efisien seperti e- banking dan transfer lintas batas negara. Internet telah berhasil mendorong perkembangan komunikasi yang semakin inovatif dan produktif, termasuk komunikasi lintas batas negara. Perkembangan ini tentunya melibatkan masyarakat dan aktor global sebagai salah satu aktor yang terlibat dalam interaksi dunia maya ini. Google dan Weibo adalah dua contoh berbagai produk yang dikembangkan di industri perangkat lunak. Perkembangan yang terjadi tidak hanya positif tetapi juga negatif, antara lain serangan siber, spionase siber, dan perang siber. Dunia maya atau ruang siber adalah wilayah abu-abu, tempat setiap aktor bisa bermain. Kondisi tersebut pada akhirnya memaksa negara harus berkontribusi dan mengambil sikap atas ancaman keamanan yang mungkin terjadi. Perkembangan dunia maya mendorong negara- negara untuk membuat kebijakan dengan kepedulian terhadap permasalahan di dunia maya. Kondisi ini memaksa negara untuk memiliki kesadaran dalam mencegah serangan siber dari pihak luar dan meningkatkan kekuatan sibernya.

Dalam kondisi keamanan kontemporer, dunia cyber akan sangat bergantung pada internet, dan internet tidak akan pernah lepas dari sejarah perkembangan teknologi di dunia dan terus berkembang baik dari segi perangkat keras, perangkat lunak, maupun dari segi jumlah. pengguna hingga saat ini. Hampir setiap aspek kehidupan di Amerika Serikat terkomputerisasi dan terhubung ke internet. Kemajuan teknologi sudah dirasakan oleh orang Amerika sejak lama. Berdasarkan data Biro Sensus Amerika Serikat, pada tahun 2016 pengguna internet di Amerika Serikat mencapai 81% dan angka tersebut meningkat pada tahun 2018 menjadi 85%.

Pada awalnya, pertumbuhan teknologi China bisa dikatakan lebih lambat dari Amerika Serikat. Namun sejak pemerintahan Deng Xiaoping yang mengeluarkan kebijakan “Reformasi dan Pembukaan” pada tahun 1978 dengan mencanangkan 4 agenda perubahan atau yang disebut dengan “*four modernizations*” (four key modernization) telah berhasil mendorong perkembangan pertumbuhan China. Kepemimpinannya menjadi awal pertumbuhan teknologi di China dengan modernisasi bidang ilmu pengetahuan dan teknologi, salah satunya dengan mengembangkan teknologi informasi (TI) dan internet. Hal inilah yang kemudian

dikembangkan oleh pemerintahan Xi Jinping untuk menjadikan China sebagai negara dengan kemampuan siber yang cukup diperhatikan. Huawei adalah contoh perusahaan teknologi China yang terkenal di dunia, terutama ketika perusahaan tersebut mulai mengembangkan teknologi 5G pada tahun 2009 dan menarik perhatian Amerika Serikat. Berdasarkan data CNNIC atau *China Internet Network Information Center*, total pengguna internet di China pada Juni 2020 meningkat 67% dibandingkan tahun 2017 dengan total pengguna internet mencapai 939,84 miliar orang. Meski pertumbuhan China lebih lambat, namun belakangan ini pertumbuhan kekuatan siber China menunjukkan perubahan yang cukup dicermati oleh Amerika Serikat karena dianggap mampu mengganggu posisinya sebagai pemegang hegemoni dunia.

Amerika Serikat pada akhirnya melakukan proteksionisme terhadap perusahaan teknologi China, misalnya dengan memasukkan Huawei ke dalam daftar hitam pasar Amerika Serikat dengan tuduhan spionase dunia maya, terutama setelah berkembangnya Artificial Intelligence (AI). Kemudian China menanggapinya dengan mencabut lisensi OS Android (google) di platform Huawei. Sikap saling serang dan proteksionisme antara Amerika Serikat dan China menunjukkan rivalitas kedua negara ini dalam menjadi hegemon dunia maya. Berdasarkan pemaparan diatas, penelitian ini bertujuan untuk mengetahui kekuatan siber yang digunakan China dalam kaitannya dengan rivalitasnya dengan Amerika Serikat dan juga untuk memperdalam informasi yang berkembang di dunia internasional khususnya terkait isu-isu seperti kekuatan siber. Yang mana dalam menganalisis pembahasan ini, penulis juga menggunakan teori sebagai landasan dalam memperkuat argumentasi dan memperkuat data yang penulis miliki.

1.1 Literature Review

Based on previous research that I found to strengthen the data in this paper, here I use 3 previous studies: The first research is a journal entitled “The Impact of China’s Cyber power Development on the Interests of the United States” written by Dewi Triwahyuni from the Indonesian Computer University in Bandung and Yayan Mochamad Yani from Padjadjaran University in Bandung. The researcher discusses how China’s cyber power development goals are and how this has an impact on the interests of the United States. President Xi Jinping’s firm statement that China must become a cyber power country is the focus of researchers in

seeing China's cyber power development goals. Researchers also found that in the records of the United States, China was the country that most frequently carried out cyber-attacks on the United States. Therefore, the rapid rise of China's cyber power is seen as a threat to the security of the United States.

The second research is a study entitled "China's Motivation to Master Cyber Technology" written by Nadya Vira Meisitha, Agung Purwanto, and Linda Dwi Eriyanti. This study discusses China's motivation in mastering Cyber Technology. Researchers show that China and the United States have the potential for war in the China Sea, especially over the issue of Taiwan, the Korean Peninsula, and the Diaoyu Islands as the trigger. So that China must master cyber technology on each of its war equipment to deal with these threats because the United States also uses cyber technology bases on its war equipment.

The third research is entitled "The Strategic Support Force and the Future of Chinese Information Operations" written by Elsa B. Kania and John K. Costello. This study examines the reform of the formation of the SSF reflecting the efforts of the Chinese PLA to solve the previous problems and, build the country's military cyber power to ensure their combat capability. SSF is considered to be increasing the PLA's ability to fight and win information wars in the future. The focus of this research includes China's military modernization, information warfare, and defense science and technology.

