International Conference on Business Economics, Social Sciences & Humanities

Cyber Espionage of F-15 Fighter Jet Data Impact To U.S. – China Relations

D Triwahyuni[1], M Azhar[2], D Cahya[3], R Andika[4]
[1]International Relations, Universitas Komputer Indonesia, Bandung
[2]Information Systems, STMIK Kaputama, Binjai

Abstract. The purpose of this study is to examine the impact of cyber espionage activities related to the F-35 Joint Strike Fighter Military Project on the relationship between the United States and China. Allegations of Chinese espionage activities first surfaced in the public sphere in early 2015. German media Der Spiegel published a number of pieces of information confirming the result of a data breach by subcontractor Lockheed Martin that allowed China access to classified data on the F-35. Cyber espionage is often carried out in order to achieve the national interests of a country in the military, political and economic fields. China's practice of cyber espionage against the United States is also an effort to fulfill its national interests. This study used qualitative methods with data collection techniques through literature study, review of books, journals, newspapers, internet media, and as well as other references. After the data that has been collected is classified according to the problems that have been identified, then it is continued by carrying out systematic content analysis and comparison with information, so that it can answer the problems raised. The results of the study show that the United States and China have not issued significant policies or cooperation in maintaining their cyber security, because they do not want bilateral relations in the economic field to be disrupted due to the data hacking incident. They only agreed that they would not carry out data hacking sponsored or assisted by their respective governments. They are reluctant to issue policies that punish one of them because they want to maintain bilateral relations for a long time, especially in the economic field.

Keywords : Cyber Espionage, National Interest, US-China Relations

1. Introduction

International relations are all relations that transcend national boundaries. Relations is running very dynamically. The interactions carried out by international relations actors are no longer only by land or sea. But it can also pass through virtual space or we can get to know cyberspace. With the renewal of ways to build relations between countries, problems that occur due to the freedom of cyber space also arise. One of them is Cyber Attack. Cyber attacks can disrupt the activities of digital information networks that individuals, companies use or even the government class can be attacked.

Advances in technology and information can not only attack, it can also threaten all aspects of human life, such as the economy, politics, culture, and security of a country [1]. For example, in the US, almost all state offices and public administrations in the US use the internet. Fields such as industry, banking,

transportation, water disinfection, health administration to security or military have been PC-based and use internet networks. The high dependence of the US on ICT and the internet ultimately presents new weaknesses and dangers for the country's cyber network protection framework [2].

The cybersecurity condition of the United States still requires massive development because all aspects of life are internet-based and computerized, so there is a risk of cyber threats entering from the US cybersecurity system which is vulnerable and has gaps. US cybersecurity system that is vulnerable and has gaps. One of the threats that attack US cybersecurity is the issue of espionage through wiretapping by China against the US. In this case, the subjects and objects of espionage are individuals or groups within one country with a note that espionage activities or other cybercriminal activities are a or other cybercrime activities constitute a cybercrime of the country concerned. For example, in February 2015 there was a DoS attack that sent false information to each computer on the targeted network and exploited an improperly configured network device via the Great Fire and CN-NYTimes hosting sites. March 2015 saw the theft of its network accessed for about a year by hackers with a case of password theft at the website register.com [3].

Based on the various conflicts regarding cyberspace between the US and China, this has finally created a sense of distrust and wariness about how each country prepares its own national defence to fulfill its national interests. An example of a cyber hacking incident carried out by a Chinese citizen against the United States is related to the high-tech F-35 Joint Strike Fighter military aircraft project. In this case China used a Chinese citizen who is an airline entrepreneur who has a factory in California named Su Bin. In his action, Su Bin was assisted by the Chinese military to oversee Su Bin's actions which were carried out in the realm of cyber space.

The impact of this incident was huge on the relationship between the US and China. In the months following the incident, relations between the two countries deteriorated further. US government began to tighten sanctions against China and restrict trade between the two countries. This caused huge losses to the Chinese economy and worsened the global economic situation. In addition, the hacking incident also sparked an international debate on information security and cyber security. The governments of the US and other countries began to tighten their policies on information security and increase efforts to prevent cyber-attacks. This sparked questions about whether countries should pay more attention to information security and cyber security or instead consider restrictions on technology and information.

However, the impact of this incident also opens up opportunities for the two countries to work together and improve their relationship. The US and Chinese governments can coordinate and work together to address cyber security issues and ensure that incidents like this do not happen again in the future. This will strengthen the relationship between the two countries and help improve the global economic situation.

