CHINA'S ECONOMIC CYBER STRATEGY IN FACING ECONOMIC CYBER THREATS 2020 - 2023

Sylvia Octa Putri
Universitas Komputer Indonesia, Bandung, Indonesia

Hanna Tri Indah Farras S
Universitas Komputer Indonesia, Bandung, Indonesia

Dio Fathul Rachman
Universitas Komputer Indonesia, Bandung, Indonesia

Intan Fauzi Septiana
Universitas Komputer Indonesia, Bandung, Indonesia

Jerry Yeremiah Sihombing
Universitas Komputer Indonesia, Bandung, Indonesia

ABSTRACT

Digital technology has succeeded in making it easier for a country to analyse data, development, improvement of a performance or product which is then included in a network. These advances in digital technology also have a risk impact on security issues. This research examines the cybereconomic strategy applied by China in dealing with the threat of economic cybers between 2020 and 2023. With the rapid growth of information technology, China faces significant challenges in ensuring its economic cybersecurity. This research analyses the steps taken by the Chinese government to address economic cyber threats, including increased regulation, investment in cybersecurity, and cyber diplomacy efforts. In this study the researcher uses a qualitative method. Qualitative method is a research or observational procedure that produces descriptive data that emphasizes the concept of a problem in research. The findings suggest that China has adopted a comprehensive and proactive approach to protecting its economic cybersecurity, although it still faces significant challenges. The implication of this research is the importance of technological innovation in overcoming economic cyber threats in the era of digital globalization.

Keywords: China, Digital economy, Cyber security

INTRODUCTION

Globalization requires a large and fast flow of information and information processes, which is difficult to achieve without the presence of information and communication technology. Strong global demands on the transformation potential of this new technology demand communication via the internet without being hindered by time differences and regional boundaries. Now the development of information and communication technology has brought significant transformations to the concept of security (Rahmawati, 2017). Currently, countries are free to interact and communicate through cyberspace/internet. Thus, the state requires new adaptations in line with this development. So the concept of cyber security is an important element of a country in securing the stability of its security.

The transaction process carried out in the business world, without a meeting between parties using the internet media is categorized as an electronic transaction. Electronic transactions in the business world take various forms, along with the application of technology in every dimension of human life, it is also followed by the misuse of technology in the cyber realm for criminal purposes. The emergence of cyber crime is a justification that this global era is identical to the era of malignant mines. A space for everyone to do activities that can be done in everyday life in an artificial way. Security threats that are prevalent in e-commerce are phishing attacks that lead to cases of money laundering, data misuse, hacking, credit card fraud and unprotected services.

In this research, there are several reference materials from previous researchers that can be used as references. First, research made by Muhammad Nizar Hidayat in 2022 with the title " Konsturktivitisme dalam Diskursus Kebangkitan Cina di Asia Timur". The discourse on the "rise" of China highlights the role of constructivism in understanding the phenomenon. The question of whether or not China threatens other countries is linked to the constructivism paradigm that emphasizes the construction of shared identities, perceptions, and ideas among actors in East Asia. This helps to see China's role in regional politics and security more comprehensively, not just from a simplistic Realist and Liberal perspective. The difference in the research that this researcher examines is about the cyber-economic strategy targeted at the Chinese state, the renewal in the author's research is the difference in the cyber-economic factors discussed, moreover the researcher discusses not from the political culture of the country alone, but China's strategy in building the cyber economy.

According to research made by Yoga Suharman and Sugiarto Pramono in 2021 with the title " Strategi Kebangkitan Ekonomi Tiongkok dan Pendekatan Long Cycle Transisi Kekuasaan Politik Dunia" An important indicator of China's rise is economic leap and expansion, driven by the Belt and Road Initiative (BRI) which also provides economic opportunities for other countries. Consequently, China's military power has increased, triggering the United States' response with its Pivot to Asia policy, suggesting that China's rise is not just a regional phenomenon, but also a factor in global politics. The factors behind the rise involve the country's vast market potential and strategies, especially in utilizing BRI and financial strategies to drive economic growth. The election of Joe Biden as US president seems to restore the traditional position of the United States, raising challenges for China's rise, which can be further explored in the relationship between the two countries in the Biden era. The concept of Modelski is important for understanding the transition of world power and the rise of China in global politics. The difference in the research that the researcher examines is the purpose and year of research and focuses more on China's strategy to deal with the cyber economy in the 2020-2023 range.