1.2 Method

In writing this research, the approach used is a qualitative approach, namely the scientific method that is often used by a researcher in conducting research in the social and humanities fields. According to Bogdan and Taylor, a qualitative research methodology is a research procedure that results in a descriptive data set out in written words from what is observed. Through a qualitative approach, the findings and data collected will be combined. The data collection carried out in this study was not intended to test hypotheses, but to describe the data found in accordance with the focus of the research studied. Research on the cyber rivalry of China and the United States in 2016-2020 according to the author is relevant by using qualitative research methods because it fulfills the characteristics of qualitative research, namely revealing more in-depth data through empirical data. This research uses library research as a data collection technique. With this library study technique data collection is done through sources that are usually stored in

libraries such as books, journals, relevant news, documents, scientific magazines, dissertations, and theses. Library research technique can also be interpreted as a data collection technique by conducting a study of the data sources being studied related to the focus of the problem being studied.

RESULT AND DISCUSSION

2.1 China Cyber Power

Since 1991, China has been seeking increased funding and development of cyber technologies. Development is carried out in various sectors, including the government, military, and civilian sectors. This development is China's holistic effort to build its political and economic power. The development and improvement of cyber technology is deliberately sought to increase cyber capabilities as an asymmetrical means in fighting the hegemony of the United States. This is inseparable from China's awareness that cyberspace can become a war domain. In addition, in the context of military power, cyber power is considered at the level of land, sea and air power, which can lead a country to victory or defeat.

Slowly but surely, China has developed into one of the world's leading cyber powers and continues to expand its capacity. China also made acquisitions of foreign technology, especially in the industrial growth sector, and this helped China to leapfrog development. The transfer of foreign technology allows China to skip years of expensive research and development by focusing on the advantages that foreign companies and militaries have.

One form of technology transfer efforts carried out by China is through joint ventures, which are routinely emphasized by China for foreign entry into its market. An example of a joint venture carried out by China is in the A320 aircraft project by Airbus. These joint ventures were successful in providing China with insights into advanced aeronautics.

Cyber power for China is not only a place for connectedness but also a force that must be controlled and developed. As it is known that cyber space is an open area, comprehensive control and involvement of many parties is needed to ensure that cyber development in state activities has a positive value. In this case, China is very aware that the development and control of cyber power are two things that cannot be separated. The development of cyber power in various sectors,

especially the economy, will further encourage the improvement of China's business climate in the global context. Meanwhile, control over cyber power will maintain the stability of China's territory and politics from various threats that may arise from inside or outside.

Overall, China's strategy in increasing its cyber power capabilities goes through several layers. China realizes that in order to create a strong cyber power, there must be integration at every level. This integration is due to the existence of an attachment to every activity carried out by citizens, both state and non-state with technological developments. Each activity has its own information flow and network. So, it is important for China to ensure that technological developments can continue but the defense of the flow of information in it must also be maintained. Referring to the availability of information in cyber space, it is only natural that China should develop its cyber power to maintain the flow of information it has.

2.2 United States Cyber Power

As it is known that the United States has been the holder of world hegemony since the end of the Cold War. Since 1957, when Russia launched a satellite called SPUTNIK, it has succeeded in triggering the United States to compete in the space technology race with Russia. The success of the United States by launching its first satellite named TELSTAR on June 10, 1962 and followed by the ERLY BIRD satellite in 1965 shows the ability of the United States' technological rivalry. The potential of satellites that can receive and transmit broadcast signals to a wider area has made satellite technology widely used even today.

The United States' victory in the Cold war made the United States' technological development superior to other countries. The United States has already succeeded in establishing its technological advantage. Today the United States military relies heavily on cyberspace, relying on a global network of 15,000 local area networks and 7 million computers linked by more than 100,000 telecommunications circuits, spread across bases around the world. Meanwhile, network developments that occurred in the United States have also become the main network of the global civil Internet. Many privately owned telecommunications companies are Internet service providers, and many operate infrastructure via cyberspace.

The United States' global network stores and transmits unclassified information, whether public or confidential. The widespread use of technology and computer networks has made the United States a strategic center of gravity. However, conditions allow adversaries to gain knowledge of information in the possession of the United States, thereby allowing others to disrupt civil and economic infrastructure. Once again, the state's cyber power capability on the one hand can be a positive value, but on the other hand it is always overshadowed by the possibility of data leakage.

The easier the information is accessed, the more vulnerable the level of defense of the information is. The US military is known to rely heavily on satellites for many critical functions such as land, air, and sea navigation, surveillance, and reconnaissance, targeting of precision strike weapons, early warning, and communications. The network of networks formed even becomes a vast general- purpose platform on which financial markets, business, and trade, as well as diplomacy, spying, national security, and war depend. Historical records show that technological advances will bring great influence in the economic, political, and military fields. But on the other hand, it can become an atomic bomb if the state is not able to maintain the defense of the information network in it. Especially for the United States information network, which has long been the center of the world's information resources.

As the use of cyberspace increases, the abuse of cyberspace also increases. The incidence of cyberattacks around the world is increasing, both in the public and private sectors. Some attacks also cause financial losses. These cyber-attacks can significantly affect various important sectors, especially the economy and civil infrastructure. Some attacks may be purely by private groups but there is an increasing trend towards the use of cyber-attacks in state conflicts. The cyber power competition between the United States and China is inseparable from the United States' suspicion that China has repeatedly targeted the United States.

According to Mandant Report, a private technology company in the United States, reported that one of the Chinese People's Liberation Army (PLA) cyber espionage units hacked New York Times computer systems during 2012 and 2013. The climax was when the issue of cyber-attacks was raised in the first conversation between President Obama and China's new President Xi Jinping. This means that cyber problems have changed from low level technical problems to strategically important issues.

General James Cartwright, former Commander of the United States Strategic Command later stated that, China has carried out a kind of reconnaissance and mapping of government and private computer networks in the United States. China also allegedly possesses the necessary networks to carry out such attacks and has the capability to cripple critical infrastructure and military command and control. In addition, China's efforts to develop cyber power are for the survival of the regime, national sovereignty, and territorial integrity, and become a competitor to the hegemony of the United States. China is considered to be trying hard to hinder the involvement of the United States in China's vital interests by showing that the country has offensive capabilities under the internal control of the government.

