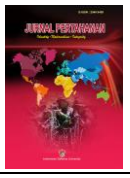

Jurnal Pertahanan: Media Informasi tentang Kajian dan Strategi Pertahanan yang Mengedepankan Identity, Nasionalism dan Integrity
Vol. 9 No. 1 (2023) pp.17-29
http://jurnal.idu.ac.id/index.php/DefenseJournal

Cyberwarfare between the United States and China 2014 -2022: in Retrospect

Nadia Dian Ardita[1*], Septyanto Galan Prakoso[2], Ferdian Ahya Al Putra[3], Arif Sulistiobudi[4], Randhi Satria[5]
[1,3,4,5]Universitas Sebelas Maret, Indonesia
[2]Universitas Sebelas Maret, Indonesia and IPS NSYSU, Taiwan

nadia.ardita97@gmail.com[1*], septyantogalan@staff.uns.ac.id[2], ferdianahya@gmail.com[3], tioyo29@outlook.com[4], ransatria@staff.uns.ac.id[5]
*Corresponding Author

Article Info

Article history:
Received: October 24, 2022
Revised: February 28, 2023
Accepted: April 29, 2023

Keywords:
China,
Cyber-security,
Cyberwarfare,
State Sovereignty,
The United States

DOI:
http://dx.doi.org/10.33172/jp.v9i1.1869

Abstract

The development of security in the context of international politics and international relations has developed from time to time. Nowadays, the practice of security done by a country's government can be imbued with the advancement of technological innovation, dubbed cyber-influenced. Hence the term cyber-security is often used to indicate the association of information technology with security. The United States and China, as two competing big-power countries, also actively utilize cyber-security over the years. This article will describe the cyberwarfare between The United States and China, focusing from 2014 until 2022. A qualitative descriptive method is used, complemented by cyber security and state sovereignty concepts to analyze the case. Results indicate that both countries are involved in cyberwarfare based on defensive reasoning. The fact that both countries are referred to as great powers in international politics also complicates the case, as they have a high-tension nature of the relationship.

INTRODUCTION

The development of digital technology is currently used to facilitate national interests. This is related to the obligation of the state to protect its nationality through increasing military or non-military strength. However, the development of digital technology also poses a new form of threat called cyber warfare. In the past, wars happened on land, air, or sea, but recently wars can be happening digitally, and tend to be difficult to detect the identity of the perpetrators (Sanchez, Lin, & Korunka, 2019). It is difficult to detect because they can act individually or in groups, and not always

represent any state. This also can be performed anywhere only with an internet connection.

When compared to traditional or conventional warfare, cyber warfare attacks intangibles, such as access to important information and data, with a lower cost of attack and causes less impact, which sometimes does not always directly impact like traditional warfare (Sanchez et al., 2019). This phenomenon then causes a state to strengthen its cyber power so that the information-based power is not new. The existence of the Advanced Research Project Agency Network (ARPANET) in 1969 and Transmission Control Protocol/Internet Protocol (TCP/IP) in 1972 which were used to transfer and connect computers showed that the development of cyber power by the state had occurred for a long time (Nye, 2010). According to Nye (2010), the development of cyber power is based on the ability to use electronic and computer-based resources to get the desired results in other domains outside cyberspace.

China is one of the countries that continue to develop its cyber power continuously. In 2004, the Chinese government had a vision described by General Xu Xiaoyan, former head of the Ministry of Communications of the Chinese General Staff, stating that China needs network confrontation technology to intercept, exploit, and destroy the enemy to sabotage the functions of information systems through computer networks (Kozlowski, 2014). In practice, its focus is on defending the PLA (People's Liberation Army) network to undertake its defense by electronic means and attacks with an integrated command with the PLA (Kozlowski, 2014). Meanwhile, in the United States (the U.S.), the Obama Administration released the Cyberspace Policy Review 2009 which discussed the government framework strategy. This review was conducted by the National Security Council and the Homeland Security Council (Hunker, 2010). From the review, five points require more attention which is: (1) improving the Governance structure for the internet; (2) building norms for the users both national and individual; (3) improving multilateral cooperation against cybercrime; (4) outlining an evolutionary path toward a "new" internet or alternative internets; and (5) define the justification for and forms of military action for cyberspace (Hunker, 2010).