Research made by Muhammad Ezra Pradana in 2022, with the title " Politik Luar Negeri Tiongkok Sejak Tahun 1978: Transisi, Rebalancing, dan Aktivisme". Where this research discusses that all forms of change and sustainability in Chinese foreign policy are strongly influenced by the conditions of the international order and also domestic factors. It was also found that since the beginning, China has had a vision to become a superpower, although in its journey it had to undergo various adjustments. This article has also paid more attention to the dynamics of US-China relations in the three phases above. Thus, this article has fulfilled its main purpose, which is to explain the changes and sustainability in China's foreign policy since 1978. The difference in the research that the researcher examines is that the researcher discusses China's strategy.

According to research made by Regina Niken Wilantari and Suryaning Bawono in 2021, with the title " Tantangan Dominasi Amerika Serikat olet Tiongkok dalam Perang Dagang". Based on the estimation results of the United States Threshold Autoregressive (TAR) GDP model and Chinese GDP, it is clear that the United States was hit hard in the 2008 crisis while China was strong enough to withstand the crisis with a very fast economic growth since 1979. From the comparison of forecasting results and comparison diagrams, it can be concluded that China has the potential to outperform the United States economically. The advantages and differences of our research are that we discuss how China's cyber economy has become China's influence and strategy in building China's economic quality internationally.

And the last research from, Emil Hekmawan, Fahriza Muhammad, and Ahmad Sahide in 2023, with the title " Kebangkitan Tiongkok dalam Membendung Hegemoni Amerika Serikat: Studi Kasus Sengketa Laut China Selatan". This study concluded that broadly speaking, the rise of China as a global economic and political power has changed the dynamics of international politics. China managed to become one of the countries with the largest economy in the world through a liberal economic system. Projections that China will become a super power replacing the United States still require further research. China is also actively controlling the Asia Pacific region through the Silk Road Initiative, although its provocative actions in the South China Sea could trigger conflict. Countries in Southeast Asia are increasingly dependent on Chinese investment and infrastructure development. As a result, the supremacy of the United States as a hegemonic state is threatened, especially in the context of Southeast Asia. The rivalry between China and the United States has the potential to heat up in the future. The difference between the research and what we researched is how China overcomes the cyber economy and China's strategy to grant wishes and discourse in 2020-2023.

Advances in technology and information can not only attack society, government agencies, and the military, but it can threaten all aspects of human life, such as the economy, politics, culture, and security of a country (Rahmawati, 2017). For example, in the US, almost all state offices and public administrations in the US use the internet. Fields such as industry, banking, transportation, and health administration to security or military have been PC-based and use internet networks. China's high dependence on ICT and the internet ultimately presents new weaknesses and dangers for the country's cyber network protection framework (Ardianto, 2017).

China is one of the most visible countries progressing in the economic field today. This happened because of significant achievements considering also how China's economic conditions used to be classified as very lacking in the 20th century, China began to carry out several revolutions that made its domestic economic stability heated up, so China through its centralistic leadership tried to modernize its economy and produce pragmatic policies. In the period after Mao Zedong's reign, China grew to have a more open power for international cooperation. Meanwhile, during the reign of Deng Xioping, its openness was loosened mainly to reconstruct the economic crisis that China experienced due to trade isolation during the Mao era.

This openness was also measured by the inclusion of democratic elements in the governance of international relations. China began to enter the era of multilateral trade after officially entering the World Trade Organization (WTO) in 2005. This is also an important tactic for China, as China has fully implemented the principles of a market economy. But in practice, China is an indication in the midst of developing excellence to rival the economic power of the United States. The first time in building competition is in the East Asian region, because it is geopolitically favorable for China, the considerable accumulation of US capital in the region, and also the factor of some important countries being US alliances. Therefore, China is trying to restart its East Asian identity along with its economic interests. This can be seen in China's efforts to lead regional economic cooperation in East Asia in the 21st century.