The major problem formulation of this journal wants to find out how the condition of relations between the US and China after the hacking of the f-15 fighter jet data that occurred in 2015 According to the U.S. Energy and Commerce Commission's Oversight and Investigations Subcommittee based on US data, suspected data hacks from China are reported to occur frequently. Hacking of US data by China has occurred since 2007. One of the indicators that China is conducting espionage against the US is so that it can create defense equipment that has the capabilities possessed by US-produced defense equipment. Uncle Sam's country, which is still the most innovative country in technologically advanced weapons, is a driving factor for China to espionage the weapons industry from the US. However, the peak of Chinese espionage against the US occurred in 2015 which required the US to impose sanctions and change or create a pattern of their cooperation in the cyber world.

Previous studies that discuss bilateral relations between the US and China are journals written by Ardi Riyanto Rum (2019) [4]. The journal discusses the soft diplomacy policy strategy of the people's republic of China in improving bilateral relations with the US. The results of this study indicate that the

PRC and the US are countries that consider the importance of cooperation. One way to improve bilateral relations, the PRC uses soft diplomacy. Diplomacy used by the PRC in order to improve bilateral relations with the US includes a cultural approach and the application of the values adopted by the PRC which are then applied in the US [4].

A study discussing Chinese espionage against the United States was authored by Muhammad Helmi Kafa Nur Iman and Andrea Abdul Rahman Azki (2018) [5]. The journal discusses how China is spying on the United States against military data on F-15 fighter jets. The magazine's findings prove that Chinese officials stole data by sending emails containing malware, known as spyware or Trojan horses, to Lockheed his Martin employees or associates. His joint his strike his fighter on the F-35 fighter [5].

Research that also examines the cyber relationship that occurs between the One of them is the *Dampak Pembangunan Cyber Power Tiongkok Terhadap Kepentingan Amerika Serikat* conducted by Dewi Triwahyuni (D. Triwahyuni & Yani, 2018) [6]. This study explains that China's national security aims to build cyber power in defending the country's communist regime, China maintains national sovereignty and territorial integrity and China tries to position itself as a regional power and world power. All these goals are achieved in China's efforts to achieve economic stability and progress, as well as the modernization of the Chinese military. It is explained that China utilizes ICT capabilities to infiltrate the US weaker defenses and conduct attacks that threaten the security of the US civilian and military infrastructure. military infrastructure of the United States [6].

Other literature is the result of a study written by Guntomo Raharjo entitled "Strategi Amerika Serikat dalam Menghadapi Eskalasi Cyber Power Tiongkok Periode 2011-2015" [7]. (Guntomo, 2016) argue that relations between the United States and China have led China's growing cyber power into a dilemma for the United States, leading to conflict between the two countries in the context of cyberspace. The escalation of China's cyber power is seen as impeding and disrupting US national interests. Existing facts indicate that China is conducting cyber attacks against the United States, and these circumstances urge the United States to immediately improve its capabilities to ensure its cybersecurity through its defense strategy. It has only provided short-term stability and only exacerbated the U.S.-China cyber warfare [7].

The last literature reference is a book entitled "*Strategic Cyber Security*" by Kenneth Geers (Geers Kenneth, 2011) [8]. Geers (Geers Kenneth, 2011) said that cyberspace is a new conflict arena that is the basis for defense strategies and attack threats that are still unclear. Like terrorism, hackers have found hype in cyberspace. The borderless nature of cyberspace makes cyber warfare different from conventional warfare and becomes a new threat to the state. and becomes a new threat to the state [8].

2. Research Methods

This study uses qualitative research methodologies to gain a better understanding of the global maritime hubs in regional architecture. The authors used qualitative research methods to explore, analyze, and explain the relationship between theory and research topic. This paper presents qualitative analysis techniques developed on the basis of primary, secondary, and tertiary literature reviews, including speech texts, primary reports, e-books, scholarly articles, think-tank review dialogues, newspapers, official websites, and handbooks. At the end of the study, the author finds out the results from the analysis.

3. Theoretical Review

3.1. Cyber Attack

Cyber-attack or commonly called cybercrime is a crime committed by a person or group that is able to use information technology connected to the internet as a crime tool. According to Murti (2005), cybercrime is a term that is widely used to describe criminal acts using computer or internet media. computer

or the internet [9]. Cybercrime as an activity will not occur if there is no medium, namely cyberspace. However, the above analogy will be inaccurate if we relate it to the problem of territorial boundaries or regions, meaning that in the real world, we can easily identify the place (location) where a person's activity takes place [10].

System security that has many gaps can cause a a hacker to take advantage of security gaps to enter the system, damage and take data that should not be known. and take data that should not be known by outsiders. Hacker is a term used to describe a person who studies, modifies, breaks into, and exploits study, modify, and break into a computer for either his own or a group's own or group interests. Based on several definitions of cybercrime above, it can be concluded that cybercrime is an unlawful act committed using the internet. Based on the actions and motives committed by a person who commits cyber-crime, according to Hius (2014) the problem is divided into five parts, namely:

1. Cybercrime as a pure crime
   A premeditated crime in which a person knowingly, intentionally, knowingly, and intentionally causes harm, theft, or anarchy to an information or computer system.