In 2010, the PLA declared to establish a cyberwar base to strengthen digital security which was officially called the Information Security Base with the PLA General Staff Department as the head of the base or other known as PLA Unit 61398 (Lee, 2013). The Chinese government divides cyber warfare activities into two groups, namely hackers affiliated with the PLA and 'patriotic' hackers who work and support the operations of the government (Kozlowski, 2014). The network hacking by China emphasizes the doctrine of disrupting and crippling. This doctrine refers to Mao Zedong's theory of "protracted-war", which is a tactic to paralyze the enemy by making them look as if they are "blind" and "deaf" to achieve victory (Mulvenon, 2009).

This behavior has led to competition between China and the U.S. From the U.S. perspective, China is considered to have many intrusions and cyber-attacks on the U.S. network stealing intellectual property and important business information (Harold, Libicki, & SCevallos, 2016). On May 19 in 2014, the Department of Justice gave an official statement five defendants were suspected as the hackers that involved in the hacking

case. The five defendants were Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui (The United States Department of Justice, 2014). They were accused by the grand jury in the Western District of Pennsylvania (WDPA) of economic espionage and stealing sensitive business information (The United States Department of Justice, 2014). The United States is then concerned about the possibility that China would be willing to launch a cyber-attack to destroy crucial infrastructure during a crisis (Harold et al., 2016).

Other research shows that China has a policy that leads to coercive diplomacy through the South China Sea dispute and the Belt and Road Initiative. Therefore, it is not surprising that there are other avenues taken by China to support its steps in the context of defense and security (Pitra, 2019). Meanwhile, the U.S. has other efforts to promote the U.S. security interests in the Indo-Pacific region, one of which is through the U.S. alliance network which in this context is carried out with Australia. This policy is considered one of the most enduring and successful parts of the U.S. Foreign Policy since World War II, where its alliance members have adapted to several changes in international events, in the post-Cold War era, competition tends to be concentrated between the two great powers. This could be a step taken to counter the growing influence of China including its relation to cyber warfare (Montolalu, 2022).

Moreover, in 2021, China, which has maritime sovereignty disputes with Japan in the East China Sea and with several Southeast Asian countries in the South China Sea, passed laws that explicitly allow its coast guard to fire on foreign vessels. In this context, the U.S. is concerned that China may use this new law to assert its unlawful maritime claims in the South China Sea, which were completely rejected by a 2016 arbitral tribunal award (Aljazeera, 2021). This show that the tension between both countries is still high at the current time. Meanwhile, further writing by Al Syahrin (2018), found the rivalry between the two countries through the rise of China, Sino-the U.S. relations are becoming increasingly important and possibly dangerous for regional security stability (Al Syahrin, 2018). Hanumbhawono, Radjendra, & Ladjide (2022) found the efforts to prevent nuclear use between China and the U.S. regarding the South China Sea dispute. This effort was obtained through the Analytic Hierarchy Process (AHP) and Analytic Network Process (ANP) which showed the same results, where ASEAN-SEANWFZ (The Association of Southeast Asian Nations Southeast Asia Nuclear Weapons Free Zone) Multilateral Diplomacy became a Policy Option that received the greatest priority, and Peaceful Solutions being the highest priority Scenarios (Hanumbhawono et al., 2022).

This article tries to examine the cyber warfare between the two countries and its impact on each of them from 2014 to 2022 when there are a lot of events and cases related to cybersecurity and cyberwarfare between China and the U.S. (especially during the Obama and Trump administration in the U.S.). This article also will track back to the previous cybersecurity dialogue between the two countries to elaborate on the analysis.

METHODS

This article is using a descriptive qualitative approach method. Descriptive research aims to describe individual characteristics, phenomena, and the frequency of

association between one symptom and another in a society (Silalahi, 2009). Descriptive research also focuses on the problem of how and then explains it by conveying facts, completely, and completely (Silalahi, 2009). The data obtained in the qualitative research refer to empirical data in the form of tangible words instead of a series of numbers. It cannot also be arranged in categories/structure classification (Silalahi, 2009). Then, to obtain the data, this article uses a literature study from journal articles, proceedings, books, book chapters, online news, etc.