The United States government's awareness that their overall information network is vulnerable to Chinese cyber exploitation and attacks has forced them to take a stand and develop to compete with China's cyber power competition. The United States views that the PLA or the Chinese Liberation Army is preparing for cyber warfare. The PLA is conducting reconnaissance in Cyberspace, seeking to create capabilities to harm the economy and damage critical infrastructure, prepare to disrupt the communications and information systems needed to support conventional arms conflicts, and prepare to conduct psychological operations to influence the American stand.

The conditions created in the end forced the United States to change its national security structure to cope with the development of China's cyber power in cyberspace. Studies by the United States government and think tanks show that China has three main national security goals, namely, First, to maintain the survival of the regime (the rule of the Chinese Communist Party (CCP), Second, to maintain national sovereignty and territorial integrity, and Third, to establish China as a regional and world power. The other main thing is that China is maintaining stable economic and social development, military modernization, and preventing Taiwan independence.

The increase in malicious cyber activity in the United States is visibly targeting large numbers of people, undermining national security, and affecting nearly every sector of its economy. Opponents take advantage of cybercrime tools and employ cybercriminals to steal United States national security secrets and intellectual property. According to a White House Economic Advisory Council assessment in the 2018 Executive Office of The President of the United States (EOP) report, malicious cyber activity cost the United States economy

an estimated $57 billion to $109 billion in 2016.93 In addition, the increase in malicious cyber activity has contributed to increase global impact.

2.3 The Readiness of China and United States in Cyber Competition

Cyber power competition that occurs between China and the United States shows the existence of a new form of competition that is not conventional in nature. Cyber power competition shows a new war limitation, a new mode, but with a larger scope covering land, sea, air, and space. The battlefield in this new type of war has also become much more difficult than in conventional conflicts. This is because it is difficult to determine the identity of the belligerent party clearly. Without this clear identification, the government cannot develop strategies to respond appropriately to opponents. The biggest difficulty in dealing with this competition lies in the responsibility of the state to prevent its territory from being used through cyber- attacks by entities that are not affiliated with the government because of the many actors involved.

As a hegemonic country, the United States which has long had a strong enough influence in the international arena certainly does not want to lose in this competition. The increase in cyber activity by the opposing party has forced the United States to use its influence, including in the economic sector. The globalization of market economies and the desire to create new tools to combat threats to security have contributed to the creation of substantial innovations in the use of coercive economic measures such as sanctions. Sanction programs continue to grow in size and scope. They can be comprehensive (i.e., restrictions on trade and commercial activity with entire countries) or targeted (i.e., restrictions on the activities of specific individuals and/or entities).

In carrying out its strategy, the United States attaches importance to several basic principles of their strategy. First, cyber security activities are a national effort. Second, the principle of protecting privacy and civil liberties. The United States government considers that the abuse of cyberspace is a violation of the privacy and freedom of citizens. This has in fact become a contradictory norm in the view of the Chinese government. The Chinese government tends to use the internet as a propaganda tool by exercising strong control so that its citizens do not have full rights to cyber freedom. Third, the principle of regulatory and market power. Government regulations will not be the main system in cyber security. Broader regulations should be put in place to enable companies to regulate information systems so that this does not create a failed cybersecurity approach.

Meanwhile, regarding cyber power competition with China, the United States uses economic influence to thwart the development of China's cyber power. One of them is the limitation of Huawei products in the United States market. The United States National Cyber Strategy more or less states that economic sanctions are included in the United States government's strategy in dealing with malicious cyber actors. The United States government advocates with other countries to establish cyber sanctions regimes and coordinates multilaterally to impose sanctions. This effort by the United States is important to contain cyber conflicts because it can create unexpected consequences for attacks. In addition, the United States has seriously issued a number of foreign policy formulations related to cyberspace or cyberspace following a number of Chinese behaviors in cyberspace that affect the national interests of the United States.

The United States military sector refers to the application of cyber power as Computer Network Operations (CNO) and divides it into three categories: Computer Network Defense (CND), Computer Network Attacks (CNA), and Computer Network Exploitation (CNE). The categories are analogous to the thinking in the Chinese People's Liberation Army. The offensive capabilities of the United States cyber power are CNA and CNE. In addition, to secure the position of the United States in the East Asia region, the United States is also building a power alliance, especially with Japan and South Korea. The United States has made the US Cyber Command a weapon of war in cyberspace.

The Cyber Command includes six elemental operational level bases, namely the Army Cyber Command, Fleet Cyber Command, Air Force Cyber, Air Marine Corps Forces Cyberspace Command., Joint Forces Headquarters – Department of Defense Information Network Command, and the Cyber National Mission Force.

In addition, the United States and Japan also agreed on several bilateral agreements to maintain their existence in the East Asia region, one of which was the establishment of the San Francisco Treaty and the Japan-US Security Treaty. Both agreements contain Japan's obligation to be able to return the occupied territories and the authority of the United States. This makes the United States has a military base there. This agreement itself was established in order to maintain regional and global security stability. The United States has the right to maintain its land, sea, and air power in Japan. This power can be used: (1) to maintain peace and security in the region without waiting for prior consultations; (2) but if

consultation is necessary, the United States may take action to defend Japan from outside attacks.

The agreement also stipulates that if there are operations carried out using Japanese bases by other parties, they must first consult with the Japanese government. In addition, the United States formed cooperation with Korea by agreeing to the Mutual Defense Treaty which contains an agreement to maintain international peace, the obligation to discuss taking action against threats when one or both feel threatened, and the permission of the United States military forces (land, sea, or air) to operate within the South Korean administration.

2.4 The Cyber Power Advantage of China and United States

As a country with a long heritage of experience, the United States independently has more sophisticated network management, in line with global practice even though the United States has heterogeneous hardware and software. The experience of maintaining a data center that is well instrumented and can reach and run-in various conditions is an advantage for the cyber power of the United States. This condition is certainly different from China, which is late in securing its network position in the global arena. The shadow of the dominance of the United States network will continue to approach and limit the scope of China's reach.