2. Cybercrime as Gray Crime
   It is not clear whether this crime is a crime because he committed theft but did not commit a crime. It is not clear whether this crime is a crime, as it did not damage information or computer systems, but involved robberies, thefts, and anarchistic acts. system.

3. Cyber Crime Targeting Individuals
   Crimes committed against others for the purpose of revenge, or inactive acts intended to defame an individual. A motive of revenge or laziness aimed at ruining someone's reputation, trying or pranking someone for personal gratification. Examples of such actions are: Pornography, cyberstalking, etc.

4. Cybercrime attacking copyright (property rights).
   Offenses against a person's work motivated by copying, marketing, and alteration for personal or public gain, or for tangible or intangible gain.

5. Cyber Crime Targeting Governments
   Crimes against the government for the purposes of terrorism, kidnapping, or subverting government security. Terrorize, kidnap, or undermine government security. A government designed to disrupt the system of government or destroy a country.

3.2. Security Dilemma Concept

In an anarchic international system, states are in an equal position, there is no power or authority higher than these states. The position of states as actors in international relations that are equal makes states unable to guarantee their own security and survival [11]. The state must struggle to maintain its existence by making security the first concern of the state [11]. Conditions where a country feels its national interests are threatened make the country will increase its power to protect its national interests [12].

Security dilemma is one of the basic concepts in international relations. As explained by Robert Jervis, the security dilemma can be understood as "many of the means by which a state tries to increase its security decrease the security of others". The meaning of this security dilemma is that the action of a state to increase the security of its country reduces the security of other countries, causing reactions from other countries that also want to increase their security [13]. Security dilemma is basically a reflection of the

difficulty of a country's government to determine its security policy options. Security dilemma generally occurs in a condition where a country increases its defense force policy purely for self-defense but is often considered by other countries that it aims to attack [14].

In an anarchic international system, the United States and China are in an equal position. Both have a fairly balanced power in carrying out the interests of their countries in an effort to survive in the international system. The United States and China continue to escalate power where cyber power becomes a new dimension of power owned by both countries. The significant increase in cyber power by China has created a security dilemma for the United States. The security dilemma that is present in the relationship between the United States and China results in competition between the two countries in cyberspace.

3.3. Offensive-Defensive Concept

Robert Jervis explains that in a security dilemma situation a country can use the choice of offensive or defensive strategies. The choice of strategy can be seen, namely whether defensive weapons and strategies can be distinguished from offensive, and whether offensive or defensive has an advantage [15].

In addition, geographical factors and technological factors also influence the choice of strategy used. To distinguish whether offensive or defensive provides an advantage and whether an offensive posture can be distinguished from a defensive posture, Jervis simplifies in a 4-world matrix. This matrix will provide an overview of the situation that occurs when a country uses an offensive or defensive strategy in the face of external threats.

3.4. Cyber Power Concept

Cyberspace is the fifth dimension of state power competition in contemporary international relations. The concept of cyber or cyberspace itself, according to the Oxford Dictionary, is defined as relating to or characteristic of the culture of computers, information technology, and virtual reality. Meanwhile, the United Nations (UN) has its own view of cyberspace.

Different perspectives on cyberspace or cyber make the definition of cyber power also very diverse. Cyber power is often defined as a set of resources related to the creation, control and communication of electronic and computer-based information such as infrastructure, networks, software, human skills. Meanwhile, Joseph S. Nye, defines cyber power as the ability to obtain desired results through the use of electronic information resources related to the cyber domain. In a broader context, cyber power can be defined as the ability to use cyberspace to create advantage and influence in the operational environment and across the instruments of power. Cyber power can be used to obtain desired outcomes in cyberspace or can use cyberspace instruments to produce more desired outcomes in other domains outside of cyberspace.

China continues to develop internet governance, information operations, critical infrastructure protection, and rules of behavior in its cyber space as an effort to maintain its dominance in the international system. Penetration through cyber platforms is also often carried out by China to other countries in an effort to gain military and economic benefits and maintain the stability of its state power.

4. Results and Discussion

4.1. Cyber Power in Modern International Relations

The development of information and communication technology (ICT) is impacting not only social life but also global political dynamics. These developments have led to an evolution of patterns of interaction between countries that has continued significantly in recent years. Currently, exchanges between nations are not only in the real dimension, but also in cyberspace and cyberspace.