The process of analyzing qualitative research data follows the interactive nature of data collection with data analysis, data collection is an integral part of data analysis activities Then, data reduction is concluding the data, then sorting the data into certain concept units, certain categories, and certain themes (Miles & Huberman, 2014). In this study, the data contains various news, academic publications and articles, and also documents that are related to cyber warfare between China and the U.S. The study also makes use of two concepts that are related to the discussion namely cyber security itself, and also state sovereignty. These concepts will support the analysis of the result and discussion process.

To understand the Cyber Security concept, Craigen, Diakun-Thibault, & Purse (2014) provide various definitions of it. While on the simple definition, it can be understood as security in the cyber realm, Craigen et al. (2014) elaborated that cyber security is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights. Then, the Committee on National Security Systems (CNSS) defines Cybersecurity as the ability to protect or defend the use of cyberspace from cyber-attacks (Committee on National Security Systems, 2017). Meanwhile, the art of ensuring the existence and continuity of the information society of a nation, guaranteeing and protecting, in Cyberspace, its information, assets and critical infrastructure (Canongia & Mandarino, 2012).

In terms of sovereignty, it is a concept that refers to the legal authority and responsibility of an independent state to govern and regulate its political affairs without any foreign interference (Stanford Encyclopedia of Philosophy, 2003). In other words, a sovereign nation has the highest authority over its territory. Political authority has always been the foundation of a state's ability to maintain its sovereignty against internal and external challenges. Although all states are considered equal by law, there have always been significant disparities in the real power which makes some states more "equal" than others (Harrison & Boyd, 2018). Tunkin (2013) defined state sovereignty as the inherent supremacy of the state in its territory and independence in international relations. Both definitions emphasize that the highest authority is located in a country, which means that there are no actors or parties who are superior to a country. This is also in line with the international law principle, namely *par in parem non-habet imperium*. *Par in parem non-habet imperium* is a general principle of international law, which forms the basis of a state's immunity. This principle asserts that a sovereign state cannot exercise jurisdiction over other sovereign states (DBpedia, n.d.).

RESULTS AND DISCUSSION

Chinese Government Policy on Cyber Security

The advancement of technology has made trust in the cyber world, especially in international relations, difficult to achieve. This happens because anonymity has troubled a state to map its intentions (Baram & Menashri, 2019). This situation also raises a new dilemma called the cybersecurity dilemma, which is a situation when a state finds that its system has been leaked thus the state takes preventive action to lessen the impact that occurs (Baram & Menashri, 2019). For the Chinese government, cyberspace is part of national sovereignty because it is key for them to create national security, economic growth, and social development. Hence, the Chinese armed forces are trying to build cyber defense capabilities to conceive China as a major actor in international relations and the cyber world (The State Council Information Office of the People's Republic of China, 2019). If information and cyber security can be safeguarded, national sovereignty will be maintained as well which will lead to social stability (The State Council Information Office of the People's Republic of China, 2019).

Then, China is enhancing its defense and security through the reorganization of the PLA and the creation of a Strategic Support Force, which has brought space, cyber, electronic warfare, and psychological warfare under one umbrella to use these capabilities more efficiently and effectively. No other country, including the U.S., does this (Mallick, 2022). Meanwhile, assessments by the National Security Agency, Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Bureau of Investigation (FBI) indicate that the People's Republic of China's state-sponsored malicious cyber activity poses a grave threat to the U.S. and Allied cyber assets. China's state-sponsored cyber actors have aggressively targeted the U.S. and allied critical infrastructure (CI) personnel and organizations to steal sensitive data, key emerging and critical technologies, intellectual property, and information that could be personally identifiable (PII). Some of the target sectors include managed service providers, semiconductor companies, Defense Industrial Bases (DIB), universities, and medical institutions. These cyber operations support China's long-term economic and military development goals (Cybersecurity Advisory, 2021).