However, compared to the United States, China has in recent times been working more focused on creating an integrated, coordinated national cyber strategy through government, military, industrial, and educational actions, and infrastructure. China has even established the PLA's centralized Information Security Base, and is purported to play a cyber-defense role, within the General Staff Headquarters. This division is even close to state decision makers China's national network and very similar to the national intranet which then subdivides the network for government, commercial/private, and academic use. China owns the physical infrastructure, either directly or in partnership with private companies, and controls the national gateway to the global Internet. China also has a well-developed content filtering system called the 'Great Cyber Wall' or the "Great Wall of China". In simple terms, China has the ability to monitor and control information entering and leaving its country and even shutting down the flow of data that is considered a threat.

China's ability to monitor and control the country's information network is certainly an added value for China compared to the United States. On closer inspection, today the ownership and control of many core elements of global internet infrastructure, for example, fiber-optic submarine cables, content delivery networks (CDNs), autonomous system numbers (ASNs), and internet exchange points (IXPs), are highly dispersed throughout the world. world, especially Europe and the BRICS (i.e., Brazil, Russia, India, China, and South Africa). This reflects the fact that in fact more and more multipolar relations have emerged in international connections and indirectly shows that the position of the United States is experiencing a temporary decline. This condition is an opportunity for China in cyber competition with the United States. How and whether China is able to improve its capabilities can lead the country to a higher state.

2.5 China and United States Cyber Power Competition

In historical records, the rivalry between China and the United States is a remnant of Cold War hostilities. China's self-perception is heavily influenced by its ancient history and civilization, predating the United States by thousands of years. As the world's oldest nation-state, they are very sensitive to outside criticism or interference. While the position of the United States as the sole winner in the Cold War and making the country have a strong hegemony for years made China feel insecure about its position. The existence of competition for identity and recognition of state status makes the competition between the two increasingly increasing and continuing. In line with the development of the era of hostility between the United States and China in cyberspace, it has become a prominent issue in the bilateral relations between the two countries.

For China, the main priority in its cyber strategy is the importance of realizing social stability and national security. These two things are the two main points of China's interest related to the policies it carries out. At the same time, China is trying to control access to its information network. This is part of a process that has been carried out by China for a long time since the country was founded. Therefore, China needs an international environment that can provide an information network for their cyber development. China finally took steps related to international strategy by including cyber development in the economic sector. China is trying to get an advantage from the economic side compared to

the military side. This is because the military strategy will have the potential to make other countries alert and feel threatened. Meanwhile, the economy can slowly support China's growth and development in other sectors because it does not cover the fact that to carry out military modernization it must be supported by strong funding.

Meanwhile for the United States, cyberspace or cyberspace is a very important world in all sectors of American society. In government, commerce, academia, and the private sector of life, cyberspace in the United States has supported hundreds of trillions of transactions. Electric grid services, water systems, health services, law enforcement, and emergency calls are just some of the important role's cyberspace has for citizens. Meanwhile, communications, research and development, collaboration between educational institutions and the private sector, military command and control, intelligence work, and government administrative work are important roles of cyberspace for the United States government. Just like China, cyberspace is very important in the United Military's global network of countries, from everyday conversations to military operations issues.

In the end, the different interpretations and interests of each country make cyber power competition inevitable. China's growing and aggressive cyber power is seriously worrying the United States. Meanwhile, the dominance of cyber and technology in the United States indirectly creates concern for China. The dynamics of cyber competition have become ups and downs. But one thing is clear that when a country tries to learn the capabilities of other countries in cyber war, that country must also consider how the country's cyber power is.

Cyber power competition that occurs is a reality that cannot be ignored in the dynamics of international relations. Referring to the theory of competitive advantage, the competition between the two occurs because the two countries are in the same competence at the same level. Where both the United States and China are trying to outperform their competitors to achieve higher victories. Therefore, it is necessary to understand and develop carefully and thoroughly in all sectors of life so that one of these countries can survive and emerge as a winner of competence.

The Chinese government recognizes that heavy industry and low-end manufacturing cannot create the engines of sustainable growth or jobs that match China's increasingly educated and skilled workforce. Therefore, in affirmation

of The 13th Five-Year Plan, the Chinese government reaffirms its support for the Made in China 2025.

(中国制造 2025 or zhongguo zhizao) and "Internet Plus" (互联网+; hulianwang) initiatives. The initiative seeks to accelerate China's transition to higher value-added intelligent manufacturing by focusing on innovation and leveraging emerging industries, such as high-end appliances, integrated circuits, biomedicine, cloud computing, mobile Internet and e-commerce.

To support these sectors, the Chinese government has enough local and national champions, negotiate technology transfer as market access prices, regulate foreign investment and technology imports through the government catalog, promote Chinese technology standards domestically and internationally, and support more Chinese exports. through the "Going Out Strategy". In the Made in China 2025 policy, the Chinese government focuses on 12 main targets with the 2020 and 2025 deadlines focused on increasing China's innovation, productivity, quality, digitalization, and efficiency.

Table 1.1: Made in China 2025 (2020 and 2025 Target)

Target	2015 (Actual)	2020	2025
R&D spending as a share of operating revenue	0.95%	1.26%	1.68%
Number of patents per 100 million RMB of total revenue	0.44	0.7	1.1
Quality competitiveness index*	83.5	84.5	85.5
Growth of industrial value-added	5.9%	7.9%	9.9%
Average annual productivity growth	6.6%	7.5%	6.5%
Penetration of broadband internet	50%	70%	82%
Use of digital design tools in R&D	58	72	84
Use of numerical control machines in key production processes	33	50	64
Change in industrial energy intensity from 2015 levels	-	-18%	-34%
Change in carbon dioxide emission intensity from 2015 levels	-	-22%	-40%
Change in water usage intensity from 2015 levels	-	-23%	-41%
Reuse of solid industrial waste as a share of total waste	65%	73%	79%

Based on 2015 data, it appears how the Chinese government is trying to set its targets for China's progress in 2020 and 2025. China itself is known to always conduct reviews and analyzes related to its national growth every five years. If you refer to the -13th FYD, it appears that the Chinese government is targeting 72% of the use of digital designs for research and development. This is in line with China's desire to advance its industry to become more technological.