Cyber space has become a new arena for political and economic contestation between countries. This adds to the complexity of modern security and international relations. According to James Adams, a neorealist who views cyber space as an anarchic system, cyber space has turned into a new arena of war for states. Cyber space is very much in line with the realist preposition because in cyber space there is no supreme power or authority capable of governing the states within it.

In an anarchic international system, strength or power becomes the main instrument so that the greater the power possessed, the greater the possibility to survive. The forms of power in modern international relations no longer rely on conventional forms of power but also new forms of power such as power in cyberspace or cyber power. Countries began to compete in building cyber power not only as an offensive effort, but also as a defensive effort because information superiority is a key success factor in both conflict situations and conflict prevention.

Since 2007, internet security company McAfee has warned countries that there will be an arms race in cyberspace where a number of countries begin to build the ability to conduct war in cyberspace. Meanwhile, based on a report from the North Atlantic Treaty Organization (NATO), there are around 120 countries that are developing their cyber power capabilities. With competent cyber power capabilities, countries can use cyber weapons such as trojans, malware, hacking, DDoS, and so on to paralyze civilian ICT resources as well as military defense systems of other countries without disabling civilian ICT resources. resources as well as other countries' military defense systems without discrimination [16].

According to AKAMAI's report, most cyberattack traffic originates from multiple countries. China ranks first with 41%, followed by the United States with 11%, Indonesia with 7%, Taiwan with 3%, Brazil with 3%, Russia with 2.9% and India with 2.6% and 2.7% respectively, followed by the public sector at 20%. The United States and China dominate cyberattacks due to their high Internet penetration, with approximately 162 million of the 795 million Internet Protocol (IP) addresses coming from the United States and 123 million coming from the China, followed by Brazil with 41 million, Japan is 40 million, and Germany is 37 million.

The cyber-attack on Estonia in 2007 is clear evidence that conflict between countries has entered a new domain. The Distributed Denial of Service (DDoS) attack is believed to have been carried out by Russia due to the heightened tension between the two countries after the Estonian government moved the Tallin monument located in Estonia. As a result of the cyber attack, the computer networks of ministries, banks, media and political parties in Estonia could not function for more than two weeks.

The attack on Estonia increased the international community's attention to the threat of cyber-attacks. And cyberspace is considered a potential conflict zone as countries begin to improve their military capabilities. According to the New York Times, fifteen countries with the largest military budgets began to increase their budgets for their country's cyber power capabilities because they consider cyber weapons such as trojans, malware, hacking, DDoS as one of the latest tools of war.

4.2. The Dynamics of US-China Relations in Cyber Space

The relationship between the United States and China is extremely important because no other country has played such an important role in issues such as peace, security, trade and the environment. How the two countries manage their relationship will be an important determinant of not only their political and economic stability, but also that of the world. Relations between the two countries are often characterized by arguments, confrontations and confrontations due to a lack of mutual distrust.

The rapid development of China's comprehensive power and the significant expansion of national interests in cyberspace have made cyber security one of the most important issues in its relationship with the United States. Both the United States and China are now highly dependent on digital infrastructure not only for their economies but also for scientific development and security. At the same time, each country continues to improve its ability to conduct attacks on the other's digital infrastructure.

US concerns about potential cyber-attacks reached a peak in 2011 after US President Barack Obama issued the Cyber Space Policy Review stating that the risk of cyber-attacks is the most serious economic and national security challenge of the 21st century. In addition, the US military also issued a cyber defense strategy to complement the establishment of the United States Cyber Command. In fact, the US government through a national counterintelligence executive report specifically mentions China as the most active actor in cyber attacks against the United States.

The Chinese government reacted strongly to the accusations from the US government. They asserted that it is their digital infrastructure that is more often subjected to cyber attacks. Since 2009, cyber attacks against China's infrastructure have increased fifteenfold. In fact, China's Ministry of Public Security announced that the number of cyber attacks on digital infrastructure and websites in China is increasing by more than 80% per year.

In December 2011, dozens of China's most popular online shopping, microblogging, social networking and gaming sites suffered cyber attacks that resulted in the email accounts and passwords of more than 100 million users being stolen. The Chinese government also asserts that most of the attacks on their computer networks come from the United States with the number of cyber attacks from the US reaching 34,000 per year. In fact, China calls the United States the "real hacking empire.

The Chinese government also complains about a country that dominates in cyberspace. Although not directly mentioned by the Chinese government, it is believed to be the United States. Chinese Cyber watchers even note that many of the routers, servers and software used to support the internet backbone in China are manufactured and controlled by US companies. In addition, they also note that of the thirteen root servers that govern the functioning of the entire internet in the world, ten are located in the United States and the other three are in US-allied countries such as Japan, the Netherlands and Sweden. Similarly, the Internet Corporation For Assigned Names And Numbers (ICANN), the body in charge of managing all internet protocol (IP) addresses in the world, is under the mandate of the US government.