To reform the politics and economy, the Chinese government established a group named Central Internet Security and Informatization Leading Group in 2014 which is chaired by Xi Jinping (Creemers, 2016). The Chinese government also reformed the State Internet Information Office/SIIO, which was established in 2011, to be an independent entity and transformed it into the administrative office of the leading group (Creemers, 2016). This entity was then widely known by its English name Cyberspace Administration of China (CAC). The Chinese government gives CAC some exclusive powers, mainly regarding internet security which refers to Xi Jinping's slogan "without internet security, there is no national security". The range of CAC work included as follows (1) conducting the annual national security propaganda annually to raise internet users' awareness of security; (2) conducting targeted campaigns to detect online criminality; (3) announcing goals related to education and talent development; (4) assisting financial support via a linked company, the China Internet Development;

(5) creating a foundation to advance the internet security standards and laws; and (6) encouraging the development of a national security system (Miao & Lei, 2016). Moreover, the CAC is also in charge of promoting information and the Internet economy because the CAC has the authority to organize and participate in various bilateral and multilateral cooperation. The CAC also has been charged to manage all online content by deleting misinformation and rumors, banning websites, and punishing those who were liable (Miao & Lei, 2016). In managing online content, the CAC then has issued several regulations and laws, such as a regulation of Instant Messaging that requires users to use their real names and a regulation on Summoning Internet News Service Companies who violate the rules (Miao & Lei, 2016).

The PLA executes mechanization, informatization, and "intelligentization" through technological modernization such as the development of Artificial Intelligence to improve the systems (Kania & Costello, 2021). In 2015, the Chinese government also established The People's Liberation Army Strategic Support Force (PLASSF) (Kania & Costello, 2021). Furthermore, in 2017, China passed the Cybersecurity Law to protect personal data and established the Data Security Law and the Personal Information Protection Law in 2021 (Tabeta, 2022). The existence of these three policies has become the basis for the Chinese government to regulate and examine data transfers abroad from individuals and industrial companies (Tabeta, 2022). Thus, those regulations cannot be separated from economic, social, and military aspects. According to Ali Burak Darcili, there are 6 main goals for strengthening the Chinese as below (Daricili & Ozdal, 2018):

1. to obtain cutting-edge technology that has a significant impact on cyber espionage operations;
2. to ensure economic growth and stability, control the internet to maintain the governance of the Chinese Communist Party (CPC), and also control the local opposing movements, separatists, and possible attempts at social insurgency;
3. to develop measures against hostile information warfare plans based on network technology and counter operations aimed at interfering in the internal affairs of the state;
4. to establish an important counter/espionage structure against planned cyber espionage activities towards CPC by foreign intelligence agencies;
5. to support military capacity in the opportunities through advanced technologies in the field of cyberspace and develop plans for the critical infrastructure of potentially hostile military forces;
6. to organize information warfare strategies and cyber activity attacks based on network technology against areas and governments in a target.

The policies and regulations on cyber power are the Chinese government's strategy to deal with threats that may occur due to technological advancement. The development of cyber power tends to require less cost compared to conventional military development but provides greater benefits with lower risks. The policies and regulations can be the fundamental aspect for enhancing cyber security in China. Those can be the basis to establish a roadmap to improve their security in the cyber world.

Therefore, their actions are very essential in this situation. Additionally, to bolster the cybersecurity systems, the Chinese government also released a plethora of workforce development and education initiatives to build professionals (Cary, 2021). In 2017, the Chinese government began to build a campus institution called National Cybersecurity Center (NCC) or formally called National Cybersecurity Center Talent and Innovation Base in Wuhan which has support from the Chinese Communist Party (CCP) (Cary, 2021). The campus graduates are expected to be able to grow China's cyber capabilities since the NCC offers certification of skill sets to support the government's goals.

China Espionages as Disruption of Cyberspace Commitment between Two States

The differences in political views and certain competition to gain greater influence in various regions have caused the U.S. and China to become a rivalry. However, according to China cyber specialist, Amy Chang, the bilateral relationship has deteriorated to the point where both countries are mistrustful of one another's intentions, deeds, and objectives (Harold et al., 2016). Her argument is supported by James Lewis that Chinese cybersecurity is characterized by political views, competition for regional influence, and an intention to weaken the United States' position in Asia (Harold et al., 2016). To analyze the retrospect of the U.S. and China cyber warfare we need to understand first how both actors achieved a legal bilateral standing within the context of cyberspace. While the U.S. and China agree on the conclusion that each side needs to regulate the meaning of cyberspace due to the fast-moving information technology era. In 2013, both actors conducted a dialogue meeting (Harold et al., 2016).