2.6 Cyber Hegemony

When discussing cyber power comprehensively the word refers to a country's ability to take action and exert influence in cyberspace. What was once a domain in which U.S. companies could operate freely while Chinese companies were still catching up has been replaced by increasingly vocal disagreements over how it is managed. Now the virtual world has become an open space that provides equal opportunities and access for every country to get involved and show themselves. China, which in recent years has focused on its cyber development, is starting to show its position. China's participation is also influenced by the notion that the United States has been militarizing cyberspace and sparking an international cyber arms race. This makes the virtual world a new important battleground for the two to compete for global influence.

How China's cyber development has made the United States inevitably have to admit that its superpower status has started to be challenged by China's capabilities. The United States must recognize that just as the Soviet Union and the United States never went to nuclear war, China's cyber capabilities do not mean that cyber war is inevitable. Coupled with China's increased national cyber defense, the United States must engage directly with China. This clearly shows the existence of competitive rivalry where China's position is considered to be able to compete and even threaten the existence of the United States. Especially with President Xi's statement to realize China's dream as a global Cyber Power center.

The competition between the two countries to lead each other creates competence between the two. This competition occurs because at this time China is much more prepared and established in facing the United States. In 1985 Harvard Business School Professor Michael Porter in his book entitled Competitive Advantage explained that a company must create clear objectives, strategies, and operations to build a sustainable competitive advantage. China in this competition

seems to have been better equipped to develop more offensive and ready-to use cyber capabilities with defense structures at all levels of the country. This key component has in fact become an important part of China's cyber strategy. On the other hand, the United States appears to be at a disadvantage. This is because its infrastructure vulnerabilities are more publicly documented than China's. Easy access to this information is certainly very possible for China to carry out mapping and exploitation through the PLA computer network. If China has the potential to become a cyber power, it has the ability to deter or defeat the United States through cyberspace.

The ease of access to information obtained by China is one of the competitive advantages for China. This condition has practically provided more favorable benefits for China. In addition, based on the explanation that was previously conveyed that China developed its cyber capabilities by pouring it into 10 sectors of the nation's development goals. China also prioritizes product innovation and technology development in every sector. It can be seen from how the country succeeded in developing 5G and AI networks and ended up encouraging the United States to use its economic and political capabilities to suppress China's dominance, further demonstrating China's success in meeting the needs of technology services in a new way. Huawei's products are highly innovative and attract a large market interest. According to Nouzy, the company's ability to innovate will be able to create the latest products and services, so that the company's products are in demand by the market.

China's success is basically the opening gate of their dream to become the world's Cyber Power. Which means they are able to reduce the dominance of the United States which was initially very centrist. This condition for the United States is clearly a big threat. The United States needs a dramatic change in its national cyber strategy to include federal cyber defense priorities, regulated or regulated improvements in the security of critical infrastructure networks and governments, bilateral discussions with China, and international efforts to regulate cyberspace. The United States must be able to organize better if the country still wants to secure the hegemonic position it has so far had. Although the tendency of defense strategies to focus on cyber-attacks and improving internal capabilities, the United States also needs an international strategy related to cyberspace. This

is because the information network has a very wide influence, it will be much better if the country is able to create conditions of mutual stability to prevent the development of China's cyber power.

For twenty years the Chinese PLA has indeed published articles about what they can do with cyber power. However, China has an assumption that the articles that have been frequently submitted by the United States regarding China's cyber developments are only a response. This is because to date, the United States government has complained but has not responded legally, militarily, or economically to China's cyber intrusions. This led China to assume that the United States was unwilling or unable to respond. The danger in this ambiguity is that China or America may experience a serious cyberattack and blame the other party, triggering retaliation and subsequent escalation.

When China and the United States are building each other complete military modernization to support cyber power capabilities. At the same time, China is considered to have already prepared for armed conflict with the United States by seeking military advantages in asymmetric war areas. Taiwan's potential independence is the most likely reason for the emergence of a Sino-American military conflict. However, the presence of China's strong cyber power can be a source of great power supply for the Chinese PLA. In addition, abundant natural resources can further encourage the possibility of the most common wars. With the world's two largest economies at stake, China and the United States may contest access to limited oil or soil minerals. The possibility of war is almost always there. Like the Soviet nuclear arsenal, China's possession of cyber weapons does not increase the likelihood of war, but rather its cyber power is a factor that must be considered and reduced.

China's demonstrated capability in exploiting computer networks has underlined the vulnerability of the United States to cyber-attacks from the bamboo curtain nation or even other possible attacks with similar capabilities. This has become China's competitive related to the cyber power competition that is happening. Coupled with the current cybersecurity posture of the United States, it is unable to maintain its national network and critical infrastructure in an integrated manner. Attacks on the United States defense agency are very likely to cause division because of the lack of coordination between countries and the international community, which will certainly clash with each other over cyber norms and rules. The United States has lost one point to China.

China has succeeded in showing its differences with the United States in this competition. China, through various policies and developers carried out either through the government or his non-state actors, succeeded in achieving success based on critical factors. Michael Porter said that in power competition, competitive advantage or competitive advantage can be achieved if there is a harmony between the distinguishing competencies of a company and the critical factors for achieving success in the industry that cause the company to have far better performance than its competitors.

2.7 Cyber Power Sector Political Control and Network Protection

The use of cyberspace will involve many actors in it, not only individuals as direct actors but also other important actors. Access to information in the world is also juxtaposed with the term freedom. In cyber competition, the difficulty of solving problems between China and the United States also stems from the term freedom which has different understandings and practices from each country. In general, freedom is seen as individualistic freedom, which emphasizes the freedom of the user as long as it does not harm other users. Freedom here can also be interpreted in the context of society, where every society must adapt to the framework of certain rules and norms. Freedom can also be seen in the context of the state or company, namely how the state controls the internet network of information that goes out and enters the country.