China fully recognizes the importance of cybersecurity and has increased its attention as an essential element in national security. As a step in line with the establishment of a leading group in the field of cybersecurity, the National People's Congress (NPC) conducted a review of the Cybersecurity Law in June 2016. In the early 1990s, China sought to boost its economic efforts by embracing the e-commerce sector. According to (Hongfei, 2017) in the

National Report on E-commerce Development in China of the United Nations Industrial Development Organization (UNIDO), the internet entered China in 1994, and in the past 20 years, it has created a huge impact on the industrial and commercial sectors in China. The fundamental changes brought by the Internet have merged with traditional industrial market operations, so in recent years, China's e-commerce sector has experienced rapid growth. Although in 2008, China's e-commerce faced obstacles from other countries, especially the United States.

The Office of the United States Trade Representative (USTR) released a "Notorious Market" list covering several markets in China, both online and physical. The list includes marketplaces that engage in or support trademark counterfeiting and copyright privacy, both in physical and online markets. One of the marketplaces listed is Taobao.com, which is part of the Alibaba Group, a leading e-commerce company in China that contributes to the economy through their e-commerce practices.

Digital technology has provided easy advancements in today's global life. Digital technology has successfully made it easier for a country to analyze data, develop, improve performance or products that are then put into the network. However, the advancement of digital technology also has a risky impact on security issues. In a country, each country has a policy to regulate and secure the national interests of its country. Including this digital technology revolution in addressing security issues that cover various fields such as social, economic, cultural and political. This change in globalization causes the strategic environment to change very quickly. In addressing these changes, countries must take action. According to Gartner IT Glossary, digitization is the process of changing from analog form to digital form.

The ease of this technology is a new challenge for every country to organize the world order in the digital economy and security. Security law, collectivity and cyberspace are often in the news in the current era, countries around the world have new challenges that come from the online world and technology in protecting the security of their country. Where these cyber threats can attack political systems, strategic fields and cyber law. (Simonangkir et al, 2023). Currently the world is grappling with the challenges of rampant cybersecurity attacks, as well as the State of China which is tightening its country's data security. China is increasingly strengthening its state government's sovereignty over data and cyberspace. By enacting policies and regulations, developing cybersecurity and formulating national standards for data protection and cybersecurity. Such as creating the National Security Law, the Civil Code based on 3 legal pillars: the Personal Information Protection Law (PIPL), the Data Security Law (DSL) and the Cyber Security Law (CSL).

The Office of the Director of National Intelligence explains and assesses the cyber threat in China today is the most active and sustained threat to government sectors and networks. China's leadership is currently building a more extensive governance regime for communications, cyberspace and information technology than any other country in the world. Technology has evolved at a faster pace than governments can control. China is one of the fastest moving countries in building regulations and policies that cover the digital economy, cybersecurity and online content all in one place.

Information and communication technology governance in China is best understood in laws, strategies, regulations, measures and security standards. Ensuring data protection regulations, internet content, encryption, crisis infrastructure and in strengthening industries in China through the digital economy. Most of China's current strategies and laws have been finalized, but many measures are still in draft form or have pending regulations. For example, around crisis infrastructure, data flows and human data information. This is a warning for government stakeholders in China's bureaucracy who debate the scope of implementation.

This research uses descriptive qualitative methods, namely data collected in the form of words, pictures, not numbers. Qualitative research is a research procedure that produces descriptive data in the form of written or spoken words from people and observed behavior (Moleong, 2012).

LITERATURE REVIEW

Cyberspace is a term that refers to the digital environment formed by a worldwide network of computers. Within cyberspace, information can be stored, processed and transmitted through computer networks. Cyberspace has unique characteristics, such as having no physical boundaries and allowing interaction between individuals, organizations and other entities globally. (Nasrullah,2012:95)

The digital economy is referred to as the internet economy (the internet produces the economy) to classify it as economic and social activities resulting from information and communication technology. Cyber economy also refers to economic activities that take place within cyberspace, including electronic commerce (e-commerce), digital business, and other economic activities that use infrastructure and information technology. It has a significant impact on global economic growth, technological innovation and overall business transformation. (Kustoro Budian, 2020)

In summary, cyberspace is the digital environment that enables interaction and information exchange globally, while the cyber economy is the economic activity that takes place within cyberspace. Both are interrelated and have an important role in today's digital era.