The dialogue tried to open opportunities regarding information exchange which includes cybersecurity with the intent of getting further cooperation between the world's two largest economies. This first dialogue could be achieved because a few months ago China had been several times accused by the U.S. of concerning cyber issues such as commercial cyber espionage activities, while at the same time, China denied it (BBC News, 2013). This was a clean negotiation held in Washington D.C. While China under President Xi Jinping asserted that such dialogue could prove that his country desired that the cyber phenomenon accusation was just a misleading understanding (Nakashima, 2013). Regarding what happened in the current era, this part is supposed to be proof that two actors had already been conflicting with each other in traditional form (military and politics) and somehow, they are preventing the conflict by later extending to the space of cyber. But we see that from the beginning, there was mistrust between the two actors because the objectives tried to be achieved by Obama and Xi Jinping are different regarding their interests. The U.S. tried to stop China's illegal cyber activities by getting them to dialogue first. On the other hand, China never acknowledged any espionage action that could be considered a threat to Washington. In this context, both parties had different claims. Each party didn't want to be recognized as the party that started the friction.

The 2013 meeting between the U.S. and China showed progressive momentum to welcome further cooperation in the security and information field. Unfortunately, the objectives of the dialogue could not be achieved somehow. This prediction again came

to a dead end when in 2014 the U.S. indicted that China had conducted cyber espionage activities. A year later, China cut off the talks regarding cyberspace following such events explained below. Those facts were later clarified as several Chinese military officers stole confidential trade data from U.S. firms. Some valuable company data that was breached by the Chinese are all categorized as economically vital data from various fields such as solar panel, aluminum, and steel industries (Louie, 2017). The U.S. Attorney General Eric Holder responded to those attacks as a serious threat against the state and added that this kind of cyber ambush was held by China in a desire to get some instant hack to gain an economic advantage for their state-owned enterprises (The United States Department of Justice, 2014). This context is often linked to reciprocity. Both parties took countermeasures. These countermeasures caused the situation to get worse, which then makes problem-solving and agreements even more difficult to realize. Since both parties are considered great power, it is very difficult to find the party that can accommodate their claims.

In April 2015 Obama stated that espionage activities by the PLA were considered a national threat (The White House, 2015). This means that the U.S. is already starting to step up its cyber interest to a scheme of an arms race in the context of digital sovereignty. Later Obama also prepared the U.S. regulations to impose sanctions to prevent and against similar events in the future through Executive Order or so-called Specially Designated Nationals and Blocked Person List (SDN List) issued in April (The White House, 2015). Xi Jinping denied such actions could be done by his PLA's officers and insisted that his country will never take any political and economic benefits through such illegal ways (Rollins, Lawrence, Rennack, & Theohary, 2015). The following event successfully led the two leaders of these two great countries to hold a meeting in September 2015 regarding cyber issues in the U.S. capital (Ministry of Foreign Affairs of PRC, 2015). According to Rollins et al. (2015), the meeting reached an agreement insisted as follows:

1. provide timely responses to requests for information and assistance concerning malicious cyber activities;
2. refrain from conducting or knowingly supporting cyber-enabled theft of intellectual property, pursue efforts to further identify and promote appropriate norms of state behavior in cyberspace within the international community; and
3. establish a high-level joint dialogue mechanism for fighting cybercrime and related issues.

In this context, it can be understood that cybersecurity issues between China and the U.S. are not only limited to the defense context but are also related to the economic context. This indicates that the cyber war between the two sides is also related to the trade war that has heated up in recent years. Both parties consider the other party as a rival and even tend to be a threat to each country's trade commodities. It is also mentioned that the U.S. claims against China are vital economic data. This shows that the action taken is considered a major violation. However, in the end, China still denied that they did not do that, so an agreement between the two became difficult to reach.