Generally, countries will block pornographic content or radical thinking, for example, or companies use the internet for their economic interests. China is known as a country that has strong protectionism against internet use. The government has great authority in controlling the flow of incoming and outgoing data. As it is known that the Chinese government also involves non-state actors in its cyber development efforts. However, the Chinese government continues to control the country's computer network. This is because there are still concerns that hacktivism could turn against the Party. China's repeated reinforcements of its domestic anti-hacking laws show that the country has concerns over the capabilities of its independent hacker population.

The Great Wall policy carried out by China shows China's efforts to show other indicators of the level of competence in cyberspace. Internet users in China use a variety of methods, including virtual private networks (VPNs), mirror sites of blocked pages owned by foreign computing services, and simple proxy

services. Limiting network access is a policy carried out by China to minimize data leakage due to ease of network access. Again, the Chinese government has strong network control for access to information of its citizens.

The main purpose of this control is censorship, namely limiting the exposure of Chinese citizens to "bourgeois-liberal ideas" and "anti-socialist China trying to combine network monitoring to form a line of defense that the government can control. When the United States government refuses to regulate the security of internal networks that are not despite the freedom and liberalism it upholds. This is in contrast to the Chinese government which mandates and enforces strict Internet security measures by incorporating regulations on hardware and software. Even at the end of December 2016, CAC (Cyberspace Administration of China) presented a new strategy for cybersecurity. This includes warnings that use of the internet for 'treason, secession, rebellion, subversion or stealing or leaking state secrets will be punished', as well as warning against anyone working with outside powers who try to subvert China's autonomy.

The so-called 'internet freedom' of the West is actually a type of cyber hegemony imposed by the United States. In the information age, seizing and maintaining an edge in cyberspace is more important than seizing sea and air command in World War II. The United States through its influence seeks to spread the notion of its freedom to be recognized and approved by many other countries. This condition is of course very opposite to that in China where all activities and internet networks there are very limited and supervised by the government.

For China, the internet is considered a major threat to the country's stability, but it is also necessary for the country's development goals. Striking the right balance between openness and repression is a delicate matter. One of the main ways China tries to balance these two concerns is by promoting domestic companies and giving them shares in the regime. Avery Goldstein in his book, Rising to the Challenge: China's Grand Strategy and International Security, provides an overview of how contemporary China is around the world. Avery argues that the key to understanding the implications of increasing economic and military capabilities, as well as China's diplomatic and foreign policy motivations and how the world (especially the United States) responds to China's "grand strategy".

The existence of different views regarding internet freedom shows that the state plays doctrine in its political policies. Doctrine itself is an important component

of a country's cyber power. This not only shows the relative importance of cyber operations but can also provide clues about their effectiveness. Since twenty years ago, China has introduced the concept of local wars under informationized conditions. The government has called for a fighting force capable of winning high-tech modern warfare and providing an asymmetrical means by which the weak can defeat the strong. This doctrine ultimately prompted Chinese leaders to modernize a broad spectrum of conventional warfare capabilities. This in fact continued until the leadership of Xi Jin Ping.

The differences and breadth of contexts make internet freedom a very difficult goal to achieve. The different paradigms of cyber warfare between China and the United States show that the different cyber world and free character create conflicts of interest. Although often the United States pressures and hopes that China can create democratic values and protect internet freedom in its country. However, in reality technological progress in China continues to run with strong protectionism by the government. Until it raises the assumption that China's cyber development is a policy that is detrimental to the United States. China is able to hack military sites, public space sites and multinational company sites and steal research data from there. The data is then used to develop domestic companies in China.

While the United States itself is more open to its citizens' internet freedom. This can be seen from the easy access to information networks through various telecommunication and technology devices and products. This is of course very different from the conditions in China. Even to find information about the bamboo curtain country is very limited by the use of different languages. In addition, access to information inside and outside has been limited. This is in fact a positive and negative value for both countries. Openness on the one hand does provide easy access and services for the community, but on the other hand it can be a threat of information leakage. If you compare in the network protections sector, China can be said to be superior to the United States.

2.8 Cyber Power in the Technology and Information Sector

When talking about cyber power, the field of technology and information is the main thing that needs to be considered. The United States until now is known to dominate in terms of software. Although on the one hand China has made great progress in its hardware such as Huawei or the development of 5G and Artificial

intelligent (AI) or the nationalization of their respective websites. However, US companies such as Microsoft, Intel, Google, Facebook, and Apple still dominate software globally and create de facto software standards.

As already mentioned, the overwhelming dominance of the United States' technology and information has in fact triggered China's rejection and distrust. China believes that the United States has the ability to damage or interfere with the functionality of any device with software made in the United States. This includes obtaining comprehensive personal and state information through their technology and information network. In addition, this dominant technology company in the United States has more or less influenced and is responsible to the government for the country's considerations regarding cyber defense strategies.

Because of the rejection and distrust of the United States in the end, it prompted the country to develop its own operating system, namely Kylin. Even this operating system is also used by the PLA. Kylin may be more secure than the Microsoft operating system used in the United States. Additionally, cyberweapons designed for Linux, UNIX, and Windows based systems may not work against Kylin. Because this operating system is not connected to an external information network, it minimizes the gap for data leakage. China is trying to narrow the gap in technology as a whole.

In conventional developments satellite technology is combined with smart, precision-guided weapons that can help military planners to precisely determine the estimated damage from attacks on civilians. This condition does not apply in cyber wars which are known to have no territorial boundaries. Unlike conventional or nuclear weapons, cyberweapons have unique capabilities for replication and dissemination. As a result, military planners cannot foresee the scale and extent of the devastation wrought by cyberweapons. It is also an argument for the creation of new rules for cyberspace similar to existing disarmament treaties for conventional and nuclear weapons. Launching cyberweapons targeting an adversary's online capabilities can in fact easily damage civilian infrastructure undetected.