In early March 2013, US internet security firm Mandiant released a report stating that a secret Chinese military cyber unit was behind cyber attacks on US companies. Mandiant released a report containing evidence in the form of IP addresses that have been traced to Shanghai and are believed to be the IP addresses of a unit of the Chinese People's Liberation Army. Mandiant said that the 61398 cyber unit has hacked data, namely the intellectual property rights of 141 companies since 2006.

In June 2014, the Pentagon released its annual report on China's military development with a focus on China's increasing defense budget. The report stated that China has steadily increased its annual defense budget in the past two decades with the aim of optimizing ballistic missile capabilities, long-range cruise missiles, and offensive cyber operations. However, the Information Bureau of China's Ministry of Defense challenged the US report and revealed that China's military optimization is natural. In 2014, US internet

security companies again said that they had evidence showing that a group of hackers affiliated with the Chinese government cyber attacked the computer networks of experts in the US related to the Iraq war issue. However, Hong Lei reiterated that China strongly opposes all forms of cyber attacks. According to him, some US internet security companies turn a blind eye to the threat posed by the US to other countries and continue to blame China for every cyber attack that occurs.

In early March 2015, the Federal Bureau of Investigation (FBI) investigated the Chinese military's involvement in a cyberattack on the register.com website. The site worldwide he manages over 2.5 million business domains. But China's defense ministry again denied any involvement of the Chinese military in the cyberattack on the site, saying the allegations were not based on hard facts. In fact, China's Ministry of Defense has stated that it firmly opposes cyber attacks of any kind and will punish cyber crimes according to current laws. Additionally, internet watchdog GreatFire.org revealed on his March 25th that the Chinese government was involved in cyberattacks against internet companies, including her Google. However, Hua Chunying again denied GreatFire.org's statement. Hua Chunying reiterated China's position on cybersecurity issues. Hua Chunying also called for all parties to take a more constructive stance, explore ways to establish international rules through dialogue based on equality and mutual respect, and jointly promote peace, security, openness and cooperation in cyberspace. proposed to support it.

The decline in the intensity of relations between the two countries made the discussion on the Bilateral Cyber Working Group discontinued. However, issues in cyberspace remained on the agenda of discussion between the two countries in the Bilateral Strategic and Economic Dialogue in mid-2015. The dialogue could be held after in June 2015, Vice Chairman of China's Central Military Commission Fan Changlong paid a visit to the United States despite the rift between the US and China due to cyber attack issues. The visit was made to ease tensions in the relationship between the two countries. General Fan held talks with Secretary. General Fan held talks with US Secretary of Defense Ashton Carter and discussed several issues shared by the two countries such as the South China Sea dispute, cyber security issues, etc. The two military leaders reaffirmed their commitment to building sustainable and substantive military-to-military relations based on mutual trust, cooperation, non-conflict and sustainability.

The dialogue succeeded in lowering tensions between the United States and China. As a result, in September 2015, the two countries held another meeting to discuss cyber issues. During the meeting, US President Barrack Obama and Chinese President Xi Jinping announced an agreement not to conduct cyber attacks against each other. The agreement restored confidence in the bilateral relationship between the two countries.

4.3. China's Cyber Attack on the United States

The contestation in cyber space has led to several countries becoming the dominant actors in the competition, including the United States, China, Germany and Russia. Each of these countries has a good ability to conduct cyber espionage. Cyber espionage is part of a cyber attack because the goal is to steal information from other countries that can be used to carry out other attacks. The increasing use of cyber attacks as a political tool reflects a dangerous trend in international relations.

Today, a country can conduct cyber espionage against another country very easily. A country can take advantage by stealing trade secrets, intellectual property, financial data, personal identity information, and confidential data from other countries' companies, institutions, defense contractors, or governments [17]. China is one of the countries often associated with cyber espionage against other countries.

China experienced an increase in economic terms thanks to the revolution carried out during the Deng Xiaoping era which embraced the free market system. The effects of Deng's revolution were felt until now which became more advanced when China joined the WTO (World Trade Organization) so that the Chinese

market became wider. That way China's income also increased, which then profits were used to improve China's defense and domestic production in terms of weapons. Evidently China is able to reduce imports of defense equipment by preferring its own production, moreover China is able to export defense equipment to other countries.

China until 2015 has exported weapons to other countries that continue to increase. to other countries that continue to increase, "according to the Stockholm International Peace Research Institution exports in China's military sector increased dramatically by 88% in the time span of 2011-2015. With such a significant increase China became the third largest arms exporting country in the world. This poses a threat to the US because a new competing actor has emerged after Russia. Russia. However, in its development, China is suspected of conducting cyber espionage against the US, which is a country that is currently developing. against the US which is a competing country. Espionage conducted by China to compete with the US in the global arms market.