1. In a study entitled "The Rise of China in International Economic Cooperation in the Eastern Region" conducted by "Wishanti, D. P. 2016" this study has a discussion of China's economic development and its impact on international economic cooperation in the eastern region, the results of this study show that the rise of the Chinese economy has had a positive impact on economic cooperation in the eastern region, especially in terms of economic growth and trade. However, there are also challenges faced, such as economic competition and security issues. Therefore, the author recommends closer cooperation between countries in the eastern region to take advantage of opportunities and overcome challenges in international economic cooperation. The advantages of this journal are that it provides an in-depth analysis of China's economic strategy in the eastern region and the topics raised are very relevant to current global economic developments, and the disadvantages are that this journal lacks detail in explaining the research methods used such as data analysis or theoretical approaches used and the discussion of this journal is limited to a certain point of view or does not cover all relevant aspects. For example, the journal may focus on economic aspects without considering political or social aspects that are also influential in international economic cooperation.

2. Rafiq Purnama in his journal "China's Strategy in the East Asia Region" discusses China's strategy in dealing with political, economic and security dynamics in the East Asia region. This research is important because China is a major actor in regional politics and economics, so its strategy has a significant impact on regional stability and development. Purnama may use various theories and frameworks in analyzing China's strategy, such as international relations theory, geopolitical theory, or international political economy theory. Research methods used may include policy analysis, case studies, and interviews with experts and practitioners in the East Asian region. The expected research outcome of this journal is a better understanding of China's strategy in dealing with challenges and opportunities in the East Asian region, as well as its implications for regional stability and international relations as a whole. As for the shortcomings of the journal's discussion, it lacks comparisons of China's strategy with other countries in the region or with similar cases elsewhere. A stronger comparative approach could provide a better understanding of the effectiveness of China's strategy.

3. 'Systemic Analysis of China's Foreign Policy: A Case Study of Cybersecurity Cooperation with the United States in 2015' This journal discusses cybersecurity cooperation between the two countries on their bilateral relations as well as recommendations for improving the effectiveness of cybersecurity cooperation in the future, the results of this research provide a better understanding of the dynamics of cybersecurity cooperation between China and the United States in 2015, as well as the factors that influence its implementation, The shortcomings of this journal are the limitations in accessing complete and accurate data related to cybersecurity cooperation between China and the United States in 2015, which may affect the validation of the research, this journal also has shortcomings in providing a discussion of the practical implications of the research results for the foreign policy of China or the United States in the context of cybersecurity.
4. research entitled "China as a cyber giant: two voices in Beijing regarding telecommunications", the discussion in this journal is to provide an overview of the internal debate in China regarding telecommunications policy. By exploring two different voices in Beijing, the author describes the political and policy dynamics that influence the country's telecommunications strategy. An in-depth analysis of these two points of view provides valuable insight into how China formulates policies in the field of telecommunications, as well as the implications of these policies for economic cyber strategy. The shortcoming of this journal is that it lacks a comparative analysis with other countries' telecommunications policies. This comparison can help understand China's position and policies in a global context.

METHODOLOGY

Research method or design is a process needed in a research implementation. In this study, researchers used qualitative methods. Qualitative method is a research or observation procedure that produces descriptive data that emphasizes the conceptuality of a problem in research. The purpose of this qualitative research aims to examine an experiment or data collection technique which is then analyzed (Sugyono, 2018). This method approach comes from the ideas of experts, theoretical frameworks or researchers' understanding which is then developed and understood in the form of empirical data and field assessments to obtain the truth. In this study, researchers conducted data analysis techniques using narrative techniques where researchers analyzed the influence of Chinese cybersecurity on Cyber economic threats. In data collection, data searches are carried out related to research carried out such as from previous researchers, journals, books, and the latest news. Through the data will be studied, analyzed and explored in depth to be developed by researchers. After carrying out the narrative analysis steps, the researchers compiled and made conclusions about what the effect of cyber security in China on the threat of the Cyber Economy in their country.

DISCUSSION

Currently, the cyber world is experiencing five major problems such as infrastructure and data weaknesses, information conflicts in living notification, cyber power, new technologies and broadcast media and raw materials. The following review is divided into six sections. In the first section we understand the inadequacies of our infrastructure. The second section and the third section deal respectively with the dangers of information combat (report engineering, conspiracy theory, social connectedness) and a description of the digital world. Sections 4 and 5 delve into the latest technologies (such as 5G, AI) and raw material barriers. Finally, in the last section, we submit a series of pointers to grow better resilience in relation to China's Cyber issues. Online media Threat Map Checkpoint reported that more than two million cyberattacks are executed every day, and even a website is devoted to investigating Global cyber warfare directly. Of course, only a few states are targeted by DDoS (Distributed Denial of Service) parties.