In addition, in relation to the development of cyber power, the Chinese government has also developed the "Internet Plus" policy. The amount of human resources is certainly a distinct advantage. The Chinese government optimizes manufacturing, finance, healthcare and government, Internet Plus plans are aimed at building domestic enterprises in the country's mobile Internet, cloud computing,

big data and Internet of Things sectors and creating global competitors by helping domestic enterprises expand overseas. China's Cyberspace Administration and Ministry of Finance launched the $14.9 billion (RMB 100 billion) China Internet Investment Fund in January to provide equity investments in China's Internet and Internet sector companies. The Agriculture Bank of China, China Development Bank, and the Industrial and Commercial Bank of China even provided a $22.4 billion line of credit (RMB 150 billion) to companies the fund had invested in.

China does encourage funding for the technology development of its state private companies, but this is not without obstacles. In addition to Huawei, a Chinese technology company has been sanctioned by the United States, namely, ZTE. This Chinese technology company in fact became the first Chinese company to be sanctioned, precisely in 2017. According to Bloomberg, the United States imposed sanctions on ZTE in the form of a ban on buying US-made electronic components, especially telecommunications chips made by Qualcomm. Although the ban was eventually lifted after ZTE agreed to pay the fine. Learning from the incident of Huawei being banned from using Google services through its Android device or from the incident of ZTE using a telecommunications chip is enough to show that Chinese companies are still dependent on technology made in the United States.

It is known until now, the United States is still the best chip-making country in the world. China has come a long way to producing a lot of electronics, but without chips from the United States, products made by Chinese companies will still lack quality and global standards. Whereas at the end of 2018, Huawei's sales were known to be able to surpass Apple's sales and become the second largest smartphone maker in the world after Samsung. China's increase is one of the thoughts of the United States of America's ban on Chinese technology companies. The US ban is done more as an effort by the United States to make it difficult for China as a major competitor to US technology companies.

According to the MIT Technology Review report, Chinese technology companies are known to be in a race to develop 5G technology. Huawei even wants to be the mainstay of the Chinese government to dominate the world's superfast wireless network as a proof of itself as one of the top technology companies in the world. China, which has ambitions to become the world's superpower country, is considered to be sure to protect and help this company. Even this company

is predicted to be the ruler of 5G in the next 5 years. However, the inclusion of Huawei in the blacklist of trade in the United States can certainly reduce the percentage of success more or less.

2.9 Cyber Power in the Military Sector

Cyber security must be an important issue for national security and national defense, including the protection of territorial sovereignty. Since governments, critical infrastructure, and emergency services depend on the Internet, cyberspace cannot be left alone when collaborative interactions and partnerships between the public and private sectors take place.

Defense needs a new way of thinking about cyber infrastructure security and a similar approach where governments oversee security but on a broader scale. Cyber security requires strong will and leadership from national executives. Since the reform era, China's military has made both quantitative and qualitative expansion in terms of personnel and capabilities. Former United States Secretary of State Condole Rice observed that because no country threatens China, making the country's military increase too large to achieve regional interests, however, this is considered less consistent with Beijing's stated goal of "peaceful rise".

Although precise figures on China's military spending are hard to come by, there is consensus that China's military spending has increased sharply in the last two decades. China's budget is divided into three categories: personnel, operations, and equipment. However, the Chinese government is considered to have omitted several relevant categories such as weapons purchases, military research, development spending, and People's Liberation Army (PLA) revenues, not to mention less clear accounting and auditing procedures. It is clear that it is relatively easy for the PLA to hide its assets and raises suspicions that China's actual military spending could be two or three times higher than the official figure. Ambitious military modernization quickly turned the country into a formidable power and a true strategic competitor to the United States.

Despite the precise figures on defense budgets, China's PLA is clearly in the midst of an ambition to rebrand its military capabilities (either qualitative or quantitative) into offensive military capabilities. In other words, China is actively seeking to transform its military from Mao Zedong's mass-oriented, infantry-heavy "People War" army to a modern and agile force capable of projecting power in the world. To achieve this, Beijing has invested heavily in Bluewater

Navy, Acquisition of Advanced Fighter Aircraft, Submarine, Aviation Refueling, Miniature Dual Nuclear Warheads, and Tactical Nuclear Weapons. Indirectly, China is carrying out an ambitious and comprehensive "Military Revolution". The condition clearly worries China's neighbors, especially the United States.

The military increase carried out by China has also become a concern for the principle of weapons proliferation, considering that China is one of the countries that sells weapons including ballistic missiles to unreputable third parties. China describes information warfare (which includes electronic warfare and cyber operations) as the most important form of warfare. In the PLA document, the 2013 Science of Military Strategy, it stipulates that "Those who hold the superiority of network warfare may adopt network warfare to cause dysfunction in the enemy's command system, loss of control over operational forces and activities, and incompetence of weapons and equipment. Up to taking the initiative in military confrontation and creating the conditions for obtaining the final victory in the war." This is evident where in recent times China's cyber operations have attracted great attention due to suspicions of massive industrial data theft, and China's relentless efforts to access military secrets of opposing countries.

Based on speculation from public sources over the years it is known that Chinese military hackers are involved in the company's cyber espionage. One of them is in a 2013 report by cybersecurity company Mandiant. Mandiant found that the Chinese military (PLA) carried out espionage efforts in the world of corpses with commercial targets belonging to the United States. The report found that Unit 61398, of the Second Bureau, belonging to the 3rd Department of the PLA General Staff Department, had stolen hundreds of terabytes of data from at least 141 organizations in various industries starting in 2006.

President Xi Jin Ping in 2015 and 2016 announced reforms to reorganize joint operations services in addition to strict CCP surveillance to ensure the military obeys the party. The PLA reorganized its bureaucratic orders and structures, establishing new institutions to deal with conceptual domains such as cyber. In the 2015 China Military Strategy white paper, the government named cyberspace as one of the new high-ranking commands in competitive strategy and stated that the Chinese Communist Party would establish a strong cyber power. In line with the reforms for China Services in 2015 and 2016, the Chinese government succeeded in establishing the Strategic Support Force (SSF). SSF is a division tasked with consolidating different cyber offices or functions within the

PLA and they are placed under one roof. SSF is tasked with conducting offensive and defensive cyber operations against intellectual property (IP) theft. The SSF cyber unit is tasked with preparing the future battlefield by using offensive cyber-attacks.