4.4. Indicators of China's Cyber Espionage Against the United States

China is in the stage of increasing capacity and capability to gain the trust of countries in the world that China has become a superior country. One of the indicators of China conducting espionage against the US is to be able to create defense equipment that has the capabilities possessed by US production equipment. Uncle Sam's country, which is still the

Uncle Sam's country, which is still the most innovative country in technologically advanced weapons, is the driving factor for China to espionage the US weapons industry. Modernization carried out by the Panda country is in the process of upgrading weapons, streamlining the number of troops in all dimensions of sea, air and land. China's military modernization in the Xi Jinping era is more emphasized. The government make the PLA more competent in carrying out its duties by incorporating elements of technology which makes China's defenses more capable of dealing with new threats that come capable of dealing with new threats coming from cyberspace. At The development of the PLA experienced a significant increase in a series of parts of the people's liberation army.

4.5. China's Cyber Espionage Activities Against the United States Regarding the F35 Joint Strike Fighter Military Project

The F-35 Joint Strike Fighter is a fifth-generation jet aircraft produced by Lockheed Martin, currently the most advanced aircraft carrier-based fighter. Production of this aircraft has been underway for a long time but many obstacles were encountered during the production period. The production cost of this aircraft is still highest than ever before. With the presence of the latest US jet aircraft made China want to also create an aircraft that could be aligned with the aircraft. However, in its development, China conducted espionage on the data of the F-35 aircraft by including Su Bin, who is a Chinese businessman domiciled in Vancouver, Canada and there his aviation industry is also established Su Bin in carrying out this cyber espionage action against THIS F-35 by phishing. Phishing is a fraudulent practice in which an attacker impersonates a reputable person through electronic mail or other media.

4.6. US Reacts to China's Cyber Espionage on Military Projects

F-35 Joint Strike Fighter The United States is one of the countries that is so dependent on cyberspace, because the US uses a computerized system in storing information. on cyberspace, because the US uses a computerized system in storing sensitive and secret government data. sensitive data and government secrets. Therefore, the United States made a policy formulation that focuses on cyberspace security called the International Strategy for Cyberspace, which was published in 2011 during the leadership of Barrack Obama. This policy is also written about strengthening partnerships, and trilateral relationships with these

steps can minimize the risk of cyber problems coming from other countries. cyber problems coming from other countries [18]. Not only making policies, the United States also imposed sanctions on China for its espionage sanctions against China for conducting espionage via cyberspace that has cost the US so much. so big. The sanctions imposed by the United States are in the form of economic sanctions against China as a reaction to its cyber espionage.

China as a reaction to cyber espionage committed by the panda country to the United States. to the United States. The sanctions were imposed before the meeting of leaders of the two countries at the Summit in California. Sanctions imposed to the suspect in the form of freezing assets and financial transactions. Then on September 24-25, 2015 a meeting was held in California. The summit held in California also discussed several points such as points such as regional and global peace, Strengthening development cooperation, strengthening bilateral relations in the military, cyber security, and eradicating terrorism. eradication of terrorism. Cyber security here keeps all cyber attacks so that they do not happen again between the two countries. . For this reason, the two countries agreed to alleviate cyber crime that harms crimes that harm the country. Furthermore, in this meeting both countries agreed to create a forum between the two countries to discuss further the In this meeting, the United States and China brought relevant ministries of both countries, intelligence agencies to communicate in order to reduce the threat of cyber crime reduce the threat of cybercrime.

4.7. US-China Cyber Security Cooperation

In the security dilemma situation experienced, the United States has two possible strategies that can be used, namely offensive strategies or defensive strategies. However, as stated earlier, the security dilemma situation experienced by the US is not significant so that the defensive strategy has a greater advantage than the offensive strategy. This is in line with the concept of security dilemma explained by the four-world matrix by Robert Jervis. The second world matrix explains how a country will use a strategy that is more compatible with the security dilemma situation faced. The status quo country will prefer to cooperate with the aggressor country because the status quo country sees the defensive strategy as more profitable than the offensive strategy.

This condition can be seen from how US President Barack Obama rejected a series of harsh measures against China, such as cyber retaliation and economic sanctions for cyber espionage committed by China against US government computer networks and private companies. An advisor to the US President revealed that the US government is concerned that such actions will potentially damage the US relationship with China as a major economic trading partner. Caitlin Hayden, a spokesperson for the White House National Security Council, said that China and the United States are the dominant actors in cyberspace, so it is important for the US and China to continue dialogue and work together to develop a common understanding of the rules of cyberspace.