Several kinds of Cyber-attacks do exist. Such as malware, phishing, or even botnets. Following in the footsteps of technological development today, the term 'cyberspace' is known to many people and has become part of the routine of today's society. Cyberspace has successfully developed to become the 'fifth domain' of community activities in addition to land, sea, air, and space due to this surrounding world gradually integrating into the lives of the population in recent decades.

However, in the midst of the increase of cyberspace, the emergence of various cyber disturbances in the form of cybercrime has caused new obstacles that not only disturb certain parties but almost all global residents without exception, so the fact that cybercrime does not have DNA samples or fingerprints to determine the perpetrator has made it easier for criminals in cyberspace to take refuge and difficult to obtain through the use of proxy servers, virtual networks themselves, or peer-to-peer software. Only time zones, physical server locations are utilized in attack techniques and country-specific tools, and indicators.

Manipulation activities in telecommunications will decrease, but phishing attacks are likely to grow. In the years since, the Chinese government has attempted to explore strategies and even sought international collaboration to combat telecommunications manipulation. In this high-pressure outreach, a cluster of telecom scams, detected in northern Myanmar, may soon collapse. In 2020, China faced various types of cyber threats, including cyber attacks that could arise from a group of foreign hackers. Organizations of other countries, or individual executors with various aspects. These threats involve manipulation attacks, espionage, cyber, malware distribution, and potential threats to the security of information and critical infrastructure. Also, some global cyber events such as ransomware attacks and coordinated cyber-attacks may also affect China's cyber security during the year.

China has implemented a range of approaches to tackle economic cyber threats, encompassing policy formulation, investment in cyber technology, market oversight, and international cyber diplomacy. They have established laws and regulations to govern online activities and safeguard data, while fostering innovation in cyber technology. Additionally, China is enhancing international collaboration to bolster cyber defense and enhance its digital standing. From 2020 to 2023, China concentrated on formulating economic cyber strategies to counter economic cyber threats. In this strategy's inception, China acknowledges the criticality of protecting cyber infrastructure, data, and information security to nurture the expansion of its digital economy.

China is intensifying international cooperation in cybersecurity to address shared challenges in the digital era. Moreover, enhancing regulation and fostering innovation in cyber technology constitute vital components of China's approach to combating economic cyber threats. From 2020 to 2023, China implemented various strategies to tackle economic cyber threats: Cybersecurity Enhancement: China is escalating efforts to fortify cyber infrastructure, safeguard sensitive data, and shield information from cyberattacks. This involves advancing cybersecurity systems and enhancing the training of security personnel. And also regulation Strengthening: The Chinese government is bolstering regulations to oversee online activities and safeguard users' intellectual property rights and personal data. This includes stricter law enforcement against cybersecurity breaches and cybercrime. Investment in Cyber Technology: China continues to invest resources in cyber technology research and development. These include the development of artificial intelligence (AI), network security, and cryptographic technologies to enhance their defenses against cyber threats. International Cooperation: China participates in international cooperation to deal with cyber threats globally. They work with other countries in sharing cybersecurity information, developing international standards, and building alliances to combat cyberattacks together.

Technology Industry Innovation and Development: China drives innovation in the cyber technology industry, such as the development of security software, hardware, and related services to strengthen their cyber infrastructure and enhance economic competitiveness in the digital age. Through this combination of strategies, China aims to increase their resilience to economic cyber threats and ensure the sustainability of their digital economy's long-term growth.

There are several reasons that encourage China to develop an economic cyber strategy in the face of cyber threats. Some of these include Increased Cyberattacks China faces serious threats from cyberattacks from both state and non-state actors. These attacks could include industrial espionage, data theft, sabotage, and other cyberattacks that could damage the country's economy and security. Digital Economy Growth: As the digital economy grows in China, more and more aspects of life and business are turning to the digital world. This makes China's cyber infrastructure more important and vulnerable to cyber-attacks. Reliance on Technology: China has become a center of technological innovation and relies on technology for sustainable economic growth.