They will attempt to lower enemy command and control, communicate, gather intelligence, and make decisions. One of the main goals of the SSF is to disrupt information and use it to defeat the enemy early in a conflict. Since its founding, SSF has continued to support services and integrate cyber effects in drills, war games and planning. President Xi's 2019 remarks signaled a shift in China's outlook from information warfare to a smarter war in which the country will showcase the merging of cyberspace with cognitive domains driven by Artificial Intelligence capabilities. The efforts made by the Chinese government are concrete actions that contemporary war forces are different from conventional forces where computer network operations only require a small number of personnel and relatively low investment of funds to achieve operating objectives. This is what China is doing.

Basically, the paradigm of thinking related to contemporary war power between China and the United States is not much different. However, there is overlap regarding the division of military network operations between the United States and China. If the United States only divides computer network operations into three component parts, namely, computer network exploitation, computer network attacks, and computer network defense. Meanwhile, according to China, the three components of military network operations consist of network reconnaissance, network attack and defense operations, and network deterrence.

The attitude of the two countries that both include cyber capabilities as an important part of their military operations network shows that cyber power competition can occur due to attacks on military systems. A country's cyber-attacks can significantly degrade the enemy's means of combat. As has been explained, the use of cyber by the opposite party will be very risky for data leakage. The leak of the data obtained does not rule out the possibility that it will be misused, especially as an opponent's military strategy. Therefore, cyber security must be of particular concern to ensure state sovereignty and security.

CONCLUSION

Cyber power competition between China and the United States is increasing, but the United States is superior to China because the United States has previously had global power dominance compared to China. The dominance of power that has been owned by the United States since the Cold War until the emergence of the United States as the holder of world hegemony is in fact still difficult to replace. Although China in recent times has experienced rapid cyber development, especially in the field of technology. However, the influence of the United States in the global order cannot simply be replaced. China still needs time to gain global recognition to replace the position and influence of the United States.

REFERENCES

Anggito, Albi, dan Johan Setiawan. *Metodologi Penelitian Kualitatif*. Sukabumi: CV Jejak, 2018.

Arianto, Adi Rio. "Cyber Security: Geometri Politik Dan Dimensi Pembangunan Keamanan Dunia Era Horizontal Abad 21." *Jurnal PIR*, Vol. 1, No. 2 (Februari, 2017): 116-117.

Bey, Matthew. "Great Powers in Cyberspace: The Strategic Drivers Behind US, Chinese and Russian Competition." *The Cyber Defense Review*, Vol. 3, No. 3 (December, 2018).

Campbell, Caitlin. "China's Military: The People's Liberation Army (PLA),"

Congressional Research Service, R46808, (June, 2021):

Daphne, Leo. *MIAW-Management In Absurd Way*. Jakarta: PT Elex Media Komputindo, 2014.

Deppa, Catherine S. "U.S. Cyber Command: An Overview", *American Intelligence Journal*, Vol. 34, No. 1 (2017):

Faida, Rahma Eliya. "Sensor Internet dan Securitization di Era Cyberwarfare: Studi Kasus Tiongkok." *Jurnal Hubungan Internasional*, Vol. VIII, No. 1 (Januari-Juni, 2015):

Harrison, Lisa. *Political Researh: An Introduction*, terj Tri Wibowo. London: Routledge, 2007.

Heginbotham, Eric, et all. "Scorecard 9: U.S. and Chinese Cyberwarfare Capabilities." (2015): 2-279.

Ikbar, Yanuar. *Metodologi & Teori Hubungan Internasional.* Bandung: PT Refika Aditama, 2014.

Institute for Security & Development Policy, "Made in China 2025", (June, 2018): 2- 31.

Jr, Joseph S.Nye. "Cyber Power." *Belfer Center for Science and International Affairs* (May, 2010): 1-24.

Kania, Elsa B, and John K. Costello. "The Strategic Support Force and the Future of Chinese Information Operations." *The Cyber Defense Revew*, Vol. 1, No. 1– Vol 6, No 2 (2018): 105-122.

Koleski, Katherine. "The 13th Five-Year Plan", *Staff Research Report,* (February, 2017): 3-12.

Lambert, Vickie A., and Clinton E. Lambert. "Qualitative Descriptive Research: An Acceptable Design." *The Pacific Rim International Journal of Nursing Research*, Vol. 16, No. 4 (October – December, 2012): 255-256.

Mamik. *Metodologi Kualitatif.* Sidoarjo: Zifatama Publisher, 2015.

Meisitha, Nadya Vira, Agung Purwanto, dan Linda Dwi Eriyanti. "Motivasi China Menguasai Cyber Teknologi." *Student Research Article* (2014): 1-5.

Moleong, Lexy J. *Metodologi Penelitian Kualitatif.* Bandung: Remaja Rosdakarya, 2000.

Nazir, Moh. *Metode Penelitian*. Bogor: Ghalia, 2005.

Nufus, Hayati. "Impian Tiongkok: Nasionalisme Tiongkok Melintas Batas dalam Pembangunan Tiongkok" *Jurnal Penelitian Politik*, Vol 11, No. 2 (Desember, 2014): 43-54.

Nursita, Rizki Dian. "Cyberspace: Perdebatan, Problematika, Serta Pendekatan Baru dalam Tata Kelola Global." *Dauliyah Journal,* Vol. 4, No. 1 (2019): 81.

Perwita, Anak Agung Banyu. *Dinamika Keamanan dalam Hubungan Internasional dan Implikasinya bagi Indonesia.* Bandung: Universitas Khatolik Parahyangan, 2018.

Rafsanjani, Lalu Azhar, Lalu Puttrawandi Karjaya, dan Khairur Rizki, "Rivalitas United States (AS) dan China dalam menjaga Security Order di Asia Timur*" Indonesian Journal of Gobal Discourse,* Vol. 2, No. 1, (Januari – Juni, 2020): 28-35.