In the cyber strategy released by the US Department of Defense in 2015, it was explicitly mentioned how the strategy used by the United States towards China. The US chooses to establish a cyber dialogue with China in order to maintain stable relations between the two countries. With this strategy, the U.S. will continue discussions with China through the framework of the U.S.-China Defense Consultative Talks and Cyber Working Group to provide mutual understanding and transparency regarding each country's cyber space policies, roles and missions.

During Chinese President Xi Jinping's visit to the United States in September 2015, the two leaders signed various agreements, including an agreement on cybersecurity issues. The United States and China commit cybercrime in the form of cybercrime, especially cybertheft of intellectual property, including trade secrets, business information, or other sensitive information, in order to gain competitive advantage in business or commercial spheres. and will not knowingly assist. The United States and China agree to provide

assistance and information regarding cyber activities harmful to each other upon mutual request. In addition, the parties will cooperate to investigate cybercrime, collect electronic evidence, and mitigate harmful cyber-activity originating from their territory, upon request and in accordance with their respective domestic laws and relevant international obligations. I agree to do so. Both sides also agreed to keep each other informed of the status and results of the investigation.

Cooperation is one of the defensive strategies used by the United States against China. In the cyber strategy of the US defense ministry, it has been revealed that the US will cooperate with China in the context of cyber security. Cooperation is a logical choice for the US because in this cooperation China agreed not to conduct cyber attacks against the United States. In fact, China agreed to conduct talks on international law on cyber space and form a cyber working group. This proves that with this defensive strategy, the threat of cyber attacks against US defenses can be minimized so that the US does not need to use offensive strategies. This is also in line with Robert Jervis' explanation where cooperation can and is very likely to occur if the big decision can be divided into a series of smaller decisions, if transparency can be increased, if the benefits of cheating and losses if cheated are relatively low, if cooperation can produce mutual benefits rather than mutual damage, if both parties implement a good mutual strategy and believe that the interaction will last for a long period. In addition to minimizing the threat of attacks, the US can also maintain its national security and interests, especially in cyberspace. In addition, with this cooperation, the United States can maintain good relations with China.

5. Conclusion

The practice of espionage carried out through cyberspace is a very complicated problem to solve because it is so complex in cyberspace and it is quite difficult to find evidence of such actions. Information technology at this time is needed to facilitate and accelerate the communication process which is so important in running the wheels of government. In this problem, the author argues that espionage in relations between countries is only to take advantage of the weaknesses of a country which has a negative impact on relations between countries which should be colored with mutually beneficial actions for each other, inversely proportional to the facts that occur in the field as in the case in this journal writing. In its development, the relationship between China and the United States United States is so good in trade relations, but it is not accompanied by diplomatic relations between the two countries. Diplomatic relations between the two countries with different political ideologies.

China, which is now starting to develop rapidly in the economic and defense fields. China's economy began to develop when the country opened up in a free market that followed international trends. Good development in China's This good development in China's economy has a good impact on China's defense, which has begun to enforce military reforms that make China strong in the military. China's defense, which began to enact military reforms that made China strong in defense, from the production of fighter jets to aircraft carriers that showed a strong from the production of fighter jets to aircraft carriers that show the strength of China's defense. In developing its defense, China is colored by acts of cyber espionage that often attack the United States, which has first become a militarily strong country with various defense equipment made by the Chinese defense industry made by its own defense industry and the US is also an international exporter of defense equipment with high economic value. The act of espionage, if unknown, is normal and does not become a problem even though it weakens the position of the country affected by espionage. weaken the position of the country affected by espionage. Therefore, espionage in international relations requires clear rules in order to at least reduce this espionage activity. this espionage activity. China and the US, which are now strong countries in terms of defense, should not carry out espionage excessively because defense should not conduct such espionage excessively because such actions can only reduce the trust of a country that is a friend or ally.

The defense strategy implemented by the United States is outlined in several strategic steps: optimizing cyber forces, building cybersecurity cooperation with allies, and building cybersecurity cooperation with China. The United States continues to increase the budget of cyber entities such as USCYBERCOM, CMF and US-CERT. By strengthening our cyber power, the United States can improve its national security, especially the security of its digital infrastructure. The cybersecurity cooperation that the United States has set up with allies such as the United Kingdom, France, and Brazil also improves the security of the United States' digital infrastructure. This will strengthen U.S. defenses in cyberspace and minimize the impact of Chinese cyberattacks. Barack Obama refuses to crack down on China, preferring to prioritize dialogue and cooperation. This is reflected in the several attempts he has made to discuss cyber issues with China. Cybersecurity cooperation between the United States and China commits the two countries not to carry out or assist each other in any form of cyberattack. US-chosen defense strategy through engagement can minimize Chinese cyberattacks against US.