Threats to their technology infrastructure can have a significant impact on the economy and social stability. Information Security: In order to maintain the security of confidential government information, corporate data, and citizen personal information, China needs to develop a robust strategy to protect their interests in the cyber domain. National Defense: Cyber threats can also affect China's national security, including critical infrastructure such as power, transportation, and communication systems. Cyber economic strategies are also part of a broader effort to maintain national security. Through economic cyber strategies, China seeks to address and mitigate the impact of cyber threats on their economies and security.

China's policy in overcoming cyber-attacks involves two main aspects, namely cyber sovereignty and control over the internet. Cyber sovereignty is a concept that describes the basic norms covering the relationship between states and cyberspace. The Great Firewall (GFW) is a system of regulation and censorship combination led by the Republic of China (PRC) to regulate the internet access of the Chinese people as well as supervise the domestic internet.

Great Firewall started in 1996, Great Firewall has been used to block access to certain websites. The Great Firewall is implemented by the National Security Agency (CAC), which is an entity within the Chinese Communist Party Committee (CPC).

However, in special regions such as Macau and Hong Kong the Great Firewall does not apply, as they have their own administrative systems and broader legal structures and autonomy. In 2024 Kaspersky scientists are still investigating the wave of phishing attacks from unknown associations in recent years that carried out QR code phishing attacks against Chinese residents, planning personal credit card information. The operations of this group do not seem to be affected by the situation in northern Myanmar, and according to Kaspersky statistics and monitored behavior patterns, the attacks are likely to reach their peak again at the end of the year and at the beginning of next year. APT attacks on critical targets will evolve to become more dynamic.

At the beginning of this year, Chinese authorities announced cyber-attacks against various national institutions and organizations. CVERC reported investigating a spyware artifact named 'Second Date'. This sophisticated cyber espionage tool can fully monitor the network devices on display and accommodate continuous information smuggling. The intervening destinations involve institutes that host military-industrial programs and government departments that maintain basic geographic data information. On the other hand Kaspersky also observed that several APT organizations engaged over a long period of time have optimized APT attacks on China's nuclear energy industry and unnoticed targets. Recognizing China's geopolitical advantages Kaspersky scientists evaluate that the overall APT attacks targeting the country will continue to grow in the future.

CONCLUSION AND RECOMMENDATION

It can be concluded that not only some countries are affected by cyber-attacks or threats, China also gets various threats of cyber-attacks. From what has been explained in the results and discussion that there are many cyber threats faced by the Chinese state such as manipulation attacks, espionage, cyber, malware distribution, and potential threats to the security of information and critical infrastructure. In global cyber-attacks such as ransomware attacks and coordinated cyber-attacks can also affect China's cyber security during the year. Therefore, cybersecurity in a country must be a top priority for companies and countries. Cyber security in a country is very important in maintaining the country's digital economy, one example is because it raises the potential for economic losses such as data leaks due to cybercrime which can cause huge economic losses in the country. Risks in security, As the digital economy increases, cybersecurity risks will soar. However, in dealing with this, China has cybersecurity policies in overcoming cyber threats, such as one of which is the Great Firewall. The Great Firewall or State of Unification of the Republic of China which aims to prevent access to information or websites that are deemed incompatible with the principles and doctrines of their party. The Great Firewall also breaks the Chinese state internet into regional versions that are different from the free internet in the outside world, as in for example the YouTube application cannot be accessed by the Chinese people if they do not use the help of special applications such as VPNs. This is a policy of the Chinese state in protecting the access of information by the people of the country. By 2024, Kaspersky predicts that phishing attacks will increase in China. However, telecom fraud activity will decrease, but phishing attacks may increase. In the past year, the Chinese government has sought international cooperation to combat telecom fraud. It is undeniable that not only the role of the government and the state is needed in maintaining cyber security, but the role of individuals is also very helpful for the government in securing their country from cyber threats. Through the knowledge and awareness of individuals who are increasingly mastering and sufficient about cybersecurity, it will be easier for governments and countries to maintain cybersecurity and the cyber economy. Understanding the threats and implementing a cybersecurity strategy, a country can oversee the growth of the digital economy and build a safe and trusted digital ecosystem. Thus, cyber-attacks will be reduced and can be overcome properly due to cooperation in every aspect and circle.

REFERENCES

A. BOOK

Emily, Ferguson, J., Picarsic, N., & Doshi, R. (2021, April 5). *China as a “cyber great power”: Beijing’s two voices in telecommunications*. Brookings.

Rafiq Purnama. (2021). Strategi China di Kawasan Asia Timur. *Jurnal Diplomasi Pertahanan*, *6*(3).

Reformasi Ekonomi Tiongkok & Kebangkitan Renminbi. (2019). Google Books.

B. JOURNAL AND ARTICLE

Ardiyanti, Hardini. Membangun Pertahanan Dan Keamanan Siber Nasional Indonesia Guna Menghadapi Ancaman Siber Global: Indonesia Security Incident Response Team On Internet Infrastructure(Id-Sirtii). 5(6): 100

Bayu Altair. (2020). China Digital As Counterweight Asia-Pacific Century. *Jurnal Asia Pacific Studies*, *4*(1), 72–85.

Binsar Simorangkir, Tri Legionosuko, & Surryanto Djoko Waluyo. (2023). Cyber Security Dalam Studi Keamanan Nasional: Politik, Hukum Dan Strategi. *Media Bina Ilmiah*, *17*(10), 2409–2414.

Febri Dirgantara Hasibuan, Azzahra Egidia Nuraini, Rama Maulana Putra (2022). "Kebijakan China paska perang dagang, pandemik, dan antisipasi menghadapi resesi tahun 2023"

Kemara Sukma Vinaya; Yandry Kurniawan, supervisor; Edy Prasetyono. (2018). *Analisis sistemik kebijakan luar negeri Cina: studi kasus kerja sama keamanan siber dengan Amerika Serikat tahun 2015.*

Masitoh Indriyani. (2017). Perlindungan Privasi dan Data Pribadi Konsumen Daring Pada Online Marketplace

System. *Justitia Jurnal Hukum*, *1*(2).

Muhammad Haikal (2019). "Kebijakan Censorship Tiongkok terhadap perusahaan Multinasional dalam bidang ICT

(Information Communication Technologies) (Studi Kasus Google Inc)"

Shafira Rizki Aulia (2018). "Cyber Diplomacy China terhadap Amerika Serikat tahun 2013-2017"

Wahyu Gusriandari, Guntur Eko Saputro, Lukman Yudho Prakoso (2023). "Strategi Ekonomi Tiongkok Menghadapi Intervensi Amerika Serikat Melalui Taiwan"

Wishanti, E. (2014). Kebangkitan China dalam Kerjasama Ekonomi Internasional di Kawasan Asia Timur. *Transformasi Global*, *1*(1).

C. INTERNET

Cahya Puja Ayu Shintawati. (2023, January 5). *Cyberspace di Dalam Ancaman dan Peluang Hubungan Internasional Halaman 1 - Kompasiana.com*. Kompasiana; Kompasiana.com.https://www.kompasiana.com/cahya2404/63b6bde508a8b507f9094332/cyberspace-di-dalam-ancaman-peluang-hubungan-internasional

China's Emerging Cyber Governance System | China Cyber Outlook | CSIS. (2024). Csis.org. https://www.csis.org/programs/strategic-technologies-program/resources/china-cyber-outlook/chinas-emerging-cyber

Cyber security in China. (2016). https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2016/08/cyber-security-in-china.pdf

Kaspersky Ungkap Jenis Ancaman Siber yang Bakal Merajalela Tahun Ini - Info Komputer. (2024). Info Komputer. https://infokomputer.grid.id/read/123993583/kaspersky-ungkap-jenis-ancaman-siber-yang-bakal-merajalela-tahun-ini

People's Republic of China Cyber Threat | CISA. (2024). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/china

PricewaterhouseCoopers. (2023). *A comparison of cybersecurity regulations: China*. PwC. https://www.pwc.com/id/en/pwc-publications/services-publications/legal-publications/a-comparison-of-cybersecurity-regulations/china.

Sean Michael Kerner. (2022). *Great Firewall of China*. WhatIs; TechTarget. https://www.techtarget.com/whatis/definition/Great-Firewall-of-China

ABOUT THE AUTHORS

sylvia.octa.putri@emailunikom.ac.id

annaatf99@gmail.com
intanfaooo@gmail.com

jerryyeremiah220502@gmail.com

diofathulrachman30@gmail.com