The United States-China Rivalry on Cyber Empowerment

The competitiveness between China and the U.S. has affected the global scale. This is because each state possesses and engages its national interest in many regions to gain more influence. As technology is growing rapidly, both countries are playing out their significant role in cyberspace. However, this is mainly reflected in network sovereignty, cyber-hackers, cyber espionage, and cyber security (Qian, 2019). According to Qian, (2019), China and the U.S. have their definition of cyber security. For the U.S., cyberspace security is used to ensure the free flow of information and prevent unauthorized access to information systems. Whilst China believes cyberspace must be controlled and supervised by the state thus the threats can be dissipated (Qian, 2019). Cyberwarfare is a serious situation that has gotten big attention from various parties. Other research showing the relevance of cyber threats to nuclear command, control, and communications (NC3) systems is attracting increasing attention (Levite et al., 2021). But it is very important to understand cyber warfare's definition. By understanding each state's definition, it can be said that ideology defines the understanding of cyberspace.

Whilst it is ideological for China thus it was a purpose of economic benefit due to the espionage they have done. For instance, the purpose of cyber espionage is based on the act of gaining sensitive industrial base data related to technology companies that already exist in the U.S. such as defense and even IT companies. The matter above is explained by National Counterintelligence and Security Center (NCSC) (National Counterintelligence and Security Center, 2018). Therefore, China could get Intellectual Property through theft with minimum resources and get valuable results maximally as it is supported by the advancement of technology. According to the NCSC report in 2017, there were several times that the Advanced Persistent Threat 10 (APT10), a China-associated cyber espionage group (referring to the unidentified IP address that entered the U.S. official governments network providers) continued to target engineering, telecommunications, and aerospace industries. Not only that, including big companies such as Google, Microsoft, Intel, and VMware caught the links between Chinese espionage actors and the CCleaner application as stated by U.S. cybersecurity researchers. By the following year until early 2018, Price Waterhouse Coopers (PWC) reported that one of China’s Advanced Persistent Threat (APT) groups, Keyboy, started to change the target to Western organizations and another reported similar espionage activity occurred in the maritime industry, academic organizations, and private firms. In this context, it can be concluded that the economic aspect contributes to the existence of cyber espionage. This shows that the economic aspect cannot be separated from the cybersecurity context. What's more, the relationship between China and the U.S. is improving every day, especially when the war is going on.

Furthermore, according to the Taiwanese Ministry of Defense's 2021 China Military Power Report, the PLA is now able to initiate soft kill, hard kill, and electronic attacks on the western region of the First Island Chain, blocking communication and blanking signals. The PLA traditional troops can also work with cyber warriors to attack the global wireline and wireless networks. These capabilities have been sufficient to

neutralize the R.O.C. Armed Forces' air defense, command of the sea, and countermeasure capabilities (Wu & Hung, 2021).

From the discussion above, it can be seen that both are great powers, and each side claims the other and feels that as a victim, they will feel entitled to reciprocate what their opponent has done. This also encourages each party to continue to strengthen the technology they use in the context of cybersecurity.

CONCLUSIONS

The current Cyber Warfare has brought countries in the world to develop their military and non-military forces in cyberspace. One of them is China, which considers that by increasing its power in cyberspace, there will be an accelerated increase in capabilities in the economic and military fields. China made a policy through the establishment of agencies dealing with cyberspace issues, including cyber warfare under the PLA. The case that occurred in 2013 was a form of cyber warfare carried out by the Chinese government through PLA Unit 61398 against the U.S. government. Although the Chinese government denied that the hacking was not an act carried out under the command of the PLA, the investigation carried out by the U.S. government has shown strong evidence through tracking the location and identity of the five hackers. Despite having carried out the indictment, up to now, the perpetrators, in this case, have received the punishment according to the judge's decision in the U.S. This is because of the applicable legal jurisdiction and the United States government will not expressly enforce the extradition of the five defendants who suspected as the hackers that involved in the hacking case. Until now, the Chinese government will continue to carry out military strategies in cyberspace to avoid attacks and to strengthen its national security, so that China's national interests will be fulfilled.

From the description and analysis above, it can be understood that cyber warfare between China and the U.S. is a complicated situation. Both China and the U.S. claimed that their actions were considered defensive actions. The problem is that China initiated its first move by attacking the U.S. cyber structure. Even though, both China and the U.S. have organized a meeting, they have no resolution for the situation. One of the factors that influenced it since both parties are a great power. Moreover, China and the U.S. have had a high-tension relationship in recent years. Therefore, even the slightest thing can affect the tension between them, especially if it is related to security issues. The analysis on this matter is still ongoing, as the competition between the two countries will continue in the future, creating possibilities for more research and studies.