Defensive strategies are a representation of the logical steps chosen by the United States in responding to China's cyber power escalation. These strategies were chosen because offensive strategies only prioritize short-term stability and the possibility of cyber warfare between the United States and China will be greater. In addition, these strategies were also chosen because they can minimize the threat and impact of cyber attacks carried out by China and maintain the security of US digital infrastructure while maintaining good relations with China.

References

1. Rahmawati, I. (2017) Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime)Dalam Peningkatan Cyber Defense. *Jurnal Pertahanan dan Bela Negara*, 7(2), 51-66. https://jurnal.idu.ac.id/index.php/JPBH/article/download/179/84 .
2. Ardianto, E. L.(2017). *Komunikasi Massa Suatu Pengantar (Edisi Revisi)*. https://inlislite.uin-suska.ac.id/opac/detail-opac?id=11727
3. Zhao, S. (2008). China-US Relations Transformed: Persepectives and Strategic Interactions, New York:Routledge, Hal 23.
4. Rum, A.R. (2019). Kebijakan Soft Diplomacy Republik Rakyat Tiongkok Dalam Peningkatan Hubungan Bilateral Dengan Amerika Serikat. WANUA: Jurnal Hubungan Internasional. Vol.4(1).
5. Iman, M.H.K.N., Andrea, A.R.A., (2018). Aktivitas Spionase Republik Rakyat Tiongkok ke Amerika Serikat Terkait Proyek Militer Pesawat F-35 Joint Strike Fighter Pada Tahun 2014-2017. Jurnal Ilmu Hubungan Internasional. Vol.2(1). 43-54.
6. Triwahyuni, D., Yani, Y.M., (2018). Dampak Pembangunan Cyberpower Tiongkok Terhadap Kepentingan Amerika Serikat. Jurnal Ilmu Politik dan Komunikasi. Vol.8(1).
7. Raharjo, G. (2016). Strategi Amerika Serikat Dalam Menghadapi Eskalasi Cyber Power Tiongkok Periode 2011-2015. Jurnal Hubungan Internasional. Vol.4.
8. Geers, K. (2011). Stategic Cyber Security. Estonia, CCDCOE. Vol.1. 9-17.
9. Murti, H. (2005). Teknologi Informasi dan Komunikasi:*Cybercrime.*
10. UNESCO (2000). The International Dimension of Cyber Space Law, (England: Ashgate Publishing Ltd., 2000) Hal 128.
11. Jackson, R, George S.(2005). Introduction to International Relation (Penerjemah: Dadan Suryadipura). Yogyakarta, Pustaka Pelajar. 300-301

12. Barry R. Posen.(1993). The Security Dilemma and Ethnic Conflict. http://web.mit.edu/SSP/people/posen/security-dilemma.pdf .vol. 35. 22-47.
13. Robert, J.(1978). Coorperation Under the Security Dilemma. Cambridge, Cambridge University Press. Vol. 30. 40-42.
14. Robert, J.(1978). Realism, Neoliberalism, and Cooperational International Security. Cambridge, The MIT Press. Vol.42. 45.
15. Daniel T.(2009). *From Cyberspace to Cyberpower : Defining the Problem*. https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-02.pdf?ver=2017-06-16-115052-210 . Vol.1 , Chapter 2.
16. R, Ardi.(2019) "Kebijakan Soft Diplomacy Republik Rakyat Tiongkok Dalam Peningkatan Hubungan Bilateral Dengan Amerika Serikat." WANUA: Jurnal Hubungan Internasional 4.1. 19-42. http://journal.unhas.ac.id/index.php/wanua/article/view/14061
17. A, Rissa.(2021) "Hegemoni Dibalik Hubungan Bilateral Tiongkok-Indonesia." Jurnal Pamator: Jurnal Ilmiah Universitas Trunojoyo 34-39. https://journal.trunojoyo.ac.id/pamator/article/view/9004https://journal.trunojoyo.ac.id/pamator/article/view/9004 .
18. A, Shanti.(2017) "Konsep Balance of Power dalam Rivalitas Amerika Serikat dan Tiongkok di Laut Tiongkok Selatan." 2-4. https://www.researchgate.net/profile/Shanti-Amelia/publication/342437435_Konsep_Balance_of_Power_dalam_Rivalitas_Amerika_Serikat_dan_Tiongkok_di_Laut_Tiongkok_Selatan/links/5ef45083299bf15a2ea095d9/Konsep-Balance-of-Power-dalam-Rivalitas-Amerika-Serikat-dan-Tiongkok-di-Laut-Tiongkok-Selatan.pdf .