REFERENCES

Al Syahrin, M. N. (2018). China versus Amerika Serikat: Interpretasi Rivalitas Keamanan Negara Adidaya Di Kawasan Asia Pasifik. *Global & Strategis*, *12*(1), 145–163. Retrieved from https://e-journal.unair.ac.id/JGS/article/view/8153/4838

Aljazeera. (2021, February 20). US Wary China’s New Coast Guard Law Could Escalate Sea Disputes. Retrieved April 30, 2021, from https://www.aljazeera.com/news/2021/2/20/us-wary-chinas-new-coast-guard-

law-could-escalate-sea

Baram, G., & Menashri, H. (2019). Why Can't We Be Friends? Challenges to International Cyberwarfare Cooperation Efforts and The Way Ahead. *Comparative Strategy*, *38*(2), 89–97. https://doi.org/10.1080/01495933.2019.1573069

BBC News. (2013, July 9). US-China Cyber Security Working Group Meets. Retrieved March 6, 2023, from https://www.bbc.com/news/world-asia-china-23177538

Canongia, C., & Mandarino, R. (2012). Cybersecurity: The New Challenge of The Information Society. In *Handbook of Research on Business Social Networking: Organizational, Managerial, and Technological Dimensions* (pp. 165–184). Pennsylvania: IGI Global. https://doi.org/10.4018/978-1-61350-168-9.CH009

Cary, D. (2021). *China's National Cybersecurity Center: A Base for Military-Civil Fusion in the Cyber Domain*. Washington D. C. https://doi.org/10.51593/2020CA016

Committee on National Security Systems. (2017). *National Information Assurance Glossary: Committee on National Security Systems (CNSS) Instruction No. 4009*.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, 13–21. https://doi.org/10.22215/TIMREVIEW/835

Creemers, R. (2016). Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century. *Journal of Contemporary China*, *26*(103), 85–100. https://doi.org/10.1080/10670564.2016.1206281

Cybersecurity Advisory. (2021). *Chinese State-Sponsored Cyber Operations: Observed TTPs*.

Daricili, A. B., & Ozdal, B. (2018). Analysis of the Cyber Security Strategies of the People's Republic of China. *Journal of Security Strategies*, *14*(28), 1–35. https://doi.org/10.17752/GUVENLIKSTRTJ.495748

DBpedia. (n.d.). About: Par in Parem non Habet Imperium. Retrieved March 6, 2023, from https://dbpedia.org/page/Par_in_parem_non_habet_imperium

Hanumbhawono, W., Radjendra, P., & Ladjide, S. (2022). Policies and Scenarios to Prevent the Use of Nuclear Weapons between the United States and China in the South China Sea. *Jurnal Pertahanan*, *8*(1), 131–156. https://doi.org/10.33172/JP.V8I1.1653

Harold, S. W., Libicki, M. C., & SCevallos, A. S. (2016). Getting to Yes with China in Cyberspace. https://doi.org/10.7249/RR1335

Harrison, K., & Boyd, T. (2018). The State and Sovereignty. In *Understanding Political Ideas and Movements*. England: Manchester University Press. https://doi.org/10.7765/9781526137951

Hunker, J. (2010). U.S. International Policy for Cybersecurity: Five Issues That Won't Go Away. *Journal of National Security Law & Policy*, *4*(1), 197–216.

Kania, E. B., & Costello, J. (2021). Seizing the Commanding Heights: the PLA Strategic Support Force in Chinese Military Power. *Journal of Strategic Studies*, *44*(2), 218–264. https://doi.org/10.1080/01402390.2020.1747444

Kozlowski, A. (2014). *The "Cyber Weapons Gap": The Assessment of China's Cyber Warfare Capabilities and Its Consequences for Potential Conflict over Taiwan*.

Lee, M. (2013). *Top China College in Focus with Ties to Army's Cyber-Spying Unit*. Retrieved from https://www.reuters.com/article/net-us-china-cybersecurity-university-idUSBRE92N01120130324

Levite, A. E., Jinghua, L., Perkovich, G., Chuanying, L., Manshu, X., Bin, L., & Fan, Y. (2021). *China-U.S. Cyber-Nuclear C3 Stability*. Washington, DC: Carnegie Endowment for International Peace.

Louie, C. (2017, September 8). U.S.-China Cybersecurity Cooperation. Retrieved March 6, 2023, from https://jsis.washington.edu/news/u-s-china-cybersecurity-cooperation/

Mallick, P. (2022). *China's Developing Cyber Warfare Capabilities*. New Delhi: Center for Land Warfare Studies.

Miao, W., & Lei, W. (2016). Policy Review: The Cyberspace Administration of China. *Global Media and Communication*, *12*(3). https://doi.org/10.1177/1742766516680879

Miles, M. B., & Huberman, A. M. (2014). *Qualitative Data Analysis: An Expanded Sourcebook*. California: Sage Publications.

Ministry of Foreign Affairs of PRC. (2015). Xi Jinping Meets with President Barack Obama of the US. Retrieved from https://www.fmprc.gov.cn/mfa_eng/topics_665678/2015zt/xjpffgcxqhbhbldhdjbbwnfjxgsfwbfnfyhnsbzczfhzltfh/201512/t20151202_704618.html

Montolalu, R. R. K. (2022). U.S. Indo-Pacific Strategy: The Utilization of The U.S.-Australia Military Alliance as Part of The U.S. Balance of Power Strategy to Respond to China Influence in Indo-Pacific Region. *Jurnal Pertahanan*, *8*(2), 222–233. https://doi.org/10.33172/JP.V8I2.1659

Mulvenon, J. (2009). PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability. In *Beyond The Strait: PLA Missions Other Than Taiwan*. Strategic Studies Institute, US Army War College.

Nakashima, E. (2013). Chinese Hackers Who Breached Google Gained Access to Sensitive Data, U.S. Officials Say. Retrieved from https://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/2013/05/20/51330428-be34-11e2-89c9-3be8095fe767_story.html

National Counterintelligence and Security Center. (2018). *Foreign Economic Espionage in Cyberspace*. Washington, DC: National Counterintelligence and Security Center.

Nye, J. S. (2010). *Cyber Power*. Cambridge: Belfer Center for Science and International Affairs.

Pitra, H. (2019). China Coercive Diplomacy Through South China Sea Conflict and Belt & Road Initiatives. *Jurnal Pertahanan*, *5*(2), 48–60. https://doi.org/10.33172/JP.V5I2.522

Qian, X. (2019). Cyberspace Security and U.S.-China Relations. *AICS 2019: Proceedings of the 2019 International Conference on Artificial Intelligence and Computer Science*, 709–712. New York: Association for Computing Machinery. https://doi.org/10.1145/3349341.3349495

Rollins, J. W., Lawrence, S. V., Rennack, D. E., & Theohary, C. A. (2015, October 16). *U.S.–China Cyber Agreement*. CRS Insight.

Sanchez, F. C., Lin, W., & Korunka, K. (2019). *Applying Irregular Warfare Principles to Cyber Warfare*.

Silalahi, U. (2009). *Metode Penelitian Sosial*. Bandung: Refika Aditama.

Stanford Encyclopedia of Philosophy. (2003, May 31). Sovereignty. Retrieved March 6, 2023, from https://plato.stanford.edu/entries/sovereignty/

Tabeta, S. (2022, July 9). China to Enforce Cross-Border Data Transfer Rules in September. Retrieved March 6, 2023, from https://asia.nikkei.com/Business/China-tech/China-to-enforce-cross-border-data-transfer-rules-in-September

The State Council Information Office of the People's Republic of China. (2019). *China's National Defense in the New Era*. Beijing: Foreign Languages Press.

The United States Department of Justice. (2014, May 19). U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage. Retrieved March 6, 2023, from https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

The White House. (2015, April 1). Executive Order -- "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities." Retrieved March 6, 2023, from https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m

Tunkin, G. I. (2013). *Theory of International Law*. Cambridge: Harvard University Press.

Wu, T.-H., & Hung, C.-L. (2021). Cyber Warfare Capabilities of the PLA Strategic Support Force. In T.-Y. Su & J.-M. Hung (Eds.), *2021 Report on the Defense Technology Trend Assessment - Assessment of the New Generation of Chinese Communist Party's Military Technology*. Taipei: Institute for National Defense and Security